ТВИНИНГ ПРОЈЕКАТ ЕУ
Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије

ВЕЗЕ CYBER КРИМИНАЛА СА ИРЕГУЛАРНОМ МИГРАЦИЈОМ И ТРГОВИНОМ ЉУДИМА

уредник
Др Владимир Урошевић

Министарство унутрашњих послова Републике Србије
2014

ВЕЗЕ *CYBER* КРИМИНАЛА СА ИРЕГУЛАРНОМ МИГРАЦИЈОМ И ТРГОВИНОМ ЉУДИМА

Београд
2014.

ВЕЗЕ *CYBER* КРИМИНАЛА СА ИРЕГУЛАРНОМ МИГРАЦИЈОМ
И ТРГОВИНОМ ЉУДИМА

Издавач:
Министарство унутрашњих послова Републике Србије

Уредник:
др Владимир Урошевић

Рецензенти:
проф. др Озрен Џигурски
проф. др Божидар Бановић
проф. др Душан Старчевић

Лектор и коректор:
Гордана Милић

Припрема за штампу:
аутори

Дизајн корица:
др Ана Батрићевић

Техничко уређење:
Гордан Радомировић

Штампа:
ИГТП "Макарије" доо Београд
www.makarije.rs

Тираж:
100

Организатори овог истраживања одају

ПРИЗНАЊЕ

следећим особама и институцијама за њихов драгоцени допринос овом пројекту:

проф. др Милан Жарковић - Криминалистичко полицијска академија

проф. др Мирјана Дракулић - Универзитет у Београду, Факултет организационих наука

проф. др Слободан Миладиновић - Универзитет у Београду, Факултет организационих наука

др Владимир Урошевић - Министарство унутрашњих послова Републике Србије

др Ана Батрићевић - Институт за криминолошка и социолошка истраживања, Београд

др Весна Лукић - Институт друштвених наука, Београд

доц. др Звонимир Ивановић - Криминалистичко полицијска академија

мр Ратимир Дракулић - Универзитет у Београду, Факултет организационих наука

Светлана Јовановић - Универзитет у Београду, Факултет организационих наука

Лазар Јанковић, вођа пројекта - Министарство унутрашњих послова Републике Србије

Митар Ђурашковић - Министарство унутрашњих послова Републике Србије

Снежана Стојичић - Министарство унутрашњих послова Републике Србије

Лидија Милановић - Центар за заштиту жртава трговине људима

Небојша Гарић - Привредна комора Србије

David Cater, стални саветник за твининг пројекат - Велика Британија

Весна Стојисављевић, асистент сталног саветника за твининг пројекат

Садржај

ИЗВОДИ ИЗ РЕЦЕНЗИЈА И МИШЉЕЊА РЕЦЕНЗЕНАТА

„На основу добијених података, научним и социолошким методама и статистичким анализама добијени су резултати који указују на узроке који, почев од друштвених, материјалних и технолошких услова и савремених околности воде до појаве и експанзије cyber криминала. Ове друштвене, технолошке и криминалне условљености имају у великој мери утицаја и на области ирегуларних миграција и трговине људима, што је био основни концепт истраживања реализованих у одговарајућем Пројекту, а чији су резултати приказани у публикацији.

Ова истраживања у области ирегуларних миграција и трговине људима имају и шире импликације, с обзиром на то да су обухватила веома велики број испитаника различитих категорија лица, међу којима су били и стручњаци из обе области. Из тог разлога, добијени резултати могу бити коришћени и од стране других институција и могу дати основе за даља, дубља и прецизнија истраживања у области ирегуларних миграција и трговине људима, али и у области високотехнолошког криминала, као и у будућим истраживањима о појавама нових облика криминалних активности, у оквиру ових области криминалитета.

Имајући у виду значај друштвених мрежа и савремених облика комуникације путем информационих мрежа, као и наведених карактеристика cyber криминала, јасно је уочљива чињеница да сви фактори друштва, али и међународна заједница уопште, имају велику одговорност у ефикасном регулисању ове области и правовремене заштите корисника информационо-комуникационих технологија, као и у сузбијању криминала у области ирегуларних миграција и трговине људима.

С обзиром на постојећи тренд развоја средстава и области примене информационих технологија, укључујући и повећање интереса и нове активности у области cyber криминала, неопходно би било, у догледно време и према могућностима, наставити истраживања у континуитету, по приказаним темама у оквиру публикације и Пројекта, и то у областима примене конкретних мера, нових информационих технологија и средстава, у циљу борбе против cyber криминала и сузбијању криминала у области ирегуларних миграција и трговине људима.

На основу истраживања спроведених у оквиру Пројекта, може се констатовати да добијени резултати истраживања, приказани у публикацији, верно приказују постојеће стање у областима cyber криминала и криминала у области ирегуларних миграција и трговине људима, у Републици Србији, и стога могу бити од велике користи и послужити за даља истраживања и доношење конкретних мера у наведеним областима.

На основу свега изложеног и приложеног у тексту као рецензент сматрам да публикација има значај и ниво монографије“

проф. др Озрен Џигурски
Факултет безбедности, Универзитет у Београду

„Предмет овог истраживања обухвата две криминалне појаве које на први поглед немају додирних тачака, осим што имају криминални карактер и што су у у значајној експанзији, те захтевају адекватну друштвену реакцију у циљу њиховог спречавања и сузбијања. Иако традиционални методи ирегуларних миграција и трговине људима, уз извесне модификације и прилагођавања, остају исти, савремене информационо-комуникационе технологије извршиоцима ових кривичних дела пружају моћно и мултифункционално средство за развијање и прикривање своје криминалне активности. Управо области у којима долази до споја ирегуларних миграција, трговине људима и информационо–комуникационих технологија представљају оквир истраживања чији су, научно верификовани резултати представљени у овој публикацији.

Теме којима се аутори овде баве, тичу се, са једне стране, појмовног одређивања високотехнолошког криминала, његових појавних облика, начина спречавања и сузбијања, а са друге стране обима и размера злоупотребе информационих технологија у сврху ирегуларних миграција и трговине људима на територији Републике Србије. Приказан је и механизам за праћење и спречавање ових криминалних појава, а на основу доступних података дат је је преглед постојећег стања у нашој држави. Публикација читаоцима пружа могућност да увиде значај успостављања ефикасног система за превенцију високотехнолошког криминала, ирегуларних миграција и трговине људима, посебно у оном делу где се информационо-комуникационе технологије користе у сврху ирегуларних миграција и трговине људима. Ово истраживање има и шире импликације, с обзиром да је, у емпиријском делу, обухватило значајан број испитаника различитих категорија, међу којима су били и стручњаци из обе области. Приказани резултати могу бити солидна основе за даља истраживања у области ирегуларних миграција, трговине људима, високотехнолошког криминала, као и за истраживања међусобних релација у оквиру ових криминалних појава.

Научни и стручни квалитет рукописа је неспоран, јер су теоријско-емпиријским путем потврђена нека страна и домаћа искуствена сазнања, али су откривене и неке нове везе и односи између делова предмета истраживања о којима раније није писано. Са стручне стране, то значи помоћ свим субјектима који се баве овом проблематиком да лакше идентификују носиоце проблема и саме проблеме, те да се са њима изборе на најадекватнији начин. Публикација ће послужити научним и стручним радницима да наставе рад на овом пољу, али и да реше оперативне проблеме у сталном супротстављању свим облицима ирегуларних миграција, трговине људима и високотехнолошког криминала.

Актуелност предмета истраживања, утемељена и коректно спроведена методологија истраживања, преко 2000 испитаника обухваћених узорком истраживања, табеле, графикони и пратећи текст којима се илуструју резултати емпиријског истраживања, обимна и релевантна литература коришћена у теоријским разматрањима, те прецизна анализа међународне и домаће легислативе, представљају вредност ове монографије. Иако је учествовало више аутора из различитих научних области и институција, текст је језички и стилски прилично уједначен.

Поглавља су логички и садржински коректно распоређена. Језик и стил су јасни и прецизни. Коришћена литература је релевантна и актуелна, а њено навођење у складу са научним стандардима.

Сматрам да због значаја, обухватности и осталих елемената књига има карактеристике монографије. "

проф. др Божидар Бановић
Правни факултет, Универзитет у Крагујевцу

„Интернет попут митског бога Јануса има два лица. У једном лику се јавља као глобални, дистрибуирани, мултимедијални и интерактивни информациони систем, а у другом лику као глобална универзална комуникациона инфраструктура. Оба вида интернета могу бити искоришћена за криминалне активности, специфично у области ирегуларних миграција и трговине људима, како је то у студији и наглашено „као циљ, средство и место извршења кривичног дела." Спроведена истраживања показују да већина учинилаца високотехнолошког криминала у Србији припада старосној доби између 25 и 35 година, што је у складу са светским трендовима, а што се означава и појмом Y генерације, рођених између 1980. и 2000. године. Реч је о генерацији која је расла заједно са интернетом и широкораспростањеном употребом рачунара у друштву.

Специфично, у области ирегуларних миграција и трговини људима доминира лични контакт у процесу вршења криминалних дела, а не софистицирано коришћење информационо-комуникационих технологија, што се може разумети имајући у виду ниски образовни и социјални положај учесника, који најчешће потичу са маргина друштвене лествице. Запажено је да азиланти више користе производе високих технологија. Сами организатори кримогених радњи користе средства из области информационо-комуникационих технологија, првенствено мобилне телефоне и интернет сајтове са лажним огласима како би врбовали људе, организовали транспорт или експлоатацију људи – жртава.

Ова монографија, поред резултата који ће бити од непосредне користи приликом успостављања ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије, може бити од већег значаја у осмишљавању и имплементацији одговарајућих мера на националном нивоу за превенцију и сузбијање криминалних дела у области високотехнолошког криминала. Такође, може да буде од користи у процесу образовања свих заинтересованих страна у борби против ове врсте криминала. Монографија представља и вредан научни допринос у више научних дисциплина, које се баве проблематиком злоупотребе информационо-комуникационих технологија, било да припадају пољу техничко-технолошких или друштвено-хуманистичких наука. Будући истраживачи наћи ће овде обиље података познатих под одредницама вискотехнолошки криминал, cyber криминал или, генерално, злоупотреба рачунара, како би обогатили и продубили своја даља истраживања.

По обиму, дубини анализе и референцама рецензирано дело је монографског карактера"

проф. др Душан Старчевић
Факултет организационих наука, Универзитет у Београду

УВОДНА РЕЧ

У оквирима Министарства унутрашњих послова Републике Србије приликом разраде многих проблема и питања, у већини случајева, користи се емпиријски метод. Проверена практична решења и практично примењиви методи најчешће имају предност. У току припрема за реализацију твининг-пројекта дошло се на идеју да се споје практичне и научне димензије, које би у заједничком напору, са научним институцијама и другим заинтересованим институцијама дале вишеструко значајне и практично проверене, као и научно засноване резултате. Научно истраживање чији су резултати представљени у овој публикацији, одвијало се у оквиру твининг-пројекта „Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије“, који се спроводи од стране представника Велике Британије и Републике Чешке, а чији су корисници Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Управе криминалистичке полиције и Управа граничне полиције Министарства унутрашњих послова Републике Србије. У оквиру активности 1.1. д овог пројекта предвиђено је истраживање високотехнолошког криминала, његовог обима и појавних облика у Републици Србији, као и примене информационо-комуникационих технологија за вршење кривичних дела, у вези са ирегуларним миграцијама и трговином људима. У сврху научног истраживања и међусобне сарадње на његовој реализацији закључени су уговори са еминентним научно-истраживачким институцијама (Институт за криминолошка и социолошка истраживања, Институт за друштвене науке), факултетима (Криминалистичко-полицијском академијом, Факултетом организационих наука), као и са Привредном комором Србије. Сарадња у оквиру истраживања је остварена и са Центром за заштиту жртава трговине људима и другим институцијама чији су представници пружали потребне информације, учествовали у анкетама и друго.

Ирегуларне миграције и трговина људима у савременом свету су реалност, како у развијеним земљама, тако и у државама које су у развоју. Традиционални методи ирегуларних миграција и трговине људима остају исти, али савремене информационо-комуникационе технологије пружају извршиоцима ових кривичних дела досада неслућене могућности да пронађу већи број жртава и рекламирају своје услуге без обзира на просторно ограничење и државне границе. Иако постоје одређена сазнања на који начин се ове технологије могу злоупотребити у сврхе ирегуларних миграција и трговине људима, слика о томе како се оне злоупотребљавају и у ком обиму и даље је прилично непозната. И сама област високотехнолошког криминала остаје недовољно истражена упркос чињеници да се у овде последњих година пуно напредовало. Истраживање које овде представљамо покушало је да пружи широј научној и стручној публици и свим другим заинтересованим странама научно верификоване резултате у наведеним областима.

У оквиру ове публикације представљени су на научним методама засновани резултати истраживања о високотехнолошком криминалу, његовим појавним облицима и начину његовог спречавања на територији Републике Србије. У исто време, обављено је истраживање о обиму и размерама злоупотребе информационих технологија у сврхе ирегуларних миграција и трговине људима на нашој територији. Пружен је и детаљан приказ механизама за праћење и

спречавање наведених појава и дат је преглед постојећег стања у нашој држави на основу доступних података. Посебан значај публикације огледа се у чињеници да је на основу научно заснованих метода и научним методама проверених чињеница читаоцима пружена могућност да на конкретном истраживању увиде значај успостављања ефикасног система за превенцију високотехнолошког криминала, ирегуларних миграција и трговине људима, посебно у оном делу где се информационо-комуникационе технологије користе у ове сврхе. Ово истраживање има и шире импликације с обзиром да је обухватило веома велики број испитаника различитих категорија лица међу којима су били и стручњаци из обе области. Резултати ће, надамо се, бити коришћени и од стране других институција и могу дати даље основе за дубља и прецизнија истраживања у области ирегуларних миграција и трговине људима, али и високотехнолошког криминала, као и у ближим и даљим везама у оквиру ових облика криминалитета.

Жеља припадника Министарства унутрашњих послова и научника који су, заједничким напорима, више од годину дана, сарађивали на реализацији истраживања јесте да се резултати истраживања, представљени у Монографији користе за унапређење система за спречавање и сузбијање криминала у наведеним областима, али и да служе као инспирација за даље бављење и унапређење праксе и науке у овим областима.

Свесни смо и чињенице да су наведене области истраживања бескрајне, као и криминална делатност, али се надамо и да ће ова публикација скренути пажњу на потребу да се на систематичан и одговоран начин приступи овим друштвено опасним појавама, које су се знатно трансформисале у XXI веку.

У име аутора:
главни и одговорни уредник
саветник твининг-пројекта
шеф Одсека за електронски криминал
др Владимир Урошевић
научни сарадник Института за упредно право у Београду

др Владимир Урошевић
Министарство унутрашњих послова Републике Србије, Институт за упоредно право

Снежана Стојичић
Министарство унутрашњих послова Републике Србије

Лидија Миловановић
Центар за заштиту жртава трговине људима

МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

1. ПРОБЛЕМ ИСТРАЖИВАЊА

Појава рачунарских мрежа и интернет сервиса *WorldWideWeb*-а утицала је вишеструко на многе аспекте савременог живота и на развој специфичних видова криминала.

Иако је још увек присутна велика разноврсност појмова и покушаја дефинисања кривичних дела извршених у оквиру рачунарских мрежа и интернет сервиса, за потребе овог истраживања користиће се термин cyber криминал или високотехнолошки криминал. Cyber криминал је такав облик криминалног понашања у cyber простору у коме се информационо-комуникационе технологије и системи, првенствено рачунари и рачунарске мреже, појављују као циљ, средство и место извршења кривичног дела. Притом се под cyber простором подразумева или врста "заједнице" сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова или "простор који креирају компјутерске мреже". Он је вештачка творевина која захтева високу техничку опремљеност, добру информациону инфраструктуру и који је ничија и свачија својина, у коме паралелно коегзистирају виртуелно и реално и код кога је комуникација колективна. У таквом окружењу изузетно је тешко говорити о националним размерама криминала и друштвеној опасности, бар не у конвенционалном смислу речи. Зато се овај криминал сврстава у најизразитији облик транснационалног криминала против кога ни борба не може бити конвенционална. Поготово што друштвени, социјални и економски контекст овог криминала није истоветан са класичним транснационалним и организованим криминалом.

Дела високотехнолошког криминала се нужно разликују од класичних кривичних дела из више разлога. Она у највећем броју случајева поседују елемент иностраности. У самом делу високотехнолошког криминала често су инкорпорирана још нека кривична дела која се могу извршити и на класичан начин – нпр. превара, фалсификовање, крађа идентитета и слично. Ова дела претпостављају коришћење нових технологија за њихово извршење. Отуда је реакција законодаваца, у земљама које су ову групу кривичних дела инкриминисале, ишла у правцу дефинисања низа нових појмова, до тада непознатих националним правним системима.

Карактеристике високотехнолошког криминалитета као што су: анонимност, брзина, организованост, виктимизација великих размера, као и мултијурисдикциона природа, посебно отежавају рад органа гоњења и доводе до радикалних промена у њиховој политици. Овај облик представља нову форму транснационалног организованог криминала и с тога је неопходно унапредити законску основу супротстављања овом виду криминала, разматрати улоге и приоритете у овој области, као и модалитете међудржавне сарадње и унапређење истраге и других сегмената значајних за гоњење и санкционисање. Решавање проблема из ове области тражи поштовање међународних обавеза, квалитетну координацију и прецизно одређену сарадњу.

У Републици Србији cyber криминал још увек није сагледан са свих аспеката, посебно када се у обзир узме шири контекст ове појаве. Велика тамна бројка извршених а непријављених кривичних дела у овој области, у потпуности је непозната државним органима.

Статистички подаци се ослањају на извештаје о спроведеним кривичним поступцима, саопштењима Министарства правде, суда, тужилаштва и полиције. На основу ових података видно је да су најчешће покретани поступци у Србији везани за овај вид криминала, у складу са Кривичним закоником: неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, прављење и уношење рачунарских вируса, рачунарска превара и рачунарска саботажа. Учиниоци су највише извршили дела преваре и неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података (88,09). Преваре су логичка последица општег стања - економске кризе, велике незапослености, тешке привредне ситуације, нестабилног политичког амбијента. Неовлашћени приступ (хакинг) је, између осталог, последица ранијег времена, такорећи рецидив периода до 2000. године, када је било веома много ових дела – најчешће из политичких и државних разлога (ангажовани државни хакери у време хакерског рата су чинили упаде из „патриотских" разлога, а такође и за време НАТО бомбардовања). „Хероји", а и они који су то желели да буду, наставили су ове активности, једино што то више није било некажњиво и славно. Ни остала два дела, иако мале заступљености, нису занемарљива. Последица су непажње, знатижеље, славе и „играња" са програмирањем (рачунарски вируси се праве и убацују и као претходница других дела, као пречица до новца, због психолошке залуђености, академских разлога, политичких разлога, некад је то из жеље да се учини зло, а понекад и да се учини добро[1] или из забаве)[2], али и из беса (рачунарске саботаже често настају због незадовољства, потиснуте агресивности и љутње)[3].

Поред ових кривичних дела која чине више од четвртине (27,1%) кривичних дела, почињена су и друга дела која су у вези са њима и то дела против: слободе и права човека (16,1%), интелектуалне својине (15,5%), полне слободе (32,3%), имовине (2,6%), уставног уређења (1,9%) и привреде (3,9%).

Истраживања која се баве овом проблематиком са ширег друштвеног аспекта (социолошког, психолошког, антрополошког, правног, политиколошког) још увек нису спроведена. Искуства из праксе указују да је потребно унапређивати професионалне компетенције стручњака, увести нове технологије и истражне криминалистичке методе које се морају применити у циљу превенције, регистровања и адекватног одговора и заштите критичних инфраструктура.

Високотехнолошки криминал све је присутнији и у области ирегулараних миграција и трговине људима. У Републици Србији недостаје комплексније разматрање проблема употребе информационо-комуникационих технологија од стране извршилаца кривичних дела у вези са илегалним миграцијама и трговином људима.

---

1 Нпр. вирус који тражи дечију порнографију је покушавао да заустави илегалне активности;

2 Hackers Write Computer Viruses (2009), http://gizmodo.com/5827405/why-hackers-write-computer-viruses; Carnahan P., Roberts D., Shay Z., Yeary J., (2005), The motivation behind computer viruses, http://vxheaven.org/lib/pdf/The%20motivation%20behind%20computer%20viruses.pdf;

3 KeeneyM. CappelliD. KowalskiE. MooreA. ShimeallT. (2005), InsiderThreatStudy: ComputerSystemSabotageinCriticalInfrastructureSectors, http://www.secretservice.gov/ntac/its_report_050516.pdf истичу да је најчешћи мотив, поготово саботера инсајдера: а) негативан однос према раду (92%); б) неуспешне жалбе и исправке грешака пре инцидента (85%); в) освета (84%). Већина се припремала за извршење дела;

Недостаци постојећег приступа у спречавању ових криминалних активности се могу изразити на следећи начин:

- не постоји довољна свест о раширености ових појава (ирегуларних миграција и трговине људима) и није довољно сагледана улога информационо-комуникационих технологија у њиховој експанзији;
- недостаје адекватан, функционални систем надгледања интернет сајтова и осталих облика комуникације који се користе за ирегуларне миграције и трговину људима;
- не постоји праћење „улоге“ друштвених мрежа у извршењу ових криминалних активности, као и довољно ефикасан систем реакције друштва на трговину људима која се одвија злоупотребом информационо-комуникационих технологија;
- недостаје свеобухватније сагледавање улоге криминалних група у ирегуларним миграцијама и трговини људима и повезаност ових група са злоупотребом информационо-комуникационих технологија.

Улога криминалних група у извршењу ових кривичних дела може бити кључна. Одређене облике ирегуларних миграција, као што је кријумчарење људима, немогуће је спровести без адекватне повезаности криминалних група више држава. Коришћење информационо-комуникациних технологија у комуникацији између чланова криминалних група, присутно је од самог почетка њихове појаве. У пракси је примећена експанзија коришћења интернета за рекламирање разних “легалних“ активности иза чега, заправо, стоји илегална миграција и трговина људима.

Република Србија се, почев од 2009. године, суочава са новим видом ирегуларне миграције – секундарном ирегулрном миграцијом држављана афро-азијског комплекса, преко држава Западног Балкана, са полазиштем из Грчке. Ирегуларни мигранти су већ ушли на територију Европске уније и након неког времена илегалног боравка и рада покушавају да иду даље ка богатијим земљама чланицама. Вишеструки тренд раста овог вида миграције проузрокован је прогресивним притиском ирегуларне миграције на грчко-турској граници, који је настављен и током 2012. године. У односу на 2011. годину када је у илегалном преласку државне границе спречено 10.383 лица, током 2012. године, спречено је 14.793 лица. Највећи број илегалних прелазака спречен је на граници са Републиком Македонијом (8.348), која је улазна тачка на територију Републике Србије. Ирегуларни мигранти транзитирају територијом Републике Србије у покушају да илегално пређу границу са Републиком Мађарском, Републиком Хрватском и Републиком Румунијом. Према могућностима даљег одласка имигранти остају извесно време и на територији Србије, илегално или злоупотребљавајући право на азил у прихватним центрима (Бања Ковиљача и Боговађа). Најзаступљенији у овој категорији ирегуларних миграната су држављани Авганистана, Пакистана и Сомалије, који користе све расположиве начине илегалног преласка државне границе, некад између граничних прелаза, а некад на самом граничном прелазу (првенствено скривањем у превозним средствима, али и употребом фалсификоване и туђе путне исправе).

Неретко злоупотребљавају право на азил и у последње време су врло добро организовани кроз мреже организованих криминалних група у државама порекла, транзита и дестинације илегалних миграната које немају строгу хијерархијску структуру, врло су флексибилне, међусобно сарађују преко интернета у складу са

фазама транспорта лица, стварајући посебне мреже на територији сваке државе, уз ангажовање локалног становништва. Када су илегалне миграције организоване од стране лица или организованих група у циљу стицања економске користи онда је то **кријумчарење људи.**

Ирегуларне миграције, поред **незаконитог преласка државне границе**, подразумевају и злоупотребе **у поступку поводом захтева за издавање визе** (подношење фалсификоване документације**), илегални боравак у некој земљи** (без обзира да ли се ушло легално, јер се онда илегално остаје након истека временског периода важења визе), **склапање фиктивних бракова и усвојења** у циљу избегавања строгих миграционих прописа о визама и боравцима и **илегални рад** у некој земљи (без дозволе надлежних органа, без обзира да ли је неко ушао легално и можда има дозволу боравка по основу школовања или студирања, али не и за рад).

Ирегуларне миграције, нарочито кријумчарење људи, често се поистовећује са трговином људима, што је супротно међународним правним правилима, јер се третман и поступање према лицима која су учествовала у ланцима кријумчарења људи разликује. Уколико се међу илегалним мигрантима, након обављеног разговора, пронађу жртве трговине људима онда су државе дужне да таквим лицима пруже заштиту (таква лица путују против своје воље или у заблуди да ће у земљи дестинације радити оно што им је обећано, али у стварности тим особама, које су заврбоване „лажним обећањима лепог живота“, организоване криминалне групе су намениле различите облике експлоатације, па тако жене најчешће заврше у проституцији, а мушкарци буду радно експлоатисани). По доласку у земљу одредишта жртве трговине људима се продају као било која друга роба.

Трговина људима је вишеслојан, комплексан и динамичан друштвени феномен који захтева свеобухватни (правни и друштвени) приступ. Жене, деца и мушкарци подвргавају се разноврсним облицима злостављања и искоришћавања, којима се повређују њихова основна људска права. Овај феномен, обухватајући фазе врбовања, транспорта и експлоатације жртава, у својим различитим облицима, дешава се на територији земаља порекла, транзита и крајњег одредишта и тада има свој транснационални карактер, али се може дешавати и унутар граница једне земље и тада је то, по свом појавном облику, национална трговина људима (јер се све фазе трговине људима одвијају унутар граница једне земље). Када је реч о транснационалној трговини људима појавни облици трговине људима и илегалних миграција су скоро истоветни (незаконито се прелази државна граница), али да би се утврдило о којој појави је реч морају се утврдити све чињенице, нарочито да ли је била намеравана експлоатација и све околности путовања, што је битно, јер се идентификованим жртвама трговине људима мора пружити помоћ и заштита.

Резултати статистичких и аналитичких података Министарства унутрашњих послова Републике Србије и Центра за заштиту жртава трговине људима и организација цивилног друштва у Србији последњих година препознају све форме трговине људима (сексуалну експлоатацију, принуду на просјачење, склапање принудног брака, радну експлоатацију, принуду ради вршења кривичних дела итд.) и указују на пораст броја малолетних жртава трговине људима и то домаћих држављана/ки, којима је трговано у оквиру граница Републике Србије, али од укидања виза се региструје и нови тренд транснационалне трговине људима - врбовање наших грађана за различите облике ескплоатације у земљама Европске уније.

Од стране Центра за заштиту жртава трговине људима, током 2013. године, идентификоване су укупно 92 жртве трговине људима, од којих је 16 потенцијалних жртава. Од укупног броја идентификованих жртава трговине људима 45 је маололетно. Најзаступљенија је сексуална експлоатација (31), затим радна експлоатација (22), па принуда на просјачење (11) и принудни брак (10), док је принуда на вршење кривичних дела заступљена у 2 случаја.

Полицијски службеници МУП-а Републике Србије поднели су, укупно, 36 кривичних пријава због сумње да је извршено кривично дело *трговина људима*, па је у овим случајевима откривено укупно 61 кривично дело *трговине људима*. Овим пријавама је обухваћено укупно 68 лица (трговци људима), од којих су 67 извршилаца држављани Републике Србије, а једно лице је без држављанства. У поднетим кривичним пријавама идентификована су 63 оштећена лица, од којих је 58 држављана Републике Србије. У 2013. години поднето је 30 кривичних пријава, а препознато је 45 оштећених жртава.

Ове области су, код нас, још увек недовољно истражене, те не постоје ни довољно добро дефинисане мере и механизми за њихово спречавање и сузбијање. Истраживање је отежано и великим бројем различитих теоријских приступа, услед чега је тешко обезбедити универзалност и ширу теоријску заснованост резултата истраживања.

2. ЦИЉ ИСТРАЖИВАЊА

Основни циљ истраживања је сагледавање постојећег стања високотехнолошког криминала и његових последица (идентификовање кривичних дела, њиховог обима, профила жртава, материјалне и нематеријалне штете), као и сагледавање „улоге“, односно заступљености информационо-комуникационих технологија и њихове злоупотребе у ирегуларним миграцијама и трговини људима.

Посебни циљеви су:

1. сагледати карактеристике информационе инфраструктуре у Републици Србији у односу на савремене информационо-комуникационе технологије, као и заступљене вештине и истражне криминалистичке методе које се користе, кроз годишње извештаје о високотехнолошком криминалу;
2. указати на врсте/облике, карактеристике и последице дела cyber криминала и сагледати стање у Републици Србији;
3. указати на отворена питања домаћих прописа у погледу високотехнолошког криминала и потребу њиховог унапређивања, анализом домаће и међународне регулативе, уз коришћење табела усаглашености националних нормативних аката са правним тековинама Еврпске уније;
4. сагледати повезаност појавних облика високотехнолошког криминала и других кривичних дела која се одвијају у електронском окружењу у вези са ирегуларним миграцијама и трговином људима, као и утицај друштвено-економских фактора у Србији на појаву и развој овог криминала;
5. сагледати капацитете, одговорност и спремност друштва, посебно државних органа за супротстављање високотехнолошком криминалу.

3. ХИПОТЕЗЕ

Истраживање је реализовано на основу пет општих хипотеза, у оквиру којих су развијене посебне хипотезе:

1. Коришћење информационо-комуникационих технологија у Републици Србији одговара трендовима у свету.

Посебне хипотезе су:

1.1. Најбројнији корисници рачунара, мобилних телефона и интернета су особе млађих генерација (до 30 година) и делом средње (од 30-45);
1.2. Рачунаре, мобилне телефоне и интернет више користе они из већих места;
1.3. Рачунаре, мобилне телефоне и интернет, кад су у питању средње и старије генерације, чешће користе високо образоване особе, док код млађих генерација нема велике разлике у односу на ниво образовања;
1.4. Припадници виших друштвених статуса у већој мери користе рачунаре него припадници нижих, без обзира на старост и ниво образовања;
1.5. Испитанице мање интензивно користе интернет од испитаника;
1.6. Већина испитаника млађих од 30 година оставља велики број података о својој личности на интернету и друштвеним мрежама;
1.7. Млађе генерације су се чешће физички срели са неким кога су упознале путем интернета него старије;
1.8. Испитанице су више од испитаника раније познавале све online пријатеље;
1.9. Деца између 6 и 10 година уопште не добијају он-лајн понуде;
1.10. Млађе генерације немају довољно знања о злоупотребама података о личности на интернету и друштвеним мрежама;
1.11. Испитаници свих категорија недовољно познају опасности везане за коришћење интернета, смарт мобилних телефона и друштвених мрежа;
1.12. Већина испитаника има индиферентан однос у вези са злоупотребама на интернету;
1.13. Мањи број испитаника је био жртва неког од облика високотехнолошког криминала;
1.14. Старија и средња генерација чешће користи друштвене мреже за личне потребе, успостављање контаката и комуникацију са пријатељима и родбином;
1.15. Млађе генерације примарно користе друштвене мреже ради забаве;
1.16. Мали број испитаника старије и средње генерације има позитиван став према малтретирању/злостављању путем друштвених мрежа;

1.17. Мали број испитаника није доживео малтретирање путем друштвених мрежа;
1.18. Велики број испитаника би пријавило „говор мржње“;
1.19. Велики број испитаника није имао преузимање идентитета на некој друштвеној мрежи;
1.20. Малом броју испитаника није нико злоупотребио платну картицу.

2. Cyber криминал у Републици Србији се разликује од трендова у свету.

Посебене хипотезе су:

2.1. Најчешћи облици и највећи број учинилаца се односе на дела рачунарске преваре и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (хакинг);
2.2. Карактеристике учинилаца у Републици Србији су сличне карактеристикама учинилаца cyber криминала у другим земљама;
2.3. У Републици Србији добро је проучен и дефинисан *modus operandi* учинилаца cyber криминала.

3. Високотехнолошки криминал на територији Републике Србије по броју и врсти кривичних дела, висини нанете штете (материјалне и/или нематеријалне) далеко је већи од оног који је регистрован од стране државних органа.

4. Капацитет надлежних органа да се супротставе овом виду криминалитета није адекватан броју и врсти извршених кривичних дела, као ни доступности средстава и уређаја који га омогућавају.

5. Информационо-комуникационе технологије својом експанзијом и све доступнијим сервисима погодују криминалним активностима у вези са ирегуларним миграцијама и трговином људима и злоупотребљавају се у све већем обиму у односу на раније злоупотребе ИКТ за исту сврху.

4. ОГРАНИЧЕЊА ИСТРАЖИВАЊА

Препозната ограничења истраживања везана су за природу појава које се испитују, као и за неке методолошке и формално-правне аспекте истраживања.

Високотехнолошки криминал и ирегуларне миграције, као и трговина људима која се одвија уз (зло)употребу информационо- комуникационих технологија, веома су тешки облици криминалитета за откривање. Веома је велика тамна бројка ових кривичних дела, а извршиоци лако крију трагове свог извршења. Понекад нпр. високотехнолошки криминал оставља веома мале последице тако да прође неопажено од стране жртава које и не сматрају да то треба пријавити да је дошло до извршења кривичног дела. Често се иза различитих огласа за послове на интернету крију извршиоци кривичних дела *трговине људима* иако, на први поглед, ти огласи

нису нешто што би само по себи било проблематично. Жртве трговине људима, у истраживачком смислу, представљају скривени узорак, чије је истраживање , а још више закључивање изузетно захтевно. Такође се ради о малим узорцима, који онемогућавају доношење генерализованих релевантних закључака. Стога је интерпретација добијених података усмерена на експлорацију постојећег стања, са предикцијама усмереним на потребне акције у односу на садашња обележја, не на предвиђање развоја саме појаве.

Ограничавајући фактор је и сама природа анкетног истраживања, имајући у виду обележја саме анкетне методе. Имајући у виду да је анкету тешко прилагодити свим испитаницима (једној групи анкета може бити лака, другој тешка), могући су друштвено позитивни одговори, као и тешкоће које настају због различитог образовања и писмености испитаника, начина израде анкетног упитника, комбинација отворених и затворених питања, коришћење упитника као основе за анкетни интервју. Добра стратификација узорка и обука анкетара за примену анкете, допринели су смањењу ових ризика.

Још један ограничавајући фактор истраживања су обележја ирегуларних мигранта, који немају лична докумената, па је тешко је проценити узраст, језичке препреке, када су у питању страни држављани, њихова мотивисаност да учествују у истраживању овог типа и слично. Примена анкете у форми анкетног интервјуа је смањила ове ризике у реалане, разумне границе.

Истраживање је предвидело учешће малолетних лица, што је посебно ризичан фактор са аспекта испуњења формално правних захтева за њихово учешће. У том циљу обезбеђено је добијање сагласности родитеља за учешће деце у истраживању, а у сарадњи са матичним школама. Такође, консултован је и заштитиник грађана у циљу верификације питања садржаних у анкети са аспекта заштите података о личности и како би се заштитила права, како малолетних лица тако и свих лица која су анкетирана. Анкетирање ученика и студената обављено је у школским институцијама и уз сагласност Министарства просвете и Савета родитеља у основним школама.

Још једно ограничење односи се на тешкоће у етичком и практичном смислу у реализацији истраживања, у групи жртава трговине људима. Због осетљивости њиховог статуса, менталног стања и тренутних практичних могућности за разумевање и учешће у анкети, постоји ризик од секундарне трауматизације жртава. Да би се ово избегло, прибегло се реализацији анкетног интервјуа који су спроводили стручњаци Центра за заштиту жртава трговине људима, који су испитаницама блиски, познати и чије је учешће омогућавало безбедно окружење за жртву, као и процену, непосредно пре или током интервјуа, да ли ће настала ситуација узнемирити или већ узнемирава жртву. Познавање жртве и њене историје омогућило је стручњацима Центра постављање питања у форми која је најпримеренија конкретној жртви, што је такође допринело квалитету добијених података.

Кодирање податка ради обезбеђење анонимности испитаника и статистичке обраде, захтевало је посебне припреме које су реализоване, као и декодирање за потребе обраде и интерпретације резултата.

5. МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

Истраживање је реализовано као неекспериментално експлоративно и дескриптивно истраживање, у складу са постављеним општим циљем истраживања, анкетног типа. Активности истраживања су реализоване на терену, осим активности које су обухватале анализу материјала и оних које су обављене у канцеларијским условима. Основне методе истраживања су:

1. анкета,
2. анкета са личним интервјуисањем,
3. елктронска анкета,
4. *desk* анализа и анализа садржаја.

Анкетно истраживање се, по правилу, реализује структурисаним упитником или интервјуом. С обзиром на то да је у анкетним истраживањима неопходно да се интервју води на основу структуираног упитника, то су мерни инструменти, који су наменски сачињени за остваривање сврхе истраживања, креирани на начин да се могу користити и као анкета, коју испитаник сам попуњава и као основ за структурисани интервју који обавља обучено лице. У наредним поглављима биће више речи о мерним инструментима.

С обзиром на сложеност испитиваних појава, истраживање је реализовано у више сегмената, који су организовани тако да омогуће тестирање постављених хипотеза. *Први сегмент односи се на коришћење информационо-комуникационих технологија, други на кривичноправни аспект cyber криминала и трећи на област коришћења информационо-комуникационих технологија у трговини људима, кријумчарењу људи и у иregуларним миграцијама*. Оваква организација истраживања омогућила је разумевање кључних варијабли истраживања, а потом и њихово међусобно повезивање и предикцију потребних мера за унапређење супротстављања cyber криминалу, односно коришћењу високо комуникационих технологија у криминалне сврхе. Према плану истраживања, етапе реализације истраживања су:

- припрема пројекта истраживања;
- припрема потребних инструмената и прикупљање литературе;
- спровођење истраживања применом планираних мерних инструмената;
- завршна анализа, презентовање резултата и
- израда финалног извештаја о резултатима истраживања.

Након непосредног теренског рада на истраживању, подаци добијени применом мерних инструмената обрађени су применом статистичких метода. С обзиром на сложеност и обим истраживања осмишљен је начин уноса и дефинисана је организација уноса података. Унос података обављен је од стране Управе криминалистичке полиције, Управе граничне полиције, Управе за аналитику, Управе за информационе технологије, у оквиру Министарства унутрашњих послова, као и Факултета организационих наука и Криминалистичко-полицијске академије. Примарна обрада попуњених упитника обављена је од стране службеника Управе за информационе технологије и Управе за аналитику Сектора за аналитику, телекомуникационе и информационе технологије Министарства унутрашњих послова.

Подаци су обрађени у програмима *Microsoft Office Excel* и *Statistical Package for the Social Sciences (SPSS).* Након обраде, подаци су дистрибуирани проблемски оријентисаним истраживачким тимовима који су анализирали добијене податке, као и литературу која је обухватала домаће и међународне прописе и постојеће извештаје и статистике у Републици Србији (дати у прилогу монографије) и сачинили прве предлоге извештаја. На основу примарне обраде података, презентовани су резултати радом у пленуму, а тимским радом су одређени правци даљих анализа и укрштених прегледа. Дискусија је вођена након сваког сумарног прегледа остварених резултата, са циљем обједињавања резултата и доношења јасних и концизних закључака истраживања, који су верификовани од старне свих учесника истраживања. Анализа садржаја и резултата укрштених прегледа је обављена уз уважавање свих предложених праваца анализе.

Током припреме пројекта истраживања дефинисани су извори података, избор и обука испитивача/анкетара и дефинисани су временски рокови за реализацију истраживања, као и поступак обраде података и обједињавања резултата истраживања.

Теренско истраживање, које се односило на спровођење анкете у општој популацији, реализовали су претежно студенти Факултета организационих наука и Криминалистичко-полицијске академије. Када су у питању посебне категорије испитаника њих су интервјуисали сами истраживачи, а узорак жртава трговине људима интервјуисали су стручњаци Центра за заштиту жртава трговине људима. Студенти који су реализовали анкету обучени су за примену мерних инструмената коришћених у истраживању.

5.1. Извори података

Извори података су попуњени мерни инструменти, одабрана литература и документација. Мерне инструменте су креирали ангажовани експерти за реализацију истраживања и они су приказани у делу о мерним инструментима. Одабрану литературу чинила је:

- научна литература и
- стручна литература.

Анализирани су следећи документи:

- међународни правни акти;
- национални правни акти;
- међународни и национални судски случајеви;
- архиве различитих институција;
- статистички извештаји;
- релевантна документа надлежних институција и организација;
- садржаји медија (штампа, телевизија, интернет) и
- експертизе из наведених области.

Сва коришћена литература дата је у посебном поглављу.

5.2. Узорак

С обзиром на сложеност појаве, а имајући у виду хипотезе које су тестиране, било је захтевно дефинисати узорак који треба да репрезентује популацију како би добијени подаци били релевантни. Узорак је пре свега намерни, док је у једној групи (жртве трговине људима) био и пригодан. Структура узорка одређена је појединачним циљевима истраживања и дефинисаним варијаблама које су оцењене као релевантне за тестирање хипотеза истраживања. Узорак је репрезентативан за области испитивања.

За истраживање коришћења информационо-комуникационих технологија и свести о облицима и размерама високотехнолошког криминала, кроз процену ставова грађана Републике Србије, узорак су чинили ученици, студенти, запослена и незапослена лица, случајни пролазници, послодавци и представници других друштвених група.

Капацитети система за сузбијање високотехнолошког криминала тестирани су на узорку припадника надлежних органа државне управе, институција и организација. Узорак су чинили представници: полиције, царине, провајдера интернет услуга, великих финансијских, телекомуникационих, пословних и других система, невладиних организација и других релевантних институција.

Повезаност информационо-комуникационих технологија са илегалним миграцијама и трговином људима испитивана је на узорку који чине: представници релевантних државних органа (полиција, тужилаштво, центри за социјални рад, Центар за заштиту жртава трговине људима, Комесаријат за избеглице и други), представници удружења грађана, Црвеног крста и међународних организација, ирегуларни мигранти, жртве трговине људима, тражиоци азила и запослени у туриситичким агенцијама.

У циљу избегавања секундарне виктимизације информације које поседују жртве трговине људима и друге заштићене категорије (нпр. малолетна лица), а које су релевантне за истраживање, прикупљене су у сарадњи са Центром за заштиту жртава трговине људима и другим надлежним социјалним установама.

Основна обележја узорка:

- **узорачки оквир:** Република Србија (без Косова и Метохије);
- **популација:** држављани Републике Србије (без Косова и Метохије) и страни држављани (у вези са ирегуларним миграцијама и трговином људима);
- **јединица посматрања:** испитаник;
- **јединица узорковања:** испитаник.

Опис узорка дат је у односу на три сегмента истраживања.

Први сегмент - Истраживање коришћења информационо-комуникационих технологија у Републици Србији

Узорак је чинио 2059 испитаника оба пола, различитих старосних група, државе рођења, националности, величине места пребивалишта, брачног, стамбеног и радног статуса, степена и области образовања и запослења. Ове карактеристике значајне су за сагледавање понашања испитаника на интернету и разумевање

различитих облика високотехнолошког криминала. Анкетирање је обављено у основним школама (свих разреда) и средњим школама (стручним и гимназијама), као и на факултетима. Одређен број испитаника су били случајни пролазници у разним местима у Републици Србији у којима се истраживање спроводило. Истраживањем су обухваћени испитаници из: Сомбора, Вршца, Зрењанина, Новог Сада, Сремске Митровице, Сремских Карловаца, Инђије, Ковина, Београда, Младеновца, Гроцке, Краљева, Крагујевца, Ниша, Врања, Пирота, Ариља, Гуче и Новог Пазара.

У дефинисању узорка водило се рачуна да социодемографска структура буде пропорционална у односу на сваки критеријум. Узорак је био свеобухватан по свим критеријумима. По неким критеријумима није био репрезентативан за популацију, али је био паритетан и структура узорка је одговарала структури корисника интернета, како би се обезбедила адекватна анализа коришћења рачунара, мобилних телефона, интернета и друштвених мрежа.

Планом истраживања предвиђено је да истраживање обухвати 2380 испитаника, и то:

- основне школе – 560 ученика; из нижих разреда (од I до IV) по 2 ученика из сваког разреда, а из виши (од V до VIII) по 5 ученика, из 20 школа, из различитих места по броју становника и степену урбанизације (са територије Београда, мањих градова и руралних крајева);
- средње школе – 400 ученика из 20 школа (10 из гимназија, 5 из техничких школа и 5 из других стручних школа);
- факултети и школе струковних студија – 700 студената са 14 универзитета (9 државних и 5 приватних);
- случајан узорак - 720 лица (стратификованих према полу, старости, статусу и месту боравка).

У реализованом узорку број испитаника је мањи за 321 (13 % од планираног узорка).

Табела 1. Опис узорка са основним социодемографским карактеристикама

Критеријум	*Опис узорка*	*Фреквенција*
Пол	мушки	50,46
	женски	49,00
Старост	од 6 – мање од 10	4,52
	од 10 – мање од 14	10,05
	од 14 – мање од 16	5,29
	од 16 – мање од 18	10,64
	од 18 – мање од 30	52,40
	од 30 – мање од 45	7,72
	од 45 – мање од 60	6,80
	преко 60	2,23
Држава рођења	СФРЈ/СРЈ/РС	92,95
	друга	3,45
	не знам/не желим да одговорим	2,33

Критеријум	*Опис узорка*	*Фреквенција*
Националност	српска	90,42
	не знам/не желим да одговорим	3,89
	друга	4,23
Величина места пребивалишта	до 5 000 становника	6,66
	5 000 до 20 000 становника	8,31
	20 000 до 100 000 становника	10,99
	100 000 до 500 000 становника	33,20
	преко 500 000 становника	36,36
Брачни статус	неожењен/неудата	67,04
	ожењен/удата	12,15
	разведен/разведена	2,43
	удовац/удовица	2,09
Стамбени статус	у стану/кући	75.74
	у изнајмљеном стану	13,96
	у ученичком/студентском/другом дому	7,68
	у кампу за азиланте/имигранте	0,39
	у привременом боравишту који ми је обезбедила Влада Србије	0,29
Образовање	без школе	8,5
	основно	15,6
	средње	49,2
	више	6,4
	високо	13,5
Област образовања	опште	29,4
	друштвено-хуманистичка	18,0
	медицинско-биолошка	7,4
	природно-математичка	9,5
	техничко-технолошка	19,5
	уметност	1,7
	остало	6,32
Радни статус	запослен/а	16,48
	незапослен/а	51,2
	привремено запослен/а	2,3
	повремено запослен/а	1,9
	пензионер	2,4
Економски статус	веома добар	4,3
	добар	24,5
	осредњи	30,1
	лош	9,0
	веома лош	2,2

Други сегмент - Кривичноправни аспект cyber криминала

Узорак у овом сегменту истраживања чинило је 64 испитаника одабраних према припадности одређеном систему, односно организацији која је релевантна за тестирање хипотезе.

Табела 2. Приказ дистрибуције узорка у односу на релевантне организације

Установа/организација	*Број јединица*
МУП – Управа граничне полиције, МУП–СБПОК, Одељење за борбу против високотехнолошког криминала, Више јавно тужилаштво Одељење за борбу против високотехнолошког криминала, судије Вишег суда	48
Интернет сервис провјадери	5
Удружење картичара, односно банкара	11
Укупно	**64**

Узорак који је обухватио испитанике из МУП-а, Вишег јавног тужилаштва и Вишег суда чини 48 испитаника оба пола, различитих старосних доби, занимања, економског статуса и друго. У одабиру узорка се водило рачуна да буде довољан број испитаника, али се водило рачуна и о томе да расподела испитаника не буде крајње диспропорцијална по полу и другим критеријумима. Упућеност и познавање материје о ВТК и ирегуларним миграцијама и трговини људима није неопходно образлагати. Узорак је према свим анализама свеобухватан по свим критеријумима.

У одабиру узорка интернет сервис провајдера водило се рачуна да буде довољан број испитаника. Узорак чине представници 5 привредних друштава која се баве пружањем услуга интернета. Узорак је према свим анализама свеобухватан по свим критеријумима. По многим критеријумима он јесте репрезентативан за популацију.

У одабиру узорка удружења картичара водило се рачуна да буде довољан број испитаника. Узорак су чинили представници привредних друштава који се баве пружањем финансијских и банкарских услуга.

Трећи сегмент - Коришћење информационо- комуникационих технологија у трговини људима, у кријумчарењу људи и у ирегуларним миграцијама

У овом сегменту узорак је, због већег броја различитих релевантних актера за тестирање хипотезе, дефинисан према релевантној појави на коју се односи.Те појаве су: трговима људима, ирегуларнре миграције и кријумчарење људи.

Трговина људима

Подгрупе узорка: жртве трговине људима, запослени који обезбеђују подршку и полицијски службеници МУП-а Републике Србије.

Узорак: жртве трговине људима

Узорак је пригодан. Обухвата све жртве трговине људима које су идентификоване у 2012. и 2013. години, а са којима је било могуће успоставити контакт. Жртве трговине људима су интервјуисане у укупно 18 места у Републици Србији: у Београду, Новом Саду, Смедереву, Алексинцу, Сомбору, Лесковцу, Бечеју, Крагујевцу, Краљеву, Панчеву, Бољевцу, Инђији, Крушевцу, Лазаревцу, Нишу, Сремској Митровици, Старој Пазови и Тителу. Највећи број жртава интервјуисан је у Београду (14), Новом Саду (6) и Смедереву (5).

Узорак: запослени који обезбеђују подршку

Овај узорак чине запослени у државним органима и невладиним организацијама који раде са жртвама трговине људима, односно који се у оквиру свог редовног запослења баве пружањем помоћи, подршке и заштите овој категорији жртава, али и откривањем учинилаца тог кривичног дела. Укупно 5 испитаника интервјуисано је у Панчеву, 5 у Београду, 3 у Прокупљу, 3 у Зрењанину, 3 у Нишу, 2 у Крагујевцу, док је по 1 испитаник интервјуисан у Новом Пазару, Лесковцу, Врању, Димитровграду, Јагодини, Кикинди, Краљеву, Ужицу, Ваљеву, Сомбору, Крушевцу, Долову, Новом Саду, Пироту и Сремској Митровици. Од укупног броја испитаника њих 33 су запослени у владином сектору, 2 испитаника су запослена у невладионом сектору, а 3 испитаника нису унели податке о сектору где су запослени. Од 40 испитаника, 3 раде за Министарство унутрашњих послова Републике Србије, у полицијским управама ради 24 испитаника и то 5 у Панчеву, 3 у Прокупљу, 3 у Зрењанину и по 1 у Крагујевцу, Сремској Митровици, Лесковцу Врању, Нишу, Јагодини, Прокупљу, Кикинди, Краљеву, Ужицу, Сомбору, Крушевцу, Пироту и Новом Саду. За 2 испитаника није унет податак о организацији у којој ради.

Узорак: полицијски службеници Министарства унутрашњих послова Србије који су поступали у предметима трговине људима

Узорак чине представници из четрнаест подручних полицијских управа. Упитник је попунио 31 полицијски службеник. Из полицијске управе (ПУ) Зрењанин упитнике је попунило 9 полицијских службеника, из ПУ Панчево 6, из ПУ Прокупље и Краљево по 3, из ПУ за град Београд 2, а по 1 из ПУ Нови Пазар, ПУ Кикинда, ПУ Сомбор, ПУ Ужице, ПУ Ваљево, ПУ Ниш, ПУ Сремска Митровица, ПУ Врање и ПУ Нови Сад. Упитник је попунио и 1 полицијски службеник са граничног прелаза Хоргош. Податке о организационој јединици нису унела 2 полицијска службеника која су попунила упитник.

Попуњавање упитника подразумевало је искуство полицијских службеника на пословима спречавања и сузбијања кривичног дела трговине људима. Гледано кроз призму линијске службе којој припадају, 24 (77,42%) анкетирана полицијска службеника су навела да обављају послове из делокруга рада одељења пограничне полиције (ОПП), 5 (16,13%) да су полицијски службеници ангажовани у оквиру Одељења за странце (ОЗС), 2 (6,45%) да су полицијски службеници Управе за странце (УЗС). Прецизније одређење линијске службе нису навела 3 (8,57%) анкетирана полицијска службеника (из ПУ Краљево), а 1 (2,86%) упитник није садржао одговор на ово питање.

Ирегуларне миграције

Узорак: тражиоци азила и ирегуларни мигранти

За потребе овог истраживања обављена су 53 интервјуа са тражиоцима азила у Центру за азил у Бањи Ковиљачи и 45 интервјуа са ирегуларним мигрантима. Категорија ирегуларних миграната обухватила је повратнике на основу Споразума о реадмисији, лица ухапшена приликом илегалног преласка границе, контроле саобраћајница, преноћишта, аутобуских и железничких станица, лица са фалсификованим документима, лица у Центру за смештај малолетних страних држављана без родитељске или старатељске пратње при Заводу за образовање деце и омладине "Васа Стајић" у Београду, лица у Прихватилишту за странце у Падинској Скели у Београду и лица у поступку азила која још нису смештена у центре за азиланте.

Узорак: запослени у државним установама и невладиним организацијама који раде са овом популацијом

Обухваћена су 92 лица.

Узорак: запослени у туристичким агенцијама

Истраживањем је обухваћено шест туристичких агенција, чланица Националне асоцијације туристичких агенција Србије - YUTA.

Кријумчарење људи

Узорак: полицијски службеници

Узорак обухвата 88 полицијских службеника, и то из: Регионалног центра граничне полиције према (РЦГП) Црној Гори 27 (30,68%), Полицијске управе (ПУ) Ужице 11 (12,5%), ПУ Панчево и РЦГП према Мађарској по 5 (по 5,68%), из РЦГП према Румунији 4 (4.55%), ПУ Прокупље и РЦГП према Хрватској по 3 (по 3,41%), ПУ Пожаревац и Станице граничне полиције (СГП) Аеродром Ниш по 2 (2,27%) и по 1 (1,14%) из ПУ Чачак, ПУ Јагодина, ПУ Кикинда, ПУ Крагујевац, ПУ Краљево, ПУ Крушевац, ПУ Лесковац, ПУ Ниш, ПУ Нови Сад, ПУ Пирот, ПУ Смедерево, ПУ Сомбор, ПУ Сремска Митровица, ПУ Шабац, ПУ Ваљево, ПУ Врање, ПУ Зрењанин, РЦГП према Бугарској и РЦГП према Македонији.

Гледано кроз призму линијске службе којој припадају, од 88 анкетираних полицијских службеника, њих 41 (46,59%) навело је да обављају послове из делокруга рада РЦГП, 12 (13,64%) је навело да обавља послове из делокруга рада одељења пограничне полиције (5 из ПУ Панчево, 4 из ПУ Ужице и по 1 из ПУ Сомбор, ПУ Врање и ПУ Нови Сад), 9 (10,23%) да су полицијски службеници криминалистичке полиције (2 из ПУ Пожаревац и 7 из ПУ Ужице), 2 (2,27%) да су ангажовани на граничном прелазу Аеродром. Којој нижој организационој јединицу у оквиру ПУ припада није навело 17 (19,32%) анкетираних полицијских службеника из 15 ПУ (3 из ПУ Прокупље и по 1 из ПУ Чачак, ПУ Јагодина, ПУ Кикинда, ПУ Крагујевац, ПУ Краљево, ПУ Лесковац, ПУ Ниш, ПУ Пирот, ПУ Сремска Митровица, ПУ Шабац, ПУ Смедерево, ПУ Зрењанин и ПУ Ваљево, као и 7 (7,95%) полицијских службеника који су навели само то да су припадници МУП-а РС без било каквог ближег означавања ниже организационе јединице.

5.3. Мерни инструменти

Мерни инструменти коришћени у истраживању наменски су конструисани у складу са сврхом и циљевима истраживања.

Сет мерних инструмената обухвата упитнике за спровођење анкете или анкетног интервјуа који чине батерију упитника истраживања:

1. упитник *„Анкета за високотехнолошки криминал“* – намењен је реализацији анкете у области коришћења информационо-комуникационих технологија. Упитник, поред основних демографских података, садржи и три групе питања: прва се односи на податке о личности и њихово он-лајн остављање, на начин остављања, недостатке свести о опасностима од неконтролисаног остављања, на могуће злоупотребе података о личности и ставове испитаника о особама које користе мобилни телефон/рачунар у недозвољене сврхе. Следећа група питања везана је за поједине облике високотехнолошког криминала и мишљења и ставове испитаника о знањима неопходним за њихово чињење. Испитивало се и да ли су испитаници били жртве тих криминалних понашања и да ли би то пријавили и коме. Трећа група питања је везана за друштвене мреже, проблеме и контакте које су успостављали и негативна искуства;
2. упитник *„Интервју за припаднике државног/цивилног сектора у вези ирегуларних миграната“* – намењен је испитивању државних службеника и представника организација цивилног друштва који раде са ирегуларним мигрантима;
3. упитник *„Интервју за припаднике државног/цивилног сектора у вези кријумчара људима“* – намењен је испитивању државних службеника и организације цивилног друштва (ОЦД) које раде у области кријумчарења људи;
4. упитник *„Интервју у вези са извршиоцима кривичног дела трговина људима“* - намењен је испитивању службеника полиције који раде на кривичном делу *трговине људима*. Испитивање је реализовано у форми рачунарски подржане анкете;
5. упитник *„Жртве трговине људима - интервју за припаднике владиних и невладиних организација“*; реализован је у форми структуираног интервјуа;
6. упитник *„Анкета за припаднике одељења за борбу против ВТК СБПОК, УКП, МУП РС и УГП, Тужилаштво и Суд“* – намењен је испитивању државних службеника које раде у области високотехнолошког криминала;
7. упитник *„ИСП провајдери“* – намењен је испитивању интернет провајдера;
8. упитник *„Друштво картичара“* – намењен је испитивању представника банака;
9. упитник *„Интервју за YUTA чланице“* – намењен је испитивању представника туристичких организација;
10. упитник *„Транспортери“* - намењен је испитивању шпедитера;
11. упитник *„Жртве трговине људима“* – намењен је испитивању жртава трговине људима и релаизован је као структуирани интервју;

12. упитник *„Интервју за мигранте“* – намењен је испитивању иregуларних миграната и реализован је у форми структуираног интервјуа;
13. упитник *„Интервју за азиланте“* – намењен испитивању тражиоца азила и реализован је у форми структуираног интервјуа.

Сви мерни инструменти дати су у прилогу монографије.

5.4. Поступак

Анкета је рађена на основу упитника „Анкета за високотехнолошки криминал“ и „Анкета за припаднике одељења за борбу против ВТК СБПОК, УКП, МУП РС и УГП, Тужилаштво и Суд“. „Анкета за високотехнолошки криминал“ рађена је на тај начин што су упитници попуњавани од стране испитаника у директном контаку са анкетарима, док су анкете за припаднике Одељења за борбу против ВТК СБПОК, УКП, МУП РС и УГП, тужилаштво и суд достављане службеном поштом како би их попунили службеници који се баве наведеном проблематиком у поменутим институција.

Анкетни интервју је рађен на основу упитника „Жртве трговине људима“, „Интервју за мигранте“, „Интервју за азиланте“ и „Жртве трговине људима - интервју за припаднике владиних и невладиних организација“ и то у директном контакту анкетара са испитаницима. Анкетни интервју са жртвама трговине људима реализован је од стране стручних радника Центра за заштиту жртава трговине људима, који су већ у контакту са жртвама и имају са њима развијен однос поверења, што је омогућило обављање интервјуа у сигурној атмосфери по жртву.

Нека питања из анкетног упитника, која се нису директно односила на коришћење ВТК у врбовању и експлоатацији, а за која су већ постојали подаци у досијеима испитаника, попуњена су на основу постојеће евиденције, па је цео поступак био организован тако да максимално смањи могућност секундарне виктимизације. Интервјуи су обављени са свим жртвама које су идентификоване током 2012. и 2013. године, а које су у моменту реализације истраживања биле доступне за успостављање контакта ради договора око обављања интервјуа. Током интервјуа није било непријатних ситуација по испитанике.

Електронска анкета је рађена на основу упитника „Интервју у вези са извршиоцима кривичног дела *трговина људима*“, „Интервју за припаднике државног/цивилног сектора у вези кријумчара људима“, као и упитника „ИСП провајдери“, „Друштво картичара“, „Интервју за YUTA чланице“ и „Транспортери“ који су достављени Привредној комори Србије путем електронске поште.

Проф. др Слободан Миладиновић
Универзитет у Београду, Факултет организационих наука

ИНФОРМАЦИОНО-КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ У ФУНКЦИЈИ СТВАРАЊА СОЦИЈАЛНОГ КАПИТАЛА

Садржај

Табеле

Графици

1. УВОД

Ми данас већ уобичајено сагледавамо интернет кроз све већу присутност друштвених мрежа у свакодневном животу људи. Истраживачи су закључили да је растућа популарност *веб-* сајтова, који се називају друштвеним мрежама, за разлику од интернета и *Web*а у целини, који су засновани на садржају, базирана на њиховој специфичности коју чине корисници и успостављању сталне интеракције међу њима. Ту се акценат ставља на заједницу која се формира на бази заједничких интересовања. Суштину такве заједнице чини олакшано отварање канала за слање и размену информација, па чак и олакшано везивање емоција за садржај порука[4]. За разлику од ранијег периода када је интернет омогућавао једносмерну испоруку информација ка кориснику, сада корисници креирају садржаји и одређују путање којима се крећу информације. Корисници више не преузимају информације већ их креирају, деле, размењују, они више нису потрошачи већ ствараоци садржаја на интернету[5].

Сигурно је да овако конципиран интернет има и позитивне и негативне стране. У литератури не постоји општа сагласност око тога да ли интернет разара или учвршћује друштвени живот својих корисника. Да би се добио ваљан одговор на ово питање, требало би имати увид пре у психолошки профил његових корисника него у структуру реалних друштвених односа, који се остварују посредством или поводом интернета. Истраживања указују на то да је комуникација преко интернета привлачна интровертним, стидљивим и друштвено анксиозним појединцима који посредством друштвених мрежа на интернету остварују (социјалну) компензацију незадовољавајуће социјалне комуникације у реалном животу, па чак и превазилазе проблеме које имају у комуникацији са другима[6]. С друге стране постоје мишљења да такве особе чине супституцију реалне комуникације виртуелном[7] која може да доведе до бихејвиоралне зависности од интернета[8].

Но, без обзира на то, употреба информационих- технологија у Србији је данас веома распрострањена, мада њихова експанзија и развој још увек трају. Оне су продрле у скоро све сфере наших живота и без њих се не може замислити нормално функционисање људског друштва. Рачунари су променили начин прикупљања, чувања, обраде и презентовања информација, а појава интернета омогућила је приступ невероватно великој количини информација и комуникацију широм света. Бројне су предности оваквог начина комуницирања и дељења

4 Mislove, A. Marcon, M. Gummadi, K. P. Druschel, P. Bhattacharjee, B.: (2007). Measurement and analysis of online social networks. Internet Measurement Conference 2007, October 24-26, 2007. San Diego, CA, USA. http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf (10.3.2014);

5 Selwyn, N (2012): 'Social Media in Higher Education', The Europa World of Learning. http://www.educationarena.com/pdf/sample/sample-essay-selwyn.pdf (10.3.2014);

6 Jochen, P. Valkenburg, P. M. & Schouten, A. P. (2005). Developing a model of adolescent friendship formation on the Internet. CyberPsychology and Behavior, 8, 423-430;

7 Caplan, S. (2007). Relations among loneliness, social anxiety and problematic Internet use. CyberPsychology & Behavior, 10, 234– 242.; Chak, K. & Leung, L. (2004). Shyness and locus of control as predictors of Internet addiction and Internet use. CyberPsihology and Behavior, 7, 559– 570;

8 Widyanto, L. & McMurran, M. (2004). The psychometric properties of the Internet addiction test. CyberPsychology & Behavior, 7, 443-450;

најразноврснијих података и информација и интернет је у том смислу значајно унапредио животе људи.

2. ДРУШТВЕНЕ МРЕЖЕ НА ИНТЕРНЕТУ

Тешко да се може оспорити теза да су друштвене мреже на интернету данас најједноставнији начин комуникације и личног представљања. Томе је допринео развој информационо-комуникационих технологија, а на првом месту преносивих рачунара и мобилних телефона, који су у иоле развијенијим деловима света већ постали део стандардне опреме већине појединаца и њихових домаћинстава. Ове технологије су убрзале интерперсоналне комуникације и ширење информација. И не само то, изашле су из сфере приватности и постале саставни део јавног живота увелико обликујући не само наше личне животе, већ и велике светске догађаје[9].

Друштвене мреже у реалном свету су веома стари феномен. Људи су од најраније историје имали природну потребу да се повезују са другима, било да би обезбедили снабдевање или се заштитили од дивљих звери, односно конкурентских друштвених заједница или из неког другог разлога. У том смислу под првим друштвеним мрежама можемо подразумевати примордијалне облике повезивања као што су проширене породице или локалне заједнице из најдавнијих времена људске историје. Социјална антропологија је забележила бројне примере обреда иницијације којима се појединци укључују нпр. у свет одраслих или постају ратници и слично. Обредом иницијације се улази у један нови свет, свет посвећених и повлашћених, у свет оних који су повезани у посебну мрежу одабраних[10].

У античком периоду се појављују прве озбиљније друштвене мреже које на интересној основи повезују различите појединце и породице (нпр. путем припадања племству или трговачког повезивања). Даљи ток историје ове мреже само чини бројнијим и комплекснијим (разни видови трговачких или занатлијских удружења, систем аристократских титула кроз средњи век итд.). Кроз читаву историју је њихова трајна карактеристика било одржавање, учвршћивање и ширење постојећег круга пријатеља и познаника. Овим се преко постојећих карика у ланцу пријатеља ступа у везу са другим појединцима и мрежама и постепено гради велика заједница умрежених пријатеља и познаника.

У блиској вези са појмом друштвених мрежа је и појам друштвеног умрежавања. Док мрежа подразумева систем веза и познанстава, дотле умреженост подразумева иницирање и покретање друштвених односа између особа које се, у принципу, не познају, а које налазе заједнички интерес у међусобном повезивању.

---

9 Милошевић, Б. (2013): Социјалне мреже и Арапско пролеће, СМ: Communication Management Quarterly: Часопис за управљање комуницирањем 27 (VIII), стр. 91–108.; Врањеш, А. (2013): Однос друштвених мрежа и грађанске партиципације на примјеру "арапског пољећа", Политеиа, vol. III, (5), str.111-119. Boyd, D. (2008). Can social network sites enable political action? International Journal of Media and Cultural Politics, 4(2), 241–244. Wilson, C. Dunn, A. (2011), Digital Media in the Egyptian Revolution: Descriptive Analysis from the Tahrir Data Sets: International Journal of Communication 5, pp. 1248–1272. Eltantawy, N. Wiest, J. B. (2011), Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory, International Journal of Communication 5, pp. 1207–1224;

10 Фрејзер, Џ. Џ. (1992), Златна грана: проучавање магије и религије, Бигз, Београд; Brain, J.L. (1977). Sex, Incest, and Death: Initiation Rites Reconsidered, CurrentAnthropology, vol. 18, no. 2. pp. 191-208;

Динамика савременог тренутка је толико бурна да је, очигледно с разлогом, привукла пажњу великог броја аутора[11]. У овој динамици велике промене су стигле и у оквире друштвене структуре, али и у оквире структуре људских комуникација. Технолошке промене су утицале да се формулише идеја да је свет састављен од мрежа, а не од група[12]. М. Кастелс[13] примећује да се традиционално вертикално-хијерархијско схватање друштвене структуре, карактеристично за друштва индустријског начин производње, мора ревидирати и заменити мрежним схватањем друштвене структуре, које одликује хоризонталност и плуралистична хијерархичност и које више одговара модерном информационом друштву. За њега су мреже саморекомбинујуће структуре комуникације које омогућавају јединство циљева и флексибилност својих активности кроз способност адаптирања окружења у којем делују.

Мрежни приступ анализе друштвених односа добија пуни смисао тек са развојем савремених информационо - комуникационих технологија[14] јер тек тада мрежа добија пуну способност увођења нових актера и садржаја у процес друштвене организације, чиме рапидно увећава своју организациону ефикасност. Кастелс сматра да дигиталне мреже прожимају целокупну друштвену структуру представљајући поједине структуралне категорије као засебне мреже које се преплићу и повезују у чворним тачкама, повезујући тиме и главне друштвене активности и чинећи их међузависним. С обзиром да се у мрежама замагљује класична структура моћи, то се губи и функција центра, те оне функционишу по принципу укључености/искључености. Тиме се друштвени актери појављују као укључени или искључени из мрежа. Укљученост у мреже или искљученост из њих може бити свеобухватна или парцијална. Легитимно питање којем Кастелс не посвећује пажњу је да ли је положај у мрежи подједнако битан као и питање укључености/искључености[15]. Чини се да постоји велика разлика у позицији оних који су у чворним тачкама мреже и оних који су далеко од њих. Кастелсова теза да одстојање повезаних унутар мреже тежи нули, а да одстојање умрежених и оних ван мреже тежи бесконачном је благо речено сумњива, с обзиром да мреже могу бити веома комплексне и имати сопствену, иначе голим оком видљиву или невидљиву унутрашњу структуру и хијерархију.

Развојем информатичке технологије стварање друштвених мрежа је пренесено и у виртуелни свет рачунарских мрежа. Суштинска карактеристика он-лајн друштвених мрежа ипак није у томе да оне повезују непознате, већ да њихове мреже чине видљивим.

---

11 Giddens, A. (1991): The Consequences of Modernity, Cambridge: Polity, Press, Cambridge; Beck, U. (1992): Risk Society: Towards a New Modernity, Newbury Park, Calif; Sage Publications. London; Castells, M. (2000): The Information Age: Economy, Society and Culture. Vol. 1, The Rise of the Network Society, Malden, MA: Blackwell Publishers, Inc. Oxford;

12 Wellman, B. (1988.). Structural analysis: From method and metaphor to theory and substance. in: Wellman,B. Berkowitz S.D. (eds), Social Structures: A Network Approach. Cambridge, UK: Cambridge University Press. (pp. 19-61);

13 Castells, M. (2000a) Uspon umreženog društva, Golden marketing, Zagreb;

14 Castells, M. (2004) "Informationalism, Networks, and the Network Society: A Theoretical Blueprint", in Castells M. (ed.), The Network Society: A Cross-cultural Perspective, Northampton, MA: Edward Elgar. p. 5;

15 Петровић, Д. (2007): „Од друштвених мрежа до умреженог друштва: један осврт на макро мрежни приступ у социологији". Социологија, Vol. XLIX (2007), N° 2. стр. 174-175;

Умрежени обично настављају комуникацију са онима који су присутни у њиховом свакодневном животу, а знатно ређе отпочињу комуникацију са новоумреженим, дотад непознатим особама. Корисник који отвара профил ставља се у центар свог виртуелног света креирајући садржаје које ће понудити на увид осталима. За разлику од реалних друштвених мрежа, које се веома често формирају по интересној основи, он-лајн друштвене мреже се углавном организују око људи или, прецизније, око профила, тако да се појављују као егоцентричне мреже са појединцем у центру сопствене заједнице[16].

Иако друштвене мреже на интернету постоје релативно дуго, још увек није формулисана њихова општеприхваћена дефиниција. У литератури се често срећу варијације на одредбу по којој су друштвене мреже интернет апликације изграђене на идеолошким и технолошким основама *Web 2.0* технологије које омогућавају креирање и размену кориснички генерисаних садржаја[17]. Слично гледиште заступа и Б. Линдзи који под друштвеним мрежама подразумева интернет апликације које омогућавају људима да остварују интеракцију и деле информације[18]. Нешто ширу варијанту је дао А. Монтањезе који под истим подразумева алате за повезивање и комуникацију који су доступни искључиво у сајбер-простору чије је функционисање засновано на технолошким хардверским (интернет и мобилне мреже) и софтверским (*Facebook, Twitter, MySpace, Linkedin, YouTube* и сличне) платформама захваљујући којима корисници могу да: комуницирају једни с другима, деле различите врсте садржаја (видео, фото, сликовне, текстуалне, звучне и друге записе), граде и учвршћују мреже на једном или више поља (професионалном, породичном, друштвеном, културном, религијском, политичком итд.) и развијају и дефинишу сопствени идентитет[19].

У најширем смислу друштвене мреже су облик интеракције при којима се помоћу постојећих познаника остварују виртуелни контакти са другим особама, пријатељима пријатеља. Под друштвеним мрежама на интернету се углавном подразумевају веб- сајтови који имају за циљ остваривање таквих интеракција. У литератури је често спомињана дефиниција друштвених мрежа по којој су исте одређују као мрежно засновани сервиси који дозвољавају појединцима да креирају јавне или полујавне профиле унутар омеђеног система, артикулишу листу осталих корисника мреже са којима су повезани и виде и укрштају своју листу контаката са онима које су направили други унутар система[20], с тим да природа и номенклатура тих веза може варирати од сајта до сајта.

---

16 Boyd, D. Ellison, N. (2008): ''Social network sites: Definition, history, and scholarship'', Journal of Computer-Mediated Communication 13(1): pp. 210–230;

17 Kaplan, A. M. i Haenlein, M. (2010): Users of the world, unite! The challenges and opportunities of social media, Business Horizons, Vol. 53, Issue 1. p. 61;

18 Lindsay, B, R. (2011): Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, CRS Report for Congress, Congressional Research Service http://www.infopuntveiligheid.nl/Infopuntdocumenten/R41987.pdf (10.3.2014);

19 Montagnese, A (2012): Impact of Social Media on National Security, Research Paper, Centro Militare di Studi Strategici, Rome. http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/2012/Stepi/social_media_20120313_0856.pdf (10.3.2014);

20 Boyd, D. Ellison, N. (2008): ''Social network sites: Definition, history, and scholarship'', Journal of Computer-Mediated Communication 13(1): p. 211, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (10.03.2014.).

Посебан квалитет тих сајтова је да они омогућавају корисницима да обликују и учине доступним на увид другим корисницима њихове личне мреже и да остварују међусобну интеракцију. Тиме је могуће остварити везу између појединаца који на други начин, због објективних разлога (најчешће физичке недоступности), не могу бити повезани. Наравно, није обавезно да се на овим мрежама траже нови контакти већ би пре требало да буде уобичајено се контакти одржавају са онима који су саставни део постојећих веза из реалног живота. Сајтови представљају нове облике друштвености кроз виртуелно одржавање веза са другима, а у циљу остваривања неког облика јавне афирмације. Дакле, ради се о глобалним виртуелним заједницама (које карактерише одсуство физичког простора, тзв. онлајн места) које повезују групу људи на једном месту са циљем размене контаката, ради остварења неког заједничког циља. Овај вид комуникације је у новије време постао посебно омиљен код припадника млађих генерација, мада полако осваја и старије и, наравно, образоване особе и оне који се могу сматрати информатички писменим у најширем значењу те речи.

Нема сумње да је корист од присуства на друштвеним мрежама један од битних мотива што им данас велики број људи приступа. Предности умрежености се пре свега огледају у повезаности са другима и добити која може да следи из те повезаности (размена информација, лична и професионална промоција, упознавање са истомишљеницима или са онима који деле исте циљеве, интересе и вредности итд.). Недостаци од присуства на друштвеним мрежама се углавном крећу у домену угрожавања приватности података који се стављају другима на увид, мада не треба занемарити ни опасност од замене реалног света виртуелним и отуђености која из тога природно следи, па чак и стицања патолошке зависности од интернета.

Предисторију друштвених мрежа на интернету је могуће пратити још од седамдесетих година XX века. BBS (*Bulletin Board System*) представља прву мрежу која личи на данашње друштвене мреже. Њена комуникациона суштина се састоји у томе што је корисницима омогућила размену порука те је данас многи сматрају претечом савремених друштвених мрежа. Крајем осамдесетих је покренута *CompuServe* мрежа која се може сматрати претечом савремених форумских заједница. Међу претече свакако спада и *AOL* (*American Online*) који уводи корисничке профиле и приказ основних података о власнику профила[21].

Развој друштвених мрежа на интернету и њихова права историја практично почињу од 1997. године покретањем сајта *Six Degrees.com*. До тог момента је концепт претраживања интернета и *Web*а био сведен само на пасивно прегледање садржаја на различитим *веб*-сајтовима[22]. *Six Degrees* је, по први пут, омогућио креирање сопственог профила, а касније и листе пријатеља као и прегледање листа пријатеља. Првобитни профили се нису разликовали од профила на сајтовима за упознавање или четовање. У периоду између 1997. и 2003. године је настало више друштвених мрежа од којих су неке стекле релативно велику популарност.

---

21 Boyd, D. Ellison, N. (2008): ''Social network sites: Definition, history, and scholarship'', Journal of Computer-Mediated Communication 13(1): p. 210–230. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (10.3.2014);

22 Boyd, D.; Ellison, N. (2008): ''Social network sites: Definition, history, and scholarship'', Journal of Computer-Mediated Communication 13 (1): p. 211, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (10.3.2014);

2002. године покренут је сајт *Friendster* који је омогућавао пријатељима пријатеља да се упознају, да међусобно одржавају контакте и размењују различите садржаје. Следећи значајан догађај је покретање мреже за професионално повезивање *Linkedin*. Следе *My Space* и *Orkrut* (2004). Најпознатија међу њима, *Facebook*, настаје те исте 2004. године као мрежа која је првобитно била замишљена да повезује студенте Харварда, али је веома брзо стекла популарност, тако да је 2006. постала свима доступна и од тада је њена популарност у успону[23].

Да бисмо схватили шта је оно што чини срж друштвених мрежа на интернету, морали бисмо да се осврнемо на њихову структуру. Основне компоненте које чине већину друштвених мрежа су:

- **профил корисника** - чине га основни подаци о њему, његове фотографије евентуално видео и аудио-записи и слично. Профил често представља својеврсан дигитални идентитет појединца који бира којим ће га садржајем испунити и коме ће подаци бити доступни на увид;
- **листа пријатеља** - јесте јавно доступан списак других корисника исте друштвене мреже, који је везан за профил власника са којима други имају успостављене везе тј. контакте. Поједини профили могу бити груписани у уже листе зависно од критеријума и циља груписања;
- **коментари** - сваки профил на друштвеној мрежи има одређен простор на којем је могуће остављати и размењивати различите садржаје са пријатељима и осталим корисницима. Суштина овог простора је у „видети и бити виђен“, попут некадашњих састајалишта као што су кафане или корза или напросто школска дворишта у време великог одмора, где је свако имао своје место и где је свако могао да оствари контакте са другима и да размени различите информације и, наравно, да себе прикаже у што је могуће бољем светлу. Овде се практично ради о полигону на којем се гради умрежена друштвена структура као вид виртуелних односа моћи, хијерархије, угледа или већ нечег другог, што може бити високо вредновано од стране корисника профила и мреже његових пријатеља;
- **канал вести** - представља проток информација којима се сви чланови личне мреже пријатеља обавештавају о променама на профилу био кога од њих;
- **статус** или **кратке статусне поруке** - представљају средство он-лајн комуникације путем кратких порука;
- **апликације** су нека врста виртуелне играонице на друштвеној мрежи којом се успостављају комуникације посредством различитих програма које друштвене мреже подржавају, од четовања до играња игрица, разговора у реалном времену, размена аудио, видео, фото или писаног садржаја и сличног.

23 Радовановић, Д. (2010): Интернет парадигма, структура и динамика онлајн друштвених мрежа: Фејсбук и млади у Србији, Панчевачко читалиште 17 (новембар). стр. 21-22;

3. О СОЦИЈАЛНОМ КАПИТАЛУ

Идеја социјалног капитала је доста стара (XVIII век), али је своју пуну афирмацију доживела почетком деведесетих година XX века кроз анализе Роберта Патнама. Сам термин се први пут спомиње 1916. године и извештају Л. Ј Ханифана[24] о сеоским школама у Вирџинији, да би се почео користити током друге половине XX века код више канадских социолога у истраживањима локалне заједнице и расних неједнакости[25]. Прву озбиљнију теоријску анализу социјалног капитала је дао Пјер Бурдије[26] у оквиру своје теорије капитала. Патнам је у почетку социјални капитал одређивао као карактеристике друштвене организације, попут поверења, норми и мрежа, које могу да побољшају организацију друштва преко реализације (подржавања или олакшавања) координираних ангажмана[27]. У каснијим радовима препознаје учеснике (партиципанте) као кориснике социјалног капитала[28], да би на крају социјални капитал одредио као везе међу појединцима, као друштвене мреже базиране на нормама реципроцитета и на основу њега изграђеног поверења[29] чиме чини легитимним становиште да социјални капитал постаје директно повезан са дугорочним личним интересима.

Социјални капитал долази до пуног изражаја када појединци ступају у међусобне односе са другим људима, тј. онда када се на основу заједничких вредности остварују социјалне интеракције и на бази њих граде социјалне мреже које имају вредност која се не огледа само на емоционалном плану, већ и у врло конкретним користима које су резултат поверења, узајамности, размене информација и сарадње повезаних у друштвене мреже. Дакле, социјални капитал се најчешће схвата као систем социјалних мрежа (и норми), насталих редовним социјалним интеракцијама, које олакшавају акцију појединаца и група унутар шире заједнице или друштва, односно као друштвени (заједнички) ресурс који олакшава/отежава приступ другим ресурсима, тј. потенцијално повећава компаративну предност у односу на оне који нису чланови мрежа. Социјалним капиталом, у принципу, располажу појединци повезани у различите социјалне мреже. У крајњој линији овако конципиран социјални капитал је израз личног (и друштвеног) поверења и представља везу која омогућава групну координацију и сарадњу ради постизања индивидуалне (или групне) користи.

Према Патнаму, социјални капитал садржи три компоненте: узајамност, мрежу повезаности и поверење. Под узајамношћу Патнам подразумева континуиране односе сарадње и размене који укључују обострана очекивања да ће оно што дајемо данас, бити враћено у будућности. Када је реч о мрежама

---

24 Hanifan, L. J. (1916): "The Rural School Community Center" Annals of the American Academy, of Political and Social Science No. 67. p. 130-138;

25 Farr, J. (2004): „Social Capital: A Conceptual History", Political Theory, Vol. 32, No. 1, pp. 6-33;

26 Bourdieu, P. (1986): „The Forms of Capital", u Richardson, J. G. (ed): Handbook of Theory and Research for the Sociology of Education, New York: Greenwoos Press, p. 241-258;

27 Putnam, R. D. Leonardi R. i Nanetti R. Y. (1993): Making democracy work: Civic Tradition in Modern Italy, Princeton: Princeton University Press. p. 167;

28 Putnam, R. (1995), „Tuning In, Tuning Out: The Strange Disappearance of Social Capitalin America", Political Science and Politics, vol. XXVIII. 4. pp. 664-683;

29 Putnam, R. (2000): Bowling Alone: The Collapse and Revival of American Community, New York: Simon and Schuster. p. 19;

повезаности, треба нагласити значај хоризонталних веза појединаца еквивалентног статуса и моћи.

С друге стране, вертикалне везе, у које су укључени појединци различитог статуса, не сматрају се значајним за формирање социјалног капитала. Кад се на једном месту нађу узајамност и хоризонталне мреже, онда се ствара плодно тле за развој међусобног поверења.

Поверење се јавља као резултат норми реципроцитета и оно се гради на уобичајеном коректном понашању и сарадњи и базира се на уверењу да, у најгорем случају, други учесник у мрежи може нанети некоме несвесну и ненамеравану штету, али је много вероватније да ће радити у његову корист. На основу тога се успостављају стабилни односи међусобне повезаности из којих се гради успешна сарадња базирана на подразумеваним нормама понашања ради остваривања заједничког интереса. Те норме понашања представљају својеврсан облик социјалне контроле који чини сувишним потребу за институционализованим легалним санкцијама. Дакле успостављено поверење омогућава утемељење социјалног капитала, а постојање социјалног капитала у другом кораку, поверење чини интензивнијим.

Проблем је у томе да се поверење може посматрати на различите начине, као партикуларизовано, интерперсонално и генерализованоно. Партикуларизовано поверење се исказује према онима који су нам по нечему слични и са којима делимо интересе који нам могу бити значајни. Управо због тога овај тип поверења тежи затварању, те може изазвати низ негативних последица из чега следи и његов конфликтни потенцијал. Генерализовано поверење је оно поверење које указујемо нама непознатим људима и које у себи носи капацитет за сарадњу независну од личних интереса. На бази генерализованог поверења је могуће градити мреже грађанске иницијативе[30].

Генерално се може констатовати да су кључне одредбе социјалног капитала да он обухвата све врсте односа међу појединцима, да су за њега значајне све приватне мреже и везе са пријатељима и породицом, те да се акценат ставља на апстрактне нормативне и вредносне стране међусобног поверења. У том смислу основ поверења могу бити различити облици солидарности: породична, политичко-идеолошка, религијска, интересна, унутаргрупна, у било ком значењу те речи. То значи да се поверење може градити на рачун аутсајдера чиме се улази у домен ин и аут груписања, те социјални капитал споља постаје видљив као инсајдерска група која поставља јасно дефинисане и чврсте границе којима се одељује од остатка друштва. Овим се отварају канали затвореног деловања које неретко може бити на граници, па чак и с друге стране законских и уопште социјално прихватљивих и прихваћених стандарда[31].

Да би социјални капитал остваривао друштвено вредан учинак поверење мора превазилазити оквире саме групе. У супротном, поверење завршава на

---

30 Matić, D. (2000): „Demokracija, povjerenje i socijalna pravda“, Revija za sociologiju, vol. XXXI, 3-4, Str. 183-195.

31 Miladinović, S. Two Faces of Social Capital in Structural Trends: Bonding and Bridging. In Cvetičanin, P. & Birešev, A. (eds): Social and Cultural Capital in Western Balkan Societies, Centre for Empirical Cultural Studies of South-East Europe and the Institute for Philosophy and Social Theory of the University of Belgrade, Belgrade 2012. p. 59-74.; Миладиновић, С. (2011): „Тамна страна социјалног капитала“, Нова српска политичка мисао, 3-4/2011. vol. XIX, стр. 287-316;

унутаргрупној солидарности, непремостивости групних граница и искључивању аутсајдера[32].

Кључни чинилац везан за значај друштвених мреже за формирање и функционисање социјалног капитала није толико њихов број, као и број повезаних припадника, колико је важан број активних чланова, као и однос мреже према јавним добрима и другим мрежама у окружењу. Наравно поставља се и кључно питање, којим мрежама дати предност приликом формирања социјалног капитала. Да ли предност дати грађанским удружењима или могу бити укључене чак и примарне заједнице типа породице, вршњачке и пријатељске групе (које се могу формирати у суседству, школи или у радно-професионалном окружењу). Питање које са овим треба довести у контекст је у којој мери је социјални капитал јавно а у којој мери приватно добро. Другим речима, питање се може поставити у облику: колико је он, као јавно добро, доступан различитим друштвеним класама и слојевима или различитим етничким, религијски или локалним заједницама или, напросто, свим заинтересованим за решавање неког проблема[33].

Из овога следи оправданост приговора Патмановом гледишту да занемарује негативну димензију социјалног капитала - тамну страну социјалног капитала (*dark side of social capital*)[34]. Реч је о повезивању на бази заједничких интереса. Социјални капитал омогућава социјалне односе, размену информација и у крајњој линији социјалну интеграцију, при чему је неопходно водити рачуна о квалитету међусобних односа. Суштина идеје социјалног капитала огледа се у томе да друштвене мреже или односи повезаности међу људима, немају само емотивни и лични значај, већ се огледају и кроз врло конкретне користи које су резултат међусобног поверења, узајамности, размене информација и сарадње повезаних субјеката. Ради се о томе да много тога што нам треба у свакодневном животу не можемо обезбедити нити сами нити одмах, потребна нам је повезаност са другим људима. Дакле, као нужност битисања поставља се потреба сарадње са другима и то на дужи (често неодређено дугачак) рок. Таква сарадња је тешко остварива без узајамног поверења. У овом контексту је битно ширити круг људи са којима се појединац повезује и тиме увећава своје потенцијалне шансе за добијање квалитетнијих информација или јаче подршке на већем броју места. Стога се о социјалном капиталу може говорити као о колективној вредности свих друштвених мрежа у које је неко укључен, у смислу квалитета друштвених односа њихових чланова тј. узајамности.

За једног од кључних аутора теорије социјалног капитала Џ. Колмана, социјални капитал представља поједине аспекте социјалне структуре који

---

32 Миладиновић, С. (2011): „Тамна страна социјалног капитала“, Нова српска политичка мисао, 3-4/2011. вол XIX, стр. 287-316;

33 Миладиновић, С.: „Проблем тумачења резултата истраживања друштвене (структуре и) покретљивости: идеја социјалног и културног капитала” у Немањић, М. и Спасић, И. (ур): Наслеђе Пјера Бурдијеа – поуке и надахнућа, Институт за филозофију и друштвену теорију, Завод за проучавање културног развитка, Београд, 2006. стр. 123-136;

34 Portes, A. and Landolt, P. (1996): „The Downside of Social Capital“, The American Prospect, vol. VII 26, p. 18-22.; Chambers, S. and Kopstein, J. (2001): „Bad Civil Society“, Political Theory, vol. XXIX, No. 6, p. 837-865.; Миладиновић, С. (2011): „Тамна страна социјалног капитала“, Нова српска политичка мисао, 3-4/2011. вол XIX, стр. 287-316;

подржавају одређене активности актера укључених у те структуре[35], с тим да он разликује социјални и људски капитал. Први је, по овом аутору, уграђен у друштвену структуру и представља јавно добро, док је други капитал окренут ка приватним користима[36]. Овде бисмо могли додати да се приватна корист постиже путем повезаних појединаца који заузимају различите (најчешће хијерархијски уједначене) положаје унутар званичних структура друштва. Појединци ступају у личне и приватне односе са другим појединцима релативно еквивалентног положаја, образовања, друштвеног угледа и друштвене моћи и тиме стварају друштвене мреже које представљају њихов социјални капитал. Тај исти социјални капитал се може појавити истовремено и као социјални капитал институција и организација којима припадају ти појединци и он тако може постати и јавно (или организацијско) добро. То значи да друштвене мреже, које појединци граде, истовремено могу представљати социјални капитал за институције и друге организације, али и за појединце који се повезују. Мрежа друштвене повезаности, која се при том образује на дуги рок, гради систем обавеза у виду дуговања и потраживања по основу раније учињених услуга[37], узајамног поверења, отвара путеве дистрибуције релативно поверљивих информација, успоставља норме (неретко прећутно прихваћене) и стандарде понашања. као и санкције за прекршај норми. Наравно, на овоме се темељи и коруптивни потенцијал социјалног капитала[38].

Данас се истраживачи и теоретичари концепта социјалног капитала могу поделити у две групе[39]. Прву чине они који следе траг Патмана, усвајајући његове одредбе, методологију и операционализацију (везану за ниво поверења и број формалних и неформалних удружења). Другу групу чине они који сматрају да постоји опасност да се овај концепт, некритичком применом, извитопери у своју супротност те стога заговарају потребу контекстуалне анализе социјалног капитала[40]. Развој поверења и узајамности међу припадницима социјалних мрежа готово закономерно повлачи за собом и дискриминацију и маргинализацију аутсајдера. Развијање унутаргрупног поверења и узајамности носи у себи и велики конфликтни потенцијал[41]. У вези с тим Фоли и Едвардс сматрају да посебну пажњу треба посветити друштвеној структури и институционалном оквиру, с обзиром на то да они постављају оквире за потенцијални капацитет појединаца за сарадњу и међусобно поверење, а могу бити подложни и квалитативној анализи.

---

35 Coleman, J. S. (1988), „Social capital in the creation of human capital“, The American Journal of Sociology, vol. XCIV. Supllement, p. 94-120;

36 Coleman, J. (1990), Foundations of Social Theory, Cambridge, Harvard University Press. p. 302;

37 Coleman, J. (1990), Foundations of Social Theory, Cambridge, Harvard University Press. pp. 102-104;

38 Miladinović, S. Two Faces of Social Capital in Structural Trends: Bonding and Bridging. In Cvetičanin, P. & Birešev, A. (eds): Social and Cultural Capital in Western Balkan Societies, Centre for Empirical Cultural Studies of South-East Europe and the Institute for Philosophy and Social Theory of the University of Belgrade, Belgrade 2012. p. 59-74;

39 Grix, J. (2001): „Social Capital as a Concept in Social Sciences: The Current State of the Debate“, Democratization, vol.VIII, No. 3. p. 189-210;

40 Foley, M. W. and Edwards, B. (1997): „Escape from Politics? Social Theory and the Social Capital Debate“, American Behavioral Scientist, Vol, 40. No. 5, p. 550-561.; Foley, M. W. and Edwards, B. (1998): „Beyond Tocqueville: Civil Society and Social Capital in Comparative Perspective“, American Behavioral Scientists, vol. XLI No. 1. p. 5-20;

41 Portes, A. (1998): „Social Capital: Its Origins and Applications in Modern Sociology“, Annual Reviews of Sociology, vol. XXIV, 1. p. 1- 24;

Дакле, поред свих потенцијалних погодности које носи поседовање социјалног капитала треба напоменути да оно може да има и негативне последице које се манифестују кроз клановске борбе, које се исказују синтагмом „ко није са нама тај је против нас“. Злоупотреба социјалног капитала ради постизања личне користи отвара канале корупције, што посебно може доћи до изражаја на вишим нивоима друштвене хијерархије и нарочито постаје видљиво у друштвима затворене класно-слојне структуре[42] у којима саморепродукција друштвених група представља доминантни социјални образац у токовима вертикалне друштвене покретљивости[43]. Такав социјално-структурални контекст отвара простор непотизму, корупцији етничкој, социјалној или некој другој затворености, мафијашком повезивању или различитим облицима идеолошке социјалне контроле деспотског типа. Ово се може објаснити преко схватања социјалног капитала које даје Колман[44], који под истим подразумева укупан збир потраживања које појединац испоставља на основу претходно учињених услуга, што се у овде поменутом контексту може свести на претходно учињено кршење принципа непристрасности у доношењу одлука, које сада постаје основ за будућа потраживања (по принципу ја теби-ти мени).

Генерално се чини да социјални капитал друштву и својим поседницима доноси корист. Међутим, већ је констатовано да неки облици социјалног капитала могу имати и негативне социјалне импликације, како за друштво у целини, посредством искључивања и дискриминације аутсајдера, тако и за саме чланове мрежа, кроз гушење слободе мишљења и ограничавање индивидуалне аутономије. Овде треба споменути и разне облике непотизма, корупције, организованог криминала, етничке, религијске и политичко идеолошке искључивости и слично.

Генерално, питање друштвеног учинка социјалног капитала треба довести у везу са доминантним облицима социјалног капитала, а посебно треба имати у виду присуство повезујућег и премошћујућег социјалног капитала[45]. Повезујући социјални капитал чине интензивни друштвени односи који се обично стварају унутар малих, хомогених и неретко затворених заједница (породица, клан, клика и слично) и појединаца који су по неком битном одређењу свог социјалног идентитета међусобно слични и на бази њега успостављају заједничке интересе које настоје својом повезаношћу остварити, а то чине путем међусобног поверења, узајамности и унутаргрупне солидарности. С друге стране премошћујући социјални капитал чини скуп веза и односа између хетерогених група и појединаца различитог социјалног, економског, политичког, верског и етничког порекла и генерално различитих идеолошко-вредносних оријентација и он се управо и развија у хетерогеним,

---

42 Миладиновић, С. (2003): Обрасци формирања и репродукције владајућих елита у бившој Југославији И -вертикална покретљивост, Социологија 2003, вол. 45, бр. 1, стр. 33-60; Миладиновић, С. (2003) “Обрасци формирања и репродукције владајућих елита у бившој Југославији II - канали вертикалне покретљивости - образовање и политичка активност”, Социологија 2003, вол. 45, бр. 4, стр. 347-376;

43 Миладиновић, С (2004) “Друштвена покретљивост као фактор глобалне друштвене конкурентности”, у Матејић, В. (ур) Технологија, култура и развој X, Удружење "Технологија и друштво", Институт "Михајло Пупин", Центар за истраживање развоја науке и технологије, Београд, 2004. стр. 147-156; Миладиновић, С. (1993) Вертикална друштвена покретљивост у Југославији. Социологија, vol. XXXV, бр. 2, стр. 263-281;

44 Coleman, J. (1990), Foundations of Social Theory, Cambridge, Harvard University Press. p. 305;

45 Baron, S. Field, J. and Schuller, T. (ed) (2000) Social Capital: Critical Perspectives, Oxford University Press. p. 11;

плуралистичким друштвима и значајан је за очување хармоничних односа међу припадницима различитих, а неретко и супротстављених друштвених група[46]. Повезујући фактор најчешће је опредмећен у неком заједничком интересу који својом важношћу превазилази индивидуалне интересе повезаних појединаца. Повезујући интерес има функцију моста који успоставља пречицу на путу повезивања различитих, како у хоризонталном тако и у вертикалном смислу, ради задовољавања интереса и потреба од којих примарну корист има заједница. Практично, премошћујући капитал је спона која конкретну социјалну акцију чини изводљивијом него што би она била у његовом одсуству.

Поред ова два, чини се кључна облика социјалног капитала, у литератури се срећу и други облици који могу бити доведени у контекст повезујућег и премошћујућег социјалног капитала. Ту спадају структурални (везан за групну и организациону сарадњу ради остваривања узајамних интереса посредством разних формалних и другух структура) и когнитивни (индивидуално усмерен, повезан са вредностима, нормама поверења, социјалним ставовима и слично и он усмерава појединце на узајамне колективне акције). Колман сматра да социјална структура постаје социјални капитал онда када је актер ефикасно користи за остваривање властитих интереса[47]. Поред тога могу се споменути и формални и неформални социјални капитал, социјални капитал снажних и слабих веза, као и интровертни (окренут ка промовисању интереса умрежених појединаца и група) и екстровертни (окренут ка јавном добру).

Форма и обухват социјалног капитала су директно одређени конкретном структуром и институционалном функционалношћу неког друштва. У складу с тим анализу делотворности социјалног капитала треба довести у дати социјални контекст јер он може да у себи носи капацитет за сарадњу ради остваривања личних циљева, иако се декларативно форсирају јавни циљеви, а лични негирају. Другим речима, појединци који, по природи својих положаја, заузимају позиције друштвене моћи повезују се у мреже узајамности и поверења ради остваривања личних циљева. У том контексту им расположиве институције и организације служе као оквир унутар којег остварују повезаност, а лични интереси усмеравају начин употребе социјалног капитала. Социјални капитал се тада развија у каналима паралелним, званичним институцијама и тиме прикрива своју неинституционалну конституцију. Појединци који су, обављајући своје редовне радне активности, распоређени у званичне институције, користе те исте институције као упоришта своје друштвене моћи и неинституционално се повезују са себи статусно равнима ради формирања неформалних мрежа формално моћних, које делују паралелно са званичним структурама и институцијама. На тај начин социјални капитал постаје главни актер дешавања у сивој зони друштва у којој се посредством њега, кроз искључивање аутсајдера, легализује нелојална конкуренција, а дискриминација се представаља као резултат тржишне утакмице[48].

---

46 Putnam, R. (2000) Bowling Alone: The Collapse and Revival of American Community, New York: Simon and Schuster. p. 22-24;

47 Coleman, J. (1990), Foundations of Social Theory, Cambridge, Harvard University Press. p. 305;

48 Миладиновић, С. (2004) "Друштвена покретљивост као фактор глобалне друштвене конкурентности", у Матејић, В. (ур) Технологија, култура и развој X, Удружење "Технологија и друштво", Институт "Михајло Пупин", Центар за истраживање развоја науке и технологије, Београд, 2004. стр. 147-156; Миладиновић, С. (2008) Друштво у раскораку, Нова српска политичка мисао, Београд;

Социјални капитал се тако ставља у функцију арбитра који пристрасно пресуђује у расподели других ресурса, било да се ради о радним местима, расподели материјалне добити, подели пројеката и ванредних послова, о упису деце у школе или упуту на лечење у респективну здравствену установу и слично.

Овај став се може објаснити посредством теорије капитала Пјера Бурдијеа који сматра да припадници различитих друштвених група имају различите стартне позиције које су последица различитог обима и квалитета капитала којима располажу. Пјер Бурдије[49] разликује три врсте међусобно повезаних облика капитала којим могу располагати појединци и, посредством њих друштвене групе, а то су економски, културни и социјални капитал. Економски капитал је лако препознатљив и може се институционализовати кроз власништво и власничка права. Културни капитал може бити институционализован у облику образовних квалификација и под одређеним условима конвертибилан у економски капитал.

Из Бурдијеове тезе о културном капиталу је касније изведена теза о хуманом капиталу који је нешто ширег обима и који, поред специјализованих знања и способности и радног искуства, подразумева и одређене личне особине појединца (нпр. здравствено стање, физичку снагу и кондицију, лични шарм, харизму, интелигенцију и слично). Овде ћемо имати у виду, пре свега, Бурдијеово виђење културног капитала као дела хуманог капитала којим располажу појединци и у социо-структуралном контексту он може да има значајну социолошку тежину. Сам појам хуманог капитала је примеренији у истраживању организационих структура, с обзиром на то да хуманим капиталом располажу организације и он укључује у свој садржај знатно више чинилаца од самог културног капитала у Бурдијеовом значењу. Социјални капитал чини сплет веза, обавеза и социјалних контаката које појединци, породице и друштвене групе остварују и такође може бити, под одређеним условима, конвертибилан у економски капитал. И на организационом нивоу се социјални капитал појединаца повезаних у организацију повезује у социјални капитал организације и њега је у повољном тренутку релативно лако конвертовати у економски капитал. У земљама развијене феудалне традиције социјални капитал се често јављао у виду аристократских титула и њима припадајућег статусног стила живота, а у земљама са традицијом реалног социјализма (где и ми спадамо) може бити институционализован кроз систем номенклатуре па чак, у транзиционом периоду, може бити директно конвертован у економски капитал (кроз лакши приступ економским добрима у процесу (буразерске) приватизације, било да се ради о легалном или нелегалном начину приступа економском капиталу, али и кроз добијање бољих послова и радних места).

Ове три врсте капитала нису равномерно распоређене на класе, слојеве и статусне групе које се срећу у друштву. Наравно, ова примедба је глобалног карактера с тим да се за наше друштво може констатовати тенденција концентрације сва три типа капитала на једном месту, тј. у вишим класно-слојним и статусним позицијама. Ово посебно долази до изражаја у друштвима затворене структуре, као што је наше.

Последица тога је да се, у условима неадекватне развијености тржишта и тржишних односа, социјални капитал показује као вишеструко значајан ресурс који уместо глобалног развоја, користећи се механизмима нелојалне конкуренције,

49 Bourdieu, P. (1986): „The Forms of Capital“, u Richardson, J. G. (ed): Handbook of Theory and Research for the Sociology of Education, New York: Greenwoos Press, p. 241-258;

омогућава социјалну промоцију умрежених појединаца, што за собом повлачи вишеструко негативне последице. Стога се као један од стратешких друштвених и развојних задатака поставља редизајнирање социјалног капитала како би он био у функцији глобалног развоја, увођења транспарентности у јавне послове, поштовања права и глобалне демократизације друштва.

Да ли ће овако одређени социјални и културни капитал бити употребљени у развојне сврхе зависи првенствено од социоструктуралног контекста сваког појединачног друштва. Друштва отворене структуре ће, у принципу, покушати да искористе иновациони, демократски и сваки други потенцијал ових врста капитала (било да су концентрисни на индивидуалном било на друштвеном нивоу) у циљу побољшавања сопствених перформанси. Друштва затворене структуре ће покушати да ове врсте капитала усмере ка постизању индивидуалне користи за њихове носиоце фаворизовањем функционисања интровертне варијанте повезујућег социјалног капитала на вишим нивоима друштвене хијерархије, на местима у којима је висока концентрација друштвене моћи посредством механизама дискриминације и маргинализације аутсајдера у корист интересно повезаних моћника.

Савремено доба је, између осталог и доба информационо-комуникационих технологија међу којима посебно значајно место заузима интернет. Појавом интернета и посебно са развојем специјализованих веб-сајтова, тзв. друштвених мрежа, створила се материјална основа да се социјални капитал појави и у виртуелној сфери. Друштвене мреже омогућавају брзу комуникацију, учвршћивање пријатељстава, али и изградњу пословних веза. Велика популарност коју су стекли за релативно кратко време подстакла је многе да размишљају о њиховој врло озбиљној примени. Разне организације се могу, посредством тих сајтова, приближити тржишту, пословним партнерима, корисницима услуга, купцима, сарадницима, запосленима и осталим заинтересованим физичким и правним лицима. Појединци могу да траже партнере за многе личне и пословне пројекте.

Политички живот је у последњих неколико година био поприште виртуелних борби, од предизборних кампања, па све до пучева и револуција. Страначки лидери покушавају да се приближе потенцијалним гласачима, а обични људи покушавају да искажу своје ставове, задовољство или незадовољство, подршку или отпор. Данас је могуће путем друштвених мрежа послати анониман позив и организовати масовну акцију. Од „арапског пролећа“ до најновијих сукоба у Босни и Украјини, друштвене мреже готово неочекивано постају главни актери на јавној сцени.

Све ово је у реду док је у границама социјално прихватљивог и прихваћеног деловања. Што је најгоре, чак и тамна страна социјалног капитала налази свој пут кроз виртуелну сферу. Разни облици етички неприхватљивих или легално недозвољених активности виде, у виртуелној сфери, шансу за сопствену (само)афирмацију. Организовани криминал, који увек говори истим језиком и не познаје политичке границе, у друштвеним мрежама налази нови инструмент подземних акција. Интернет пиратерија, педофилија, фишинг, хакинг и остало препознају вредности интернета и друштвених мрежа за своје мрачне циљеве. Наравно, повезује се и класични „реални“ криминал.

Списак уочених и већ, за ово кратко време, реализованих могућности употребе и злоупотреба социјалног капитала је дугачак. У овом моменту нам није циљ да анализирамо методе капитализације друштвених мрежа већ да покушамо, на бази емпиријског истраживања, да утврдимо да ли грађани Србије уочавају и

користе потенцијал друштвених мрежа за стварање и изградњу сопственог социјалног капитала. Другим речима, интересује нас да ли постоје конкретне активности или бар назнаке да се уочава могућност трансформације друштвених мрежа у социјални капитал.

4. ДРУШТВЕНЕ МРЕЖЕ И СОЦИЈАЛНИ КАПИТАЛ

У даљем тексту ће бити анализирани резултати емпиријског истраживања. Ова анализа ће обухватити следеће делове: анализу коришћења рачунара, анализу коришћења интернета и анализу коришћења друштвених мрежа. Налазе везане за наведена питања смо укрстили са генерацијском припадношћу, степеном образовања и величином насеља у којем испитаници живе. Показало се да су статистички најзначајније везе са генерацијском припадношћу, те да су везе са осталим индикаторима или без статистичке значајности или, ако су статистички значајне, оне су слабе или знатно слабије од веза посматраних варијабли са генерацијском припадношћу. Стога смо одлучили да анализирамо посматране варијабле према генерацијској припадности корисника. У разматрање смо узели само пунолетни део популације, тзв. радни контигент, с обзиром да је тема формирања и обликовања социјалног капитала најрелевантнија за тај узраст.

У контексту теме читавог пројекта ова материја има значај с обзиром да се уочава да постоји тенденција коришћења интернета и друштвених мрежа у вршењу многих кривичних дела, а између осталог и дела везаних за трговину људима и кријумчарења људи у различите сврхе, било да је у питању радна експлоатација, кријумчарење потенцијалних тражилаца политичког азила, секс- трафикинг или нешто друго. Тзв. тамна страна социјалног капитала овде долази до пуног изражаја самом чињеницом да вршиоци ових кривичних дела прелазе из реалног у виртуелни свет с намером да буду повезани не само са својим жртвама већ и са осталим актерима у ланцу криминала, што би требало да им омогући брзо деловање, размену информација о њиховом кретању и стању на терену и свакако оно за њих најзначајније, да стално буду бар један корак испред свих оних који желе да спрече и зауставе њихову противзаконити активност.

Циљ овог рада је да се утврде обрасци коришћења рачунара, интернета и друштвених мрежа у функцији јачања социјалног капитала. Примарни циљ овог истраживања је био да се, у овом погледу, утврде навике млађе популације у Србији (до 30 година старости) у вези са коришћењем интернета и друштвених мрежа. Стога је највећи део узорка управо и био концентрисан на омладину (18-30 година). Но, да би се дошло до озбиљнијих закључака о коришћењу рачунара, интернета и друштвених мрежа, ради изградње и обликовања сопственог социјалног капитала, узорку младих је придружен и један број старијих испитаника, што нам омогућава међугенерацијска поређења и утврђивање генерацијских приоритета, као и праћење кроз време, мерено генерацијским распонима, трендова прихватања и усвајања нових технологија и наравно њиховог коришћења.

Рачунари и, уопште, примена информационо-комуникационих технологија су у свакодневну употребу код нас ушли релативно скоро, тако да још увек не можемо сматрати да су постали опште прихваћени ни као алат за обављање различитих послова нити као средство редовне и свакодневне комуникације.

С обзиром да постоји закономерност у прихватању техничких и технолошких новина то се **може претпоставити да је употреба рачунара везана за:**

- **генерацијску припадност** - рачунаре су прихватиле пре свега млађе генерације тако да се може претпоставити да их сада највише користе млађи нараштаји (до 30 година) и делом средње генерације (од 30 до45 година) док су старији мање заинтересовани за њихову свакодневну употребу.
- **степен образовања** - рачунаре, када су у питању средње и старије генерације, чешће користе високо образоване особе, док у млађим генерацијама нема велике разлике у коришћењу рачунара у односу на ниво образовања.
- **друштвени статус** - припадници виших друштвених статуса у већој мери користе рачунаре него што то чине припадници нижих статусних група, без обзира на старост и ниво образовања. Тако је нпр. 88,9% домаћинстава, чији је просечан месечни приход већи од 600 евра, током протекле (2013) године поседовало рачунар. Штавише, број тих домаћинстава је у релативној стагнацији већ три године уназад. Са друге стране рачунар поседује тек 47,2% домаћинстава са приходом мањим од 300 евра и њихов број се у протекле три године увећао за преко 10%, што значи да и сиромашнији слојеви становништва увиђају значај (и предности поседовања) рачунара, информационо-комуникационих технологија и информатичке писмености, како за себе тако и за своју децу, те и поред тешке материјалне ситуације одлучују да га себи приуште. На нивоу Србије готово стопостотна студентска популација је у последња три месеца, пред спровођење анкете Завода за статистику, користила рачунаре, док број запослених који их је у том периоду користио износу од око 80%. С друге стране, тек сваки други незапослени је у истом временском периоду користио рачунар[50].
- **тип и величина насеља насеља** - с обзиром на комуналну инфраструктуру, очекивана је највећа употреба рачунара у великим градовима. Најновији подаци Завода за статистику казују да је већи број интернет прикључака у урбаним насељима. У периоду од 2011. до 2013. године број прикључака у урбаним насељима је повећан са 51% на 63,8%, док је у руралним тај број у истом периоду повећан са 27,2% на 42,5%[51].

Најраспрострањенија примена рачунара за личне потребе је за успостављање контаката и комуникацију са рођацима и познаницима посредством сајтова који се уобичајено називају друштвене мреже. У том погледу млађе генерације чешће користе рачунар у ове сврхе него старији

50 Републички завод за статистику, (2013), Употреба информационо-комуникационих технологија у Републици Србији, саопштење за јавност, 23 .9. 2013. стр. 3-6. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/14/03/PressICT2013.pdf (10.3.2014);

51 Републички завод за статистику, (2013), Употреба информационо-комуникационих технологија у Републици Србији, саопштење за јавност, 23 .9. 2013. стр. 3. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/14/03/PressICT2013.pdf (10.3.2014);

Млађе генерације користе друштвене мреже примарно **ради забаве** док **старији** настоје да на тај начин **одржавају контакте са пријатељима и родбином**.

Коришћење рачунара и друштвених мрежа за обезбеђивање тзв. социјалног капитала, тј. ради **стицања интересно заснованих контаката,** још увек код нас **није ушло у ширу употребу,** али без обзира на то постоји тенденција да се рачунари, интернет и друштвене мреже користе и у ове сврхе.

4.1. Коришћење рачунара

Готово да није потребно доказивати да су рачунари постали саставни део нашег свакодневног живота. Њих данас налазимо у свакој кући и у свакој установи, предузећу, на јавним местима и слично. Деца данас већ у нижим разредима основне школе почињу да упознају рачунарску технику и посебно њихову примену. Но, и поред свега, постоје генерације које нису имале прилику да се кроз редовно образовање упознају с рачунарима. Многи припадници средње и старије генерације су или потпуно неупућени или су самоуки корисници рачунара који их познају само површно и у свакодневном раду на њима користе само елементарна знања.

Познавање основа рада на рачунарима је данас ствар опште писмености, нешто што се у многим ситуацијама, нпр. приликом тражења посла, комуникације са многим институцијама или напросто тражења информација било које врсте, готово подразумева, а што ипак није још увек општеприсутно у свакодневном животу и раду многих. Нас је на самом почетку овог рада интересовало колико су грађани Србије упознати са радом на рачунарима, за шта их користе, у којој мери и за које намене користе интернет и да ли су повезани на друштвене мреже и колико их и ради чега користе. Наравно, узели смо у обзир и чињеницу да су се рачунари појавили у релативно скорије време, те да је било потребно да прође доста времена да они буду прихваћени и уведени у свакодневни живот.

У почетку су рачунари представљали само мало софистицираније играчке које су могле да имају и неке друге функције (писање текста, вођење различитих евиденција, табличне калкулације, цртање, припрема за штампу и слично). Након не тако пуно времена додатне функције су усавршаване тако да су рачунари освојили и радни сектор, али и домове многих људи. Једноставно су постали саставни део многих домаћинстава, подразумевани део кућне опреме попут телевизора, електричног шпорета или фрижидера. Појава интернета, а касније и друштвених мрежа, само је убрзала њихово увођење у свакодневни живот обичних људи. Данас је многима живот постао незамислив без рачунара. Овде, кад кажемо рачунари мислимо на шири спектар производа који могу у мањој или већој мери да обављају многе рачунарске функције, укључујући десктоп и лаптоп рачунаре, али не занемарујући ни, у новије време, све популарније таблет рачунаре и њима сличне уређаје, попут мобилних телефона који се у својим новијим варијантама могу сматрати мини рачунарима па чак и малим електронским канцеларијама.

Да бисмо видели какво је стање на терену, анализу спроведеног истраживања смо почели од питања „да ли знате да користите рачунар?“.

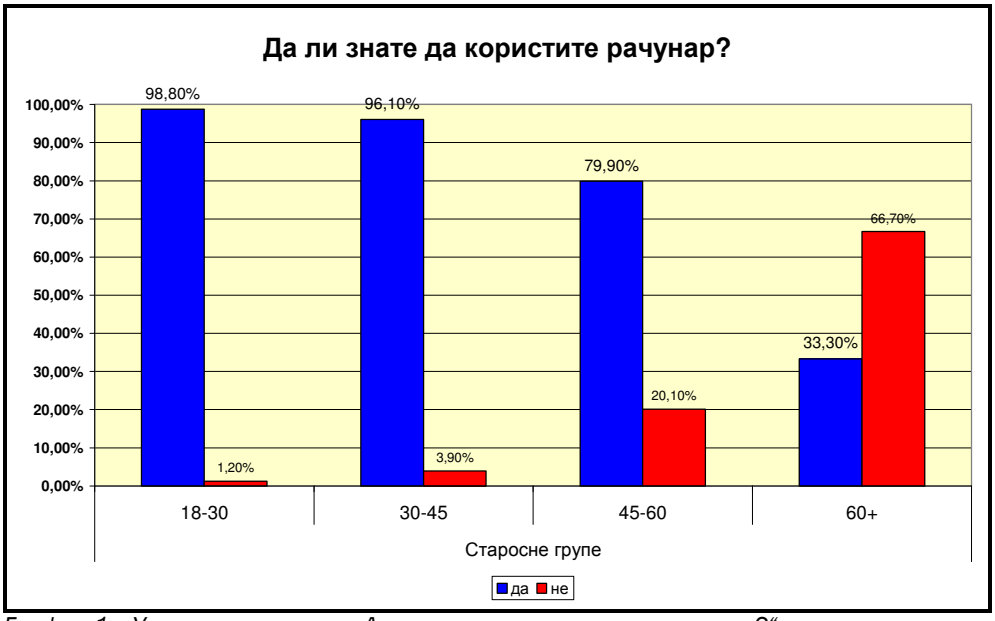


График 1. Укрштање питање „Да ли знате да користите рачунар?“ са генерацијским групама

Табела 1. Укрштање питања „Да ли знате да користите рачунар?“ са генерацијским групама

Да ли знате да користите рачунар?		Старосне групе			
		18-30	30-45	45-60	60+
да		98,8%	96,1%	79,9%	33,3%
не		1,2%	3,9%	20,1%	66,7%
Тотал	N	1073	155	139	42
	%	100,0%	100,0%	100,0%	100,0%

Сви	x^2=410,838	V=0,540	p<0,000
Без 60+	x^2=132,956	V=0,312	p<0,000

Као што смо претпоставили на самом почетку анализе, показало се да је познавање рада на рачунарима генерацијски детерминисано, те да постоји видна разлика у познавања рада на рачунарима међу припадницима различитих генерација. Мерено Крамровим V коефицијентом утврђена је веза средње јачине (која нагиње ка јачој вези) познавања рада на рачунарима и генерацијске припадности (V=0,54). Ако из разматрања искључимо старије од 60 година, тада долази до драстичног пада вредности Крамеровог коефицијента на износ 0,31, што директно указује на чињеницу постојања статистички значајне генерацијске поделе на оне који знају и оне који не знају да раде на рачунарима, а чија граница се подиже на ниво старијих педесетих година или ранијих шездесетих година. То значи да је генерацијска детерминација везана за период када су се рачунари појавили на нашим просторима. Практично, они који су у том моменту били тридесетогодишњаци или старији, у принципу, нису се адаптирали на „ново чудо

(или чедо) технике", те нису стигли, могли или хтели да се с њим ближе упознају. Може се претпоставити да су најстарији добили подстицај да се упознају са рачунарима или због потребе посла при крају њихове радне каријере или да би могли бити у контакту с најближима, а првенствено с децом која су, одвојивши се од породице у којој су одрасла, кренула својим путем. Овај мотив је посебно актуелан код великог броја оних чија су деца, посебно током деведесетих али и касније, напуштала Србију и одлазила у удаљене земље, чак и преко океана, у потрази за својим животним шансама. Њима су се интернет и друштвене мреже појавили као веома рационалан начин комуникације.

Подаци у табели 1 казују да млађи од 30 година, готово сви, знају да користе рачунар (98,8%). Ништа лошије није стање ни у генерацији 30-45 година који у 96,2% случајева знају да раде на рачунарима. Већ у генерацији старости од 45-60 година има 79,9% оних који владају рачунарима, што се такође може сматрати изузетно добрим резултатом, тим пре јер се ради о генерацијама које нису имале прилику да се упознају са рачунарском техником током свог редовног школовања. Овде је реч о радном контигенту, те се може претпоставити да је велики број припадника ових генерација, напросто због потреба посла, морао да савлада рад на рачунарима, ако већ то није могао да постигне током школовања. Са старијима од 60 година ситуација је знатно лошија. У тој генерацији тек једна трећина влада овим знањима. Управо се ради о онима који су имали тридесет и више година у време када су на наше просторе стизали први синклери, спектруми и комодори, рачунари који су пре били мало боље играчке него компјутери у садашњем значењу. Реч је о генерацијама које једва да су могле да осете значај нове технологије за надолазећа времена, те у складу с тим нису ни показивале интерес да се с њом ближе упознају. Ради се о генерацији која се у ширем глобалном контексту може сматрати трензицијским и глобализацијским губитником у вртлозима дешавања из деведесетих на просторима бивше Југославије. У питању је генерација која је била највећа жртва идеолошке индоктринације из ранијег периода и која напросто, као генерација, није имала довољно снаге да се прилагоди већини друштвених промена, па самим тим ни новим технолошким решењима која је изнедрио развој информационо-комуникационих технологија.

На бази ових података се може закључити да велика већина становништва Србије, а млађих од 45 година, готово у потпуности влада елементарним знањима потребним за рад на рачунарима. То још увек не значи да су оспособљени да обављају сложеније задатке, али у сваком случају су оспособљени за сналажење на интернету или неком од уобичајених програма за свакодневну употребу.

Табела 2. Где и колико често користите рачунар?

	Где и колико често користите рачунар?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
118-30	код куће	47,15%	41,16%	9,09%	1,80%	,80%	100,00%
	факултет/школа	5,07%	19,04%	37,40%	26,85%	11,64%	100,00%
	на послу	15,01%	6,24%	5,31%	6,47%	66,97%	100,00%
	у интернет-кафеу	2,73%	6,18%	13,09%	23,45%	54,55%	100,00%
	у играоници	2,19%	6,18%	8,76%	14,14%	68,73%	100,00%
	на јавном месту	7,12%	16,89%	27,81%	22,19%	25,99%	100,00%
30-45	код куће	30,77%	41,26%	18,18%	6,99%	2,80%	100,00%
	Факултет/школа	8,82%	8,82%	5,88%		76,47%	100,00%
	на послу	43,00%	23,00%	6,00%	8,00%	20,00%	100,00%
	у интернет-кафеу		3,45%	12,07%	24,14%	60,34%	100,00%
	у играоници			1,92%	5,77%	92,31%	100,00%
	на јавном месту	4,69%	12,50%	29,69%	15,63%	37,50%	100,00%
445-60	код куће	13,56%	38,14%	25,42%	7,63%	15,25%	100,00%
	Факултет/школа	1,75%	3,51%	5,26%		89,47%	100,00%
	на послу	42,27%	14,43%	8,25%	1,03%	34,02%	100,00%
	у интернет-кафеу	1,69%	1,69%	5,08%	8,47%	83,05%	100,00%
	у играоници		1,72%		3,45%	94,83%	100,00%
	на јавном месту		11,29%	8,06%	4,84%	75,81%	100,00%
60+	код куће	3,23%	16,13%	6,45%	9,68%	64,52%	100,00%
	Факултет/школа					100,00%	100,00%
	на послу	8,00%			4,00%	88,00%	100,00%
	у интернет-кафеу					100,00%	100,00%
	у играоници					100,00%	100,00%
	на јавном месту					100,00%	100,00%

Табела 3. Крамерови V коефицијенти и мере значајности веза за укрштање питања „Где и колико често користите рачунар“, са старосним групама

Где и колико често користите рачунар?	Старосне групе / сви			Без 60+		
	x^2	V	p	x^2	V	p
код куће	464,932	0,35	0,000	175,750	0,27	0,000
на факултету/у школи	338,751	0,37	0,000	279,946	0,41	0,000
на послу	128,846	0,26	0,000	117,965	0,30	0,000
у интернет-кафеу	36,160	0,13	0,000	20,082	0,12	0,010
у играоници	38,191	0,14	0,000	29,548	0,16	0,000
на јавном месту	113,246	0,22	0,000	69,766	0,24	0,000

Из претходне табеле (табела 1) видели смо да се велика већина испитаних, с изузетком старијих од 60 година, изјаснила да зна да користи рачунар. Да бисмо сагледали размере коришћења рачунара потребно је да видимо где и колико често испитаници користе рачунаре. Уобичајена места на којима се могу користити су код куће, на факултету или у школи, када је реч о млађим корисницима рачунара, на послу, у интернет-кафеима, у играоницама или на јавним местима. Динамику коришћења рачунара ћемо сагледати кроз одговоре увек, често, понекад, ретко и никад.

За млађе од 30 година се може констатовати да рачунаре редовно (увек или често) користе код куће (83,31% уз 18,18% оних који то чине понекад), а да их велики број њих понекад или ретко користи на факултету или у школи (64,25%), односно на јавним местима (укупно 50%). Припадници генерације 30-45 година рачунаре користе код куће, а одговоре увек или често даје њих 72,03% или на послу (66%). Скоро трећина њих рачунаре повремено користи на јавним местима. Припадници старосне скупине 45-60 година рачунаре најчешће користе код куће и то увек, често или понекад чини њих 77,12% или на послу (увек и често 56,7% уз 8,25% оних који то чине понекад). Старији од 60 година углавном не користе рачунаре.

Места на којима наши испитаници углавном не користе или ретко кад користе рачунаре су интернет-кафеи и играонице. Такође није уобичајено да исте користе на јавним местима.

Укрштањем генерацијске припадности и места у учесталости коришћења рачунара, утврђена је статистички значајна веза у свим комбинацијама. Мерено Крамеровим V коефицијентом најјача веза је регистрована код укрштања генерацијске припадности са коришћењем рачунара у школи или на факултету где вредност V коефицијента, рачунајући и старије од 60 година, износи 0,41 (веза средње јачине). Искључењем најстаријих вредност V коефицијента пада на 0,37 (веза на граници средње и слабе јачине). Веза средње јачине утврђена је још у комбинацији коришћења рачунара код куће, уз искључење најстаријих (V=0,35). Овоме доприноси чињеница да већина породица купује рачунар због деце (укључујући и старију децу – до 30, па и преко 30 година, која у Србији још увек уживају повлашћени статус унутар породице), а да га родитељи односно старији укућани користе само када им млађи за то оставе простора. Вредност V коефицијента од 0,30 је регистрована и у случају коришћења рачунара на послу (комбинација у којој су узети у разматрање и старији од 65 година), чиме се само потврђује чињеница да велику већину старијих од 60 година чине пензионери, који по природи ствари немају приступ рачунарима на послу.

Табела 4. За које сврхе користите рачунар (и колико)?

	За које сврхе користите рачунар (и колико)?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
18-29	учење	21,60%	45,41%	24,16%	4,99%	3,83%	100,00%
	посао	17,55%	15,19%	13,02%	12,03%	42,21%	100,00%
	информисање	39,83%	47,16%	9,93%	1,18%	1,89%	100,00%
	комуникацију	40,19%	43,24%	11,08%	3,29%	2,19%	100,00%
	забаву	32,27%	40,61%	17,30%	6,38%	3,44%	100,00%
	играње игрица	14,85%	16,97%	20,61%	26,06%	21,52%	100,00%
	коцкање	2,42%	2,97%	6,32%	6,69%	81,60%	100,00%
	остало	10,60%	5,96%	8,61%	2,65%	72,19%	100,00%
30-45	учење	11,11%	31,94%	23,61%	9,72%	23,61%	100,00%
	посао	52,83%	15,09%	11,32%	7,55%	13,21%	100,00%
	информисање	26,85%	43,52%	22,22%	3,70%	3,70%	100,00%
	комуникацију	20,00%	41,00%	22,00%	10,00%	7,00%	100,00%
	забаву	11,11%	36,67%	34,44%	10,00%	7,78%	100,00%
	играње игрица	1,45%	11,59%	28,99%	23,19%	34,78%	100,00%
	коцкање		1,79%	3,57%	3,57%	91,07%	100,00%
	остало	3,57%	10,71%	7,14%		78,57%	100,00%
45-60	учење	4,23%	14,08%	14,08%	11,27%	56,34%	100,00%
	посао	50,00%	15,31%	9,18%	7,14%	18,37%	100,00%
	информисање	18,75%	38,54%	20,83%	2,08%	19,79%	100,00%
	комуникацију	8,64%	25,93%	20,99%	12,35%	32,10%	100,00%
	забаву	2,53%	15,19%	29,11%	7,59%	45,57%	100,00%
	играње игрица		5,88%	13,24%	20,59%	60,29%	100,00%
	коцкање			1,59%	6,35%	92,06%	100,00%
	остало	2,22%	2,22%			95,56%	100,00%
60+	учење		3,70%	11,11%	3,70%	81,48%	100,00%
	посао	7,41%		3,70%	3,70%	85,19%	100,00%
	информисање	3,45%	20,69%	6,90%	3,45%	65,52%	100,00%
	комуникацију	3,57%	7,14%	3,57%	7,14%	78,57%	100,00%
	забаву			8,00%	8,00%	84,00%	100,00%
	играње игрица		4,00%	4,00%		92,00%	100,00%
	коцкање					100,00%	100,00%
	остало	4,55%				95,45%	100,00%

Табела 5. Крамерови V коефицијенти и мере значајности веза за питање „За које сврхе користите рачунар (и колико)?“, са старосним групама

За које сврхе користите рачунар (и колико)?	Старосне групе / сви			Без 60+		
	x^2	V	p	x^2	V	p
учење	366,155	0,34	0,000	259,827	0,36	0,000
посао	124,806	0,24	0,000	95,505	0,26	0,000
информисање	304,055	0,31	0,000	112,083	0,23	0,000
комуникацију	385,844	0,35	0,000	196,005	0,31	0,000
забаву	380,101	0,35	0,000	239,723	0,35	0,000
играње игрица	117,636	0,22	0,000	66,828	0,21	0,000
коцкање	14,644	0,09	0,262	9,603	0,09	0,294
остало	19,384	0,16	0,080	14,205	0,18	0,077

С обзиром на широку применљивост рачунара у свакодневном животу, корисно је видети у које се сврхе они најчешће користе. На питање „за које сврхе користите рачунар и колико?“ испитаницима су били понуђени одговори: за учење, посао, информисање, комуникацију, забаву, играње игрица, коцкање и остало а за динамику упражњавања наведених активности понуђени су им одговори: увек, често, понекад, ретко и никад. Показало се да постоје извесне разлике у обрасцима коришћења рачунара међу припадницима различитих генерација.

Од посматраних осам комбинација укрштања сврхе коришћења рачунара са генерацијским кохортама, статистички значајна веза утврђена је код шест комбинација. Значајне везе нема само код укрштања генерацијске припадности са коцкањем и категоријом остало. Највиша вредност Крамеровог V коефицијента утврђена је у укрштању генерацијске припадности са учењем (V=0,36) и забавом (V=0,35) на укупном узорку пунолетне популације, док је у радном контигенту вредност V коефицијента највиша при укрштању са забавом и комуникацијом (у оба случаја V=0,35). Може се сматрати да се ради о очекиваним налазима с обзиром да су у питању активности којима су склоније млађе генерације за које је већ потврђено да чешће користе рачунаре од старијих. У питању је веза слабог интензитета која нагиње вези средње чврстине. Интензитет ове везе је очекиван с обзиром да се најмлађи не оријентишу само на забаву, већ користе рачунаре и за друге потребе (нпр. учење, комуникацију, информисање и слично) док се старији претежно окрећу ка послу и информисању, а употребу рачунара као средства за забаву запостављају, што се може уочити на осново података из табеле 4.

У генерацији млађих од 30 година одговори увек и често су били најзаступљенији код изјашњавања да рачунаре користе ради информисања. Те одговоре дало је 86,99%. На другом месту је одговор ради комуникације који у обе поменуте варијанте даје њих 83,43%. Следе забава (72,88%) и учење (67,01%). Генерација старости од 30-45 година најчешће користи рачунар ради информисања (70,37%), затим ради посла (67,92%) и комуникације. Следе забава и учење које практикује нешто мање од половине испитаника ове старосне скупине. Генерација старости између 45-60 година, рачунаре најчешће користе због посла и код њих заступљеност одговора увек и често износи 65,31%. На другом месту је информисање (57,29%), а на трећем је комуникација којој се приклања тек трећина испитаних припадника ове генерацијске скупине (34,57%).

Са друге стране млађи од 30 година рачунаре користе ретко или никад ради онлајн коцкања (88,29%), с тим да одговор никад даје њих 81,60%. Други одговор по учесталости некоришћења рачунара је ради посла који даје 54,24% испитане популације. На трећем месту је играње игрица (47,58%). Овде треба напоменути да је играње игрица приметна али не и доминантна активност код 31,82% припадника исте популације. Дакле један део млађих од 30 година се не занима за играње игрица док му други, не мали део (трећина), посвећује пуно времена. Припадници генерације 30-45 година најмањи свог времена за рачунаром посвећују онлајн коцкању (94,64%) и игрању игрица (57,97%). Трећа активност коју ова генерација најмање упражњава за рачунаром је учење (33,33%). Најмање популарне активности за рачунаром код генерације старости 45- 60 година су коцкање (98,41%) и играње игрица (80,88%). Следе учење (67,61%), забава (53,16%) и комуникација (44,45%).

На основу података из табела може се закључити да постоје различите оријентације у коришћењу рачунара које су генерацијски детерминисане. Учење и стицање нових знања су приоритет млађих од 30 година и са преласком из једне у другу старосну скупину долази до смањивања интереса за ову активност. То је и разумљиво с обзиром да се знатан део ове популације налази у процесу школовања, те да по завршетку школовања јењава интерес за учењем и уопште стицањем нових знања. Такође је занимљив податак да и употреба рачунара ради комуникације драстично опада са преласком из једне у другу генерацијску кохорту. Млађи од 30 година је не практикују тек у 5,48% случајева, они између 30 и 45 година у 17,00% случајева, а старији део радног контигента чак у 44,45% случајева. Сличне тенденције су и са коришћењем рачунара ради забаве. Посматрано по генерацијским кохортама млади рачунар редовно користе ради забаве у 72,88% случајева, они између 30 и 45 година у 47,78% случајева, док генерација старости од 45 до 60 година прибегава рачунарској забави тек у 17,72% случајева. На основу овога можемо закључити да се млађе генерације брже прилагођавају технолошким новинама од старијих, те да су спремнији да преузму нове обрасце друштвености док су старији, као генерално конзервативнији, склони да се држе проверених социјалних образаца на које су већ навикнути и нису спремни да у томе нешто битније мењају.

У време када су рачунари почињали да улазе у наш живот, три деценије уназад, они су били готово синоним за играње игрица. Компјутерске игрице су биле и, на неки начин, све до данас остале заштитни знак кућних рачунара. Налази овог истраживања казују да оне данас немају ни приближан значај који су имали за просечног корисника рачунара из ранијих времена. Временом се пуно тога променило, од хардверске конфигурације самих рачунара до софтверских апликација и могућности њихове употребе у свакодневном животу и раду. У међувремену је еволуирала њихова практична употребљивост, али је такође дошло и до засићења игрицама. Овоме су сигурно допринели и други облици рачунарске забаве (појава интернета са сајтовима музичких, филмских и других забавних садржаја) који су извесно повукли и један број оних који су рачунаре користили за играње игрица.

Треба напоменути да је још једна активност забавног карактера ушла у виртуелни простор, а то је коцкање. Некада су коцкарнице и казина били резервисани само за клијентелу са дубљим џеповима, а у земљама попут Србије, у којима је доминирао социјалистички друштвени поредак, ова врста забаве је чак

била искључиво толерисана за стране држављане. Распадом социјалистичког система се и казина отварају за домаће грађане, а појавом интернета и коцкање постаје демократизовано. Он-лајн казина су сада доступна на интернету. Преко оваквих сајтова се окреће велики новац и они постају атрактивни многима, од власника казина и коцкарница и представника организованог криминала па све до државе која може посредством њих да убира велики порез. За разлику од професионалних казина у којима се углавном игра на веће улоге, у онлајн-казинима је могуће коцкање и за мање новца и та чињеница вероватно има значај за њихову растућу популарност. Срећна је околност што интерес за овом врстом забаве на нашим просторима није узео маха, али и поред тога евидентно је да један број корисника рачунара исте користи да би приступио онлајн-коцкању. Овде се очигледно ради о проблему који несумњиво заслужује већу друштвену пажњу и потребу да буде јасније правно регулисан.

На основу реченог се може закључити да постоји веза генерацијске припадности са социјалним обрасцима коришћења рачунара у различите сврхе, с тим да су млађе генерације окренуте ка учењу, забави и комуникацији, а да рачунаре слабо користе због посла. Део објашњења овог тренда треба тражити у чињеници да је значајан део младих, до 30 година старости, још увек на школовању, те да се у овом сегменту популације налази и велики број незапослених, али и оних који нису формирали породице, па добар део свог слободног времена усмеравају на образовање, забаву и унутаргенерацијску комуникацију. Потврда овом је податак из табеле 4 да због посла рачунаре користи тек трећине припаднике ове генерацијске скупине, а да их, с друге стране, за исте потребе, ретко или никад не користи нешто више од половине њих (54,24% односно 42,21% који их због посла уопште не користе). Средња и старија генерација радног контигента користе рачунаре, у највећој мери, управо због посла и нешто мање због информисања и комуникације. Приметно је да употреба рачунара рапидно опада са генерацијском припадношћу, што се и овом приликом може објаснити већом пријемчивошћу млађих нараштаја за коришћење информационо-комуникационих технологија за ове намене. Старији остају верни старим методама информисања посредством штампаних и електронских медија. У најстаријем делу радног контигента (између 45 и 60 година) долази до видног, ако не чак и рапидног, опадања интереса за коришћење рачунара ради забаве и комуникације са другима. Старији остају верни традиционалним механизмима забаве и комуникације.

4.2. Коришћење интернета

Питање од којег ћемо поћи у емпиријској анализи социјалних образаца коришћења интернета је „да ли користите интернет?". На основу података у табели 6 може се закључити да млади у највећој мери користе интернети те да са старошћу опада број његових корисника. Крамеров V коефицијент утврђује везу средње јачине у укрштању генерацијске припадности са коришћењем интернета (Крамеров V=0,51). Налази казују да та веза постепено слаби код радно активног контигентиа а да код старијих од шездесет година долази до драстичног пада коришћења интернета. Искључивањем из разматрања старијих од 60 година долази до видног смањивања вредности Крамеровог коефицијента на V=0,27и што значи да је у

радно активном делу становништва веза ове две посматране варијабле у граници слабе јачинеи али ипак статистички значајна (p<0,000). У овоме налазимо потврду става да је коришћење интернета код старијих генерација делом и радно-професионално детерминисано, односно да многи од њих користе интернет у вези са потребама на послу. Наши налази се поклапају за резултатима истараживања Републичког завода за статистику које показује да постоји значајна разлика између оних који користе и оних који не користе интернет. Просечан корисник интернета у Србији је млађи и образованији од оних који га не користе и претежно припада урбаној популацији[52].

Табела 6. Укрштање питања „Да ли користите интернет?“ са генерацијским групама

Да ли користите интернет?	Старосне групе			
	18-30	30-45	45-60	60+
да	97,1%	91,8%	76,8%	23,8%
не	2,9%	8,2%	23,2%	76,2%
	100,0%	100,0%	100,0%	100,0%
N	1074	158	138	42
Сви	x^2=361,072	V=0,51	p<0,000	
Без 60+	x^2=98.644	V=0,27	p<0,000	

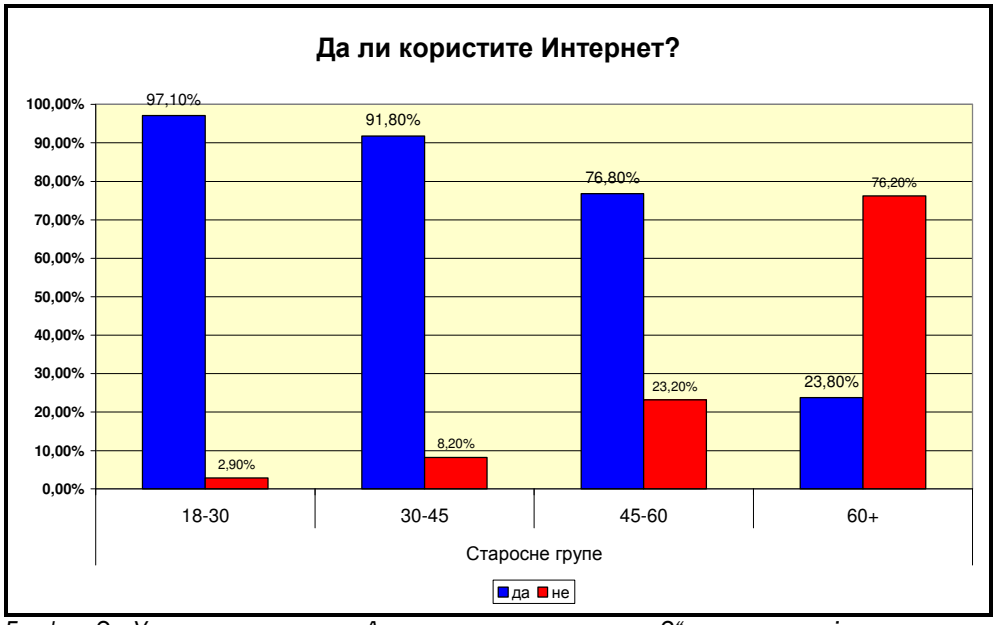


График 2. Укрштање питања „Да ли користите интернет?“ са генерацијским групама

52 Републички завод за статистику, (2013), Употреба информационо-комуникационих технологија у Републици Србији, саопштење за јавност, 23 .9. 2013. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/14/03/PressICT2013.pdf (10.3.2014);

Као и у претходном случају и овде можемо констатовати да су касне педесети или ране шездесете године граница на којој рапидно опада употреба интернета и такође као и у претходном случају и овде можемо говорити о генерацијском јазу који је, између осталог, условљен и историјским тренутком у којем су рачунари и њихова употреба стигли на наше просторе. Може се претпоставити да сама чињеница припадности радном контигенту представља значајну детерминанту коришћења интернета с обзиром да је данас готово незамисливо обављати свакодневне послове и радне задатке без помоћи информационо-комуникационих технологија. Друга претпоставка која се намеће из ових налаза је да се рапидни пад коришћења интернета код најстаријих може повезати и са чињеницом да је већина њих већ била у зрелој доби кад су на наше просторе стигли персонални рачунари. Њих су уобичајено, прво прихватили припадници млађих генерација, тј. они који сада већ увелико припадају средњим и старијим генерацијама у радном контигенту, али не и старијим генерацијама у укупној популацији. Како су се смењивале генерације тако су и рачунари постепено улазили у свакодневни живот и рад људи на простору Србије и наравно, у највећој мери бивали прихватани од стране млађих генерација радног узраста и школске омладине.

Табела 7. Крамерови V коефицијенти и мере значајности веза за питање „Ако користите Интернет, колико често?“ са генерацијским групама

Ако користите интернет, колико често?	Старосне групе			
	18-30	30-45	45-60	60+
неколико пута месечно	2,2%	8,2%	17,3%	27,3%
једном недељно	2,4%	4,1%	3,6%	27,3%
неколико пута недељно	12,5%	17,0%	24,5%	-
свакодневно до једног сата	27,4%	28,6%	21,8%	9,1%
свакодневно од једног до пет сати	42,4%	32,7%	28,2%	36,4%
свакодневно преко пет сати	13,1%	9,5%	4,5%	-
Тотал	100,0%	100,0%	100,0%	100,0%
N=1326	1058	147	110	11

Сви	χ^2=129,036	V=0,18	p<0,000
Без 60+	χ^2=90,885	V=0,19	p<0,000

За разлику од навике коришћења интернета, која је између осталог и генерацијски детерминисана, интензитет коришћења интернета је, мерено Крамеровим V коефицијентом, у веома слабој вези са генерацијском припадношћу корисника интернета. Оно што се види из података у табели је да корисници млађи од 60 година интернет свакодневно користе у надполовичном износу (млађи од 30 година га свакодневно користе у 82,90% случајева, средњи део радног контигента га користи у 70,80% случајева, док га свакодневно користи 50,40% најстаријих из радног контигента). Дакле, млађи од 45 година интернет у већини случајева користе свакодневно док је динамика коришћења интернета код старијих од 45 година релативно равномерно распоређена на све понуђене временске интервале с изузетком свакодневног коришћења у трајању дужем од пет сати. Овај закључак донекле ремети релативно мали подузорак старијих од 60 година, од којих већи део не користи интернет, те се о динамици његовог коришћења изјаснило свега 11 испитаника.

Дакле, и овде је на делу генерацијска детерминација. Са старошћу опада динамика коришћења интернета. Иако је веза генерацијске припадности и динамике коришћења интернета веома слаба, она је ипак статистички значајна.

Табела 8. Које сајтове посећујете на Интернету (и колико)?

	Које сајтове посећујете на интернету (и колико)?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
18-30	образовне	16,41	46,28	27,98	6,97	2,36	100,00
	информативне	28,56	54,38	13,77	2,05	1,25	100,00
	музичке/филмске	26,87	50,06	17,95	2,62	2,50	100,00
	за поруке	21,50	31,78	17,45	13,24	16,04	100,00
	чет рум-ове	9,48	16,75	12,18	18,44	43,15	100,00
	друштвене мреже	38,69	38,69	12,66	5,04	4,92	100,00
	за игрице	11,28	21,33	18,55	24,27	24,57	100,00
	за игре на срећу	3,28	14,85	6,22	10,36	65,28	100,00
	за преузимање филмова и музике	23,92	37,43	23,11	7,70	7,84	100,00
	за упознавање	3,90	14,43	13,41	22,58	45,67	100,00
	за тражење посла	4,17	20,03	19,53	18,20	38,06	100,00
	нешто друго	11,00	20,46	19,95	11,00	37,60	100,00
30-45	образовне	15,46	46,39	17,53	10,31	10,31	100,00
	информативне	21,01	50,42	24,37	1,68	2,52	100,00
	музичке/филмске	6,06	43,43	34,34	11,11	5,05	100,00
	за поруке	9,23	24,62	21,54	18,46	26,15	100,00
	чет рум-ове		10,00	11,67	23,33	55,00	100,00
	друштвене мреже	14,89	36,17	24,47	9,57	14,89	100,00
	за игрице	4,84	16,13	14,52	25,81	38,71	100,00
	за игре на срећу		3,85	3,85	11,54	80,77	100,00
	за преузимање филмова и музике	7,79	25,97	29,87	23,38	12,99	100,00
	за упознавање	1,75	3,51	22,81	10,53	61,40	100,00
	за тражење посла	2,70	25,68	27,03	13,51	31,08	100,00
	нешто друго		11,76	32,35	14,71	41,18	100,00
45-60	образовне	4,55	28,41	23,86	15,91	27,27	100,00
	информативне	20,37	45,37	16,67	3,70	13,89	100,00
	музичке/филмске	6,41	16,67	26,92	8,97	41,03	100,00
	за поруке	4,35	14,49	8,70	14,49	57,97	100,00
	чет рум-ове		9,68	3,23	3,23	83,87	100,00
	друштвене мреже	2,56	24,36	17,95	8,97	46,15	100,00
	за игрице		7,46	11,94	19,40	61,19	100,00
	за игре на срећу		7,69	4,62	4,62	83,08	100,00

	Које сајтове посећујете на интернету (и колико)?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
	за преузимање филмова и музике	2,90	8,70	13,04	18,84	56,52	100,00
	за упознавање		7,81	4,69	4,69	82,81	100,00
	за тражење посла	2,94	14,71	17,65	7,35	57,35	100,00
	нешто друго		5,77	9,62	5,77	78,85	100,00
60+	образовне	5,26	5,26	21,05	5,26	63,16	100,00
	информативне	9,52	28,57	9,52		52,38	100,00
	музичке/филмске		11,76	5,88	5,88	76,47	100,00
	за поруке		21,05		5,26	73,68	100,00
	чет рум-ове		5,88		5,88	88,24	100,00
	друштвене мреже		11,11		5,56	83,33	100,00
	за игрице		5,88			94,12	100,00
	за игре на срећу		5,88			94,12	100,00
	за преузимање филмова и музике				5,88	94,12	100,00
	за упознавање			5,88		94,12	100,00
	за тражење посла		5,88			94,12	100,00
	нешто друго		6,25	6,25	6,25	81,25	100,00

Табела 9. Крамерови V коефицијенти и мере значајности веза за укрштање питања „Које сајтове посећујете на интернету (и колико)?“ са генерацијским групама

Које сајтове посећујете на интернету (и колико)?	Старосне групе / сви			Без 60+		
	x^2	V	p	x^2	V	p
образовне	216,907	0,26	0,000	125,363	0,25	0,000
информативне	207,867	0,25	0,000	73,665	0,18	0,000
музичке / филмске	366,986	0,34	0,000	265,489	0,36	0,000
за поруке	108,603	0,21	0,000	79,114	0,23	0,000
чет рум-ове	58,917	0,16	0,000	47,556	0,18	0,000
друштвене мреже	286,355	0,30	0,000	195,636	0,31	0,000
за игрице	81,718	0,19	0,000	48,978	0,18	0,000
за игре на срећу	22,376	0,10	0,034	16,681	0,11	0,034
за преузимање филмова и музике	271,975	0,32	0,000	188,909	0,33	0,000
за упознавање	59,461	0,17	0,000	46,096	0,18	0,000
за тражење посла	37,767	0,13	0,000	16,709	0,11	0,033
нешто друго	51,239	0,19	0,000	41,367	0,21	0,000

Као што смо у претходним анализама добили социјалне обрасце коришћења рачунара по генерацијским групама, тако је могуће утврдити и социјалне обрасце коришћења интернета. Претпоставка од које полазимо је да су и овде млађе генерације склоне посећивању веб-сајтова забавног садржаја док су старији склони посећивању веб-сајтова информативно-образовног садржаја.

Генерацијска припадност је укрштена са основном наменом веб-сајтова које корисници интернета уобичајено посећују. Веб-сајтови су разврстани на следеће категорије: образовни, информативни, за гледање филмова и слушање музике, сајтови за поруке, чет румови, друштвене мреже, сајтови за игрице, за игре на срећу, за преузимање филмова и музике, за упознавање, сајтови за тражење посла и остали (у табели означени као нешто друго). И овог пута је динамика посећивања поменутих сајтова категорисана као увек, често, понекад, ретко и никад.

Све комбинације укрштања овде анализираних старосних група са свим поменутим категоријама веб-сајтова су се показала статистички значајним. Мерено Крамеровим V коефицијентом везу најјачег интензитета има укрштање генерацијске припадности са посећивањем сајтова за гледање филмова и слушање музике (V=0,34/0,36). За њим следе према јачини веза укрштања са сајтовима за преузимање филмова и музике (V=0,32/0,33) и сајтовима друштвених мрежа (V=0,30/0,31). За све ове комбинације Крамерови V коефицијенти се крећу у износима од 0,30 до 0,36 што указује на статистички значајну везу слабе јачине, која у појединим случајевима показује тенденцију нагињања ка вези средње јачине. Разлика у висини Крамерових коефицијената за подузорке са и без популације старије од 60 година, занемарљива је и не доприноси битно интерпретацији резултата.

Подаци у табели 8 казују да млађи од 30 година најчешће (одговори увек и често) посећују сајтове информативног карактера (82.94%). На другом месту су друштвене мреже које редовно (увек и често) посећује њих 77,38%. Следе сајтови за слушање музике и гледање филмова (76,93%) и образовни сајтови (62,69%). Високо посећени су и доста спорни сајтови за преузимање филмова и музике (61,35%) као и сајтови за поруке (52,38%).

Припадници генерације од 30 до 45 година најчешће посећује информативне (71,43%) и образовне (61,85%) сајтове. Половина њих посећује друштвене мреже (51,06%) и сајтове за слушање музике и гледање филмова (49,49%). Генерацијска скупина од 45 до 60 година старости најчешће посећује информативне сајтове (65,74%). На другом месту су сајтови образовног садржаја, које редовно посећује њих 32,96%. Сви остали сајтови се знатно ређе посећују. Због малог броја корисника интернета у категорији старијих од 65 година, свака дубља статистичка анализа је непоуздана, али се може уочити као тенденција да се највише прате сајтови информативног карактера и сајтови за поруке.

Са друге стране се налазе сајтови који се најмање или се уопште не посећују. Млади до 30 година ретко или уопште не посећују сајтове за игре на срећу, тзв. онлајн коцкарнице и слично (75,64%), сајтове за упознавање (68,25%), чет румове (61,59%) и сајтове за тражење посла (56,26%). Генерација стрости од 30 до 45 година ретко кад посећује или никад не посећује сајтове за игре на срећу (92,31%), чет- румове (78,33%), сајтове за упознавање (71,93%) и за игрице (64,52%). Овоме се придружује и категорија осталих сајтова у износу од 55,89% ретког или никаквог посећивања. Генерацијска скупина од 45 до 60 година показује слабо или готово никакво интересовање за већину типова сајтова. Од тога је чак пет категорија које

се никад или ретко кад посећују од стране више од четири петине испитаних корисника сајтова из ове старосне групе. То су сајтови игара на срећу, за упознавање, чет румови, сајтови категорисани као нешто друго и сајтови за игрице. Следе, са више од 70% корисника који се изјашњавају да никад или ретко посећују сајтове за преузимање филмова и музике и сајтове за поруке. Сајт које не посећује две трећине испитаника је сајт за тражење посла, док више од половине испитаника из ове категорије не посећује друштвене мреже и а половина не посећује сајтове за слушање музике и гледање филмова. Огромна већина старијих од 65 година нема навику редовног посећивања свих наведених категорија веб-сајтова тако да о њима у овом контексту можемо говорити само условно.

Дакле, генерално се може констатовати да највише врста сајтова посећују млађи од 30 година, с тим да су већим делом заинтересовани за друштвене мреже, сајтове информативног, образовног и забавног карактера. С друге стране, преласком у старије генерацијске скупине спектар сајтова који се уобичајено посећују се редукује на информативне и образовне, да би се код још старијих, од 45 година, генерално свео само на информативне сајтове које у категорији старијих од 65 година посећује тек нешто мање од две четвртине оних који користе интернет.

И овде, као и у претходној анализи, може се закључити да су млађи спремнији на шире коришћење интернета од старијих. То се закључује на основу ширег спектра сајтова које уобичајено користе у односу на оне које посећују старији. Илустративан је и налаз да се преласком у старије старосне скупине редукују садржаји који се редовно прегледају на интернету и да се практично своде на информисање. Најстарији део популације (од 60 година) готово је свео употребу Интернета само на тражење вести и других информативних садржаја. Такође је илустративан и налаз да интерес за стицање знање опада са старошћу. То се, и у овом случају, делом може разумети као последица престанка потребе за формалним образовањем, али и као последица засићења информацијама које су с једне стране данас на интернету доступније него икад раније, а са друге стране су до те мере постале неселективне и непоуздане да се тешко могу узимати за озбиљно.

Доказ да су млади спремнији да прихвате нове облике друштвености које нуди интернет је и податак да више од три четвртине млађих од 30 година отвара профиле на друштвеним мрежама и ступа у редовну размену информација са познатим и непознатим особама, док се међу припадницима старијих генерација редукује број корисника друштвених мрежа, али и број особа са којима ови остварују редовну виртуелну интеракцију. Тако нпр. половина корисника интернета из генерације 30 – 45 година и само четвртина њих из генерације 45-60 година посећује сајтове друштвених мрежа док то чини занемарљив број старијих од 60 година (сваки десети).

4.3. Коришћење друштвених мрежа

На бази одговора на питање „На којим друштвеним мрежама поседујете налоге?“ може се закључити да међу посматраним генерацијским скупинама постоји јединствен редослед у коришћењу друштвених мрежа, односно да не постоје друштвене мреже које су пријемчиве овој или оној генерацијској скупини. Убедљиво најпопуларнија од свих друштвених мрежа је *Facebook*. Са генерацијском

припадношћу долази до видног опадања учесталости њеног коришћења. Млади у готово девет десетина случајева имају отворен налог на фејсбуку. Како прелазимо на следеће генерације, тако се и учешће оних који користе фејсбук значајно смањује у односу на претходну генерацијску скупину (18-29: 87,77%; 30-44: 62,89%; 45-59: 35,97%). Друга по популарности је *You Tube,* трећа *Google* + и четврта *Twitter*. Остале друштвене мреже су присутне у готово занемарљивој мери.

Табела 10. На којим друштвеним мрежама поседујете налоге (вишеструки одговори)

На којим друштвеним мрежама поседујете налоге	Старосне групе							
	18-30		30-45		45-60		60+	
	%	N	%	N	%	N	%	N
Facebook	87,77%	947	62,89%	100	35,97%	50	10,87%	5
Twitter	22,34%	241	14,47%	23	4,32%	6		
You Tube	49,12%	530	26,42%	42	12,95%	18	2,17%	1
Linkedin	6,12%	66	6,92%	11	3,60%	5		
Google +	31,42%	339	22,01%	35	6,47%	9	2,17%	1
Foursquare	3,43%	37	1,89%	3	,72%	1		
Tumblr	4,91%	53	,63%	1				
друге	5,19%	56	2,52%	4				
Тотал/број мрежа и учесника	2,10	1079	1,38	159	0,64	139	0,15	46

У просеку, типичан припадник генерације млађе од 30 година је присутан на 2,10 друштвених мрежа (табела 10, последњи ред испод ознаке %), док је припадник следеће старије скупине (30-45 година) присутан на 1,38 друштвене мреже, а припадник генерације 45-60 година је присутан на 0,64 друштвених мрежа. Према нашем подузорку типичан представник генерације старије од 60 година је присутан на 0,15 друштвених мрежа. Овај последњи податак треба прихватити са извесном резервом с обзиром на величину узорка и релативно мали број корисника интернета унутар ове скупине.

Linkedin је, гледано из угла формирања социјалног капитала, свакако концепцијски најзначајнија професионална друштвена мрежа и њега у популацији до 44 године старости користи око 6-7% корисника интернета, а у групи оних 45-60 година тек њих 3,6%. На основу ових података можемо закључити да ова друштвена мрежа на нашем простору није заживела у пуној мери, те да се генерално социјални капитал гради на неком другом простору (у реалном друштву) или на другим друштвеним мрежама.

Табела 11. Крамерови V коефицијенти и мере значајности веза за укрштање питања „На којим друштвеним мрежама поседујете налоге?“ са старосним групама

На којим друштвеним мрежама поседујете налоге	Старосне групе / сви			Без 60+		
	x^2	V	p	x^2	V	p
Facebook	235,143	0,41	0,000	338,647	049	0,000
Twitter	28,379	0,14	0,000	40,229	0,17	0,000
You Tube	85,604	0,25	0,000	116,653	0,29	0,000
Linkedin	1694	0,04	0,429	4,654	0,06	0,199
Google +	41,170	0,17	0,000	56,805	0,20	0,000
Foursquare	3,870	0,05	0,144	5,406	0,06	0,144
Tumblr	13,058	0,10	0,001	15,351	0,10	0,002
друге:	9,422	0,08	0,009	11,815	0,09	0,008

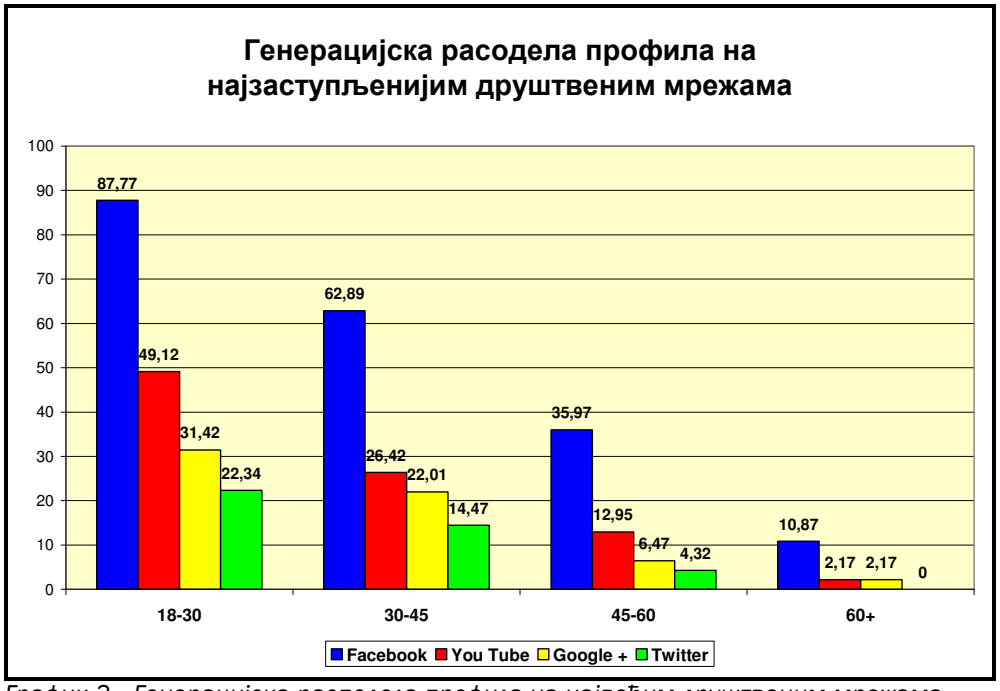


График 3. Генерацијска расподела профила на највећим друштвеним мрежама

Укрштање старосних група даје статистички значајне везе са поседовањем налога на свим друштвеним мрежама осима на *Linkedin* и *Google +*. Мерено Крамеровим V коефицијентом, најјача је веза установљена са поседовањем налога на *Facebook*. У комбинацији у којој су узети у разматране старији од 60 година вредност Крамеровог V коефицијента износи 0,49, што указује на везу средње јачине. Искључивањем ове групе из разматрања добија се вредност V=0,41, што је тек нешто мало изнад границе везе слабе и средње јачине. Ово је потврда

чињенице да је *Facebook* у Србији првенствено друштвена мрежа младих и млађих генерација. Такође бисмо, на основу вредности V коефицијента и *You Tube* условно могли одредити као мрежу младих, с обзиром да се у комбинацији у којој је урачуната и популација старијих од 65 година вредност V коефицијента V=0,29 што је тик испод прага релевантности за озбиљнију анализу. Иако овај коефицијент имплицира слабу везу, он ипак наговештава да постоји, макар у назнакама, генерацијска детерминација у расподели корисника ове мреже.

Табела 12. Са ким комуницирате путем друштвених мрежа (и колико)?

	Са ким комуницирате путем друштвених мрежа (и колико)?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	
18-30	са члановима породице	23,64	34,77	24,02	11,38	6,19	100,00
	са најближим пријатељима	45,34	43,73	7,94	1,96	1,04	100,00
	са емотивним партнером	34,37	31,69	15,35	8,73	9,86	100,00
	са он-лајн пријатељима	12,71	24,50	28,18	20,67	13,94	100,00
	са познаницима	10,42	25,83	35,80	21,60	6,34	100,00
	са колегама и сарадницима	18,12	40,80	25,53	7,13	8,42	100,00
	са непознатима	2,63	4,55	10,68	27,15	54,99	100,00
30-44	са члановима породице	8,97	44,87	26,92	16,67	2,56	100,00
	са најближим пријатељима	17,98	57,30	16,85	6,74	1,12	100,00
	са емотивним партнером	14,29	26,53	24,49	20,41	14,29	100,00
	са он-лајн пријатељима	14,29	17,86	39,29	19,64	8,93	100,00
	са познаницима	8,77	26,32	36,84	24,56	3,51	100,00
	са колегама и сарадницима	14,75	21,31	42,62	18,03	3,28	100,00
	са непознатима	2,04	8,16	12,24	38,78	38,78	100,00
45-60	са члановима породице	20,00	25,00	30,00	17,50	7,50	100,00
	са најближим пријатељима	16,67	33,33	33,33	8,33	8,33	100,00
	са емотивним партнером	4,55	13,64	13,64	9,09	59,09	100,00
	са он-лајн пријатељима	3,70	11,11	29,63	25,93	29,63	100,00
	са познаницима	7,14	14,29	42,86	14,29	21,43	100,00
	са колегама и сарадницима	11,43	22,86	25,71	25,71	14,29	100,00
	са непознатима			8,70	34,78	56,52	100,00

Табела 13. Крамерови V коефицијенти и мере значајности веза за укрштање питања „Са ким комуницирате путем друштвених мрежа (и колико)?“ са старосним групама

Са ким комуницирате путем друштвених мрежа (и колико)?	Старосне групе / сви		
	x^2	V	p
са члановима породице	15,412	0,09	0,05
са најближим пријатељима	78,657	0,20	0,00
са емотивним партнером	67,999	0,21	0,00
са онлајн пријатељима	12,892	0,09	0,12
са познаницима	13,201	0,09	0,11
са колегама и сарадницима	30,053	0,16	0,00
са непознатима	7,972	0,08	0,44

Социјалне обрасце коришћења друштвених мрежа смо анализирали посредством одговора даваних на питање с ким комуницирате путем друштвених мрежа и колико. И код овог питања је претпоставка да постоји генерацијска детерминација, те се очекује да ће млади комуницирати првенствено с пријатељима и особама са којима одржавају емотивну везу, док ће се код старијих интересовање за овај вид комуникације померити ка породици, родбини, колегама и сарадницима. Са друге стране се претпоставља да ће се најмањи интерес за ову врсту комуникације показати за непознате особе. Искуство је показало да посредством друштвених мрежа већина учесника не тражи нове познанике са којима би се повезали већ настоје да одржавају везу са људима које познају од раније[53]. У популацији старијој од 60 година добили смо само два испитаника која су одговарала на ова питања тако да свака анализа њихових одговора губи смисао те овде неће бити ни узети у разматрање.

Статистички значајне везе у укрштању генерацијске припадности и категорије повезаног корисника са којим се (не)остварује комуникација путем друштвених мрежа су евидентиране само у три случаја: у укрштањима са најближим пријатељима, емотивним партнерима и колегама и сарадницима, с тим да су вредности Крамеровог V коефицијента веома мале, те можемо констатовати постојање врло слабих веза посматраних категорија са генерацијском припадношћу. Елиминацијом из разматрања старијих од 65 година добија се статистички значајна веза и у укрштању са члановима породице и рођацима, али са неизмењеном вредношћу Крамеровог V коефицијента.

Генерација млађих од 30 година најчешће комуницира са најближим пријатељима. Одговоре увек и често даје њих 89,07%. На другом месту је комуникација са особама са којима ступају у емотивне везе (66,06%). Следе колеге и сарадници и чланови породице. Дакле, најмлађи су уједно и најдруштвенији корисници інтернета и друштвених мрежа. Док више од половине млађих од 30 година успоставља редовну комуникацију чак са четири категорије особа повезаних на њихову друштвену мрежу, дотле припадници генерацијске скупине 30-44 године на својој листи најучесталијих контаката имају само две категорије умрежених пријатеља са којима редовно комуницира више од половине њих: најближе

53 Boyd, D. Ellison, N. (2008): ''Social network sites: Definition, history, and scholarship'', Journal of Computer-Mediated Communication 13(1): p. 211, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (10.3.2014);

пријатеље (75,28%) и чланове породице (53,84%). Високо заступљена комуникација са емотивним партнерима у категорији млађих од 30 година сада пада са две трећине на две петине корисника друштвених мрежа. Наравно, овакав налаз би требало да се сматра очекиваним с обзиром да је у млађој популацији много више оних који још увек не живе у брачној или ванбрачној заједници, тј. у истом домаћинству са својим емотивним партнером, те у складу с тим имају и већу потребу да с њима одржавању виртуелну комуникацију. Код старијих старосних група се тај проблем делимично компензира заједничким животом, па се природно смањује потреба за редовном интеракцијом ове врсте. Најстарији део радног контигента, они од 45 до 60 година су склони да време које проводе на друштвеним мрежама поделе само са својим најближим пријатељима (50,0%), рођацима и члановима породице (45,0%). Са колегама и сарадницима преко друштвених мрежа комуницира тек једна трећина њих.

Најређу комуникацију млађи од 30 година остварују са непознатима. С њима ретко или никад комуницира 82,14% испитаних припадника ове генерацијске скупине, док више од половине њих то не чини уопште. Други по редоследу искључености из свакодневне комуникације су тзв. он-лајн-пријатељи, тј. особе које су по различитим критеријумима укључене у мрежу, али са којима се у принципу не остварује било која врста примарне комуникације. Треба напоменути да је дистрибуција одговора који указују на динамику комуникације са тзв. он-лајн-пријатељима релативно равномерно распоређена на обе стране комуникацијског опсега, 37,21% корисника са њима остварује редовну комуникацију, а 34,61% то чини ретко или никад. Дакле, не ради се о групи која је у принципу искључена из комуникације већ се ради о групи која заузима друго место на скали поређених комуникација. Може се рећи да је генерација 30-45 година мало отворенија за непознате, али још увек њих три четвртине ретко или никад не комуницира са непознатима. На другом месту по поређености комуникације налазе се емотивни партнери, али је овде дистрибуција комуникације са њима релативно равномерно распоређена на све понуђене одговоре (40,82% испитаних корисника друштвених мрежа из ове старосне скупине с њима остварује редовну комуникацију посредством друштвених мрежа док нешто мало мање њих то чини ретко или никад). Припадници генерације 45-60 година ретко или никад контактирају са непознатима и то чак у 91,30% случајева. Практично, старији од 45 година су најнеповерљивији у комуникацији са непознатима јер се нико од њих није изјаснио да са непознатима остварује редовну комуникацију. Поред непознатих, ова генерацијска скупина не остварује значајну комуникацију ни са емотивним партнерима као ни с категоријом осталих он-лајн пријатеља, а приметно је и смањење комуникације са колегама и сарадницима у односу на обе млађе генерацијске скупине.

Оно што је интересантно за старосну групу 30-45 година је да се појављује релативно велики број оних који са појединим категоријама повезаних у своју друштвену мрежу остварују повремену комуникацију, тако да 42,62% њих повремено комуницира са колегама и сарадницима, 39,29% са осталим он-лајн пријатељима и 36,84% са познаницима. Дакле, може се закључити да знатан број корисника друштвених мрежа на интернету, из ове генерације, успоставља релативно умерену виртуелну комуникацију са својим он-лајн-пријатељима. Слична констатација важи и за генерацију 45-60 година старости с обзиром да и они, са извесним категоријама повезаних на њихову мрежу, остварују релативно умерену

комуникацију тако да понекад комуницирају са познаницима (42,86%), најближим пријатељима (33,33%) и члановима породице и рођацима (30,0%).

На основу приказаних података се може закључити да не постоје битније разлике у социјалним обрасцима комуникације преко друштвених мрежа припадника различитих генерација у односу на посматране категорије умрежених пријатеља. Видно је да постоји генерацијска разлика у смислу да старије генерације проводе мање времена на друштвеним мрежама, али се не може тврдити да постоји битна разлика између самих социјалних образаца остварене комуникације.

Табела 14. У које сврхе користите ове сајтове?

	У које сврхе користите ове сајтове?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
18-30	за зближавање са члановима породице	17,17	25,00	19,43	18,07	20,33	100,00
	за зближавање са пријатељима	24,76	32,24	21,77	11,02	10,20	100,00
	за проналажење „изгубљених“ рођака, пријатеља и познаника	10,73	19,13	30,79	18,97	20,37	100,00
	за упознавање што више особа	4,33	11,25	20,59	27,68	36,16	100,00
	за повезивање са особама сличних / истих интересовања	4,79	15,56	26,50	27,35	25,81	100,00
	за посредовање	1,53	5,15	14,12	25,95	53,24	100,00
	за остваривање емотивних веза	2,72	7,25	12,32	20,47	57,25	100,00
	за проналажење посла	2,48	8,38	12,57	25,90	50,67	100,00
	то је део мог посла	5,10	7,76	9,59	11,02	66,53	100,00
	за „убијање времена“	15,34	32,60	29,94	11,50	10,62	100,00
30-45	за зближавање са члановима породице	11,48	36,07	21,31	16,39	14,75	100,00
	за зближавање са пријатељима	13,04	37,68	24,64	17,39	7,25	100,00
	за проналажење „изгубљених“ рођака, пријатеља и познаника	3,39	27,12	35,59	22,03	11,86	100,00
	за упознавање што више особа		8,16	24,49	53,06	14,29	100,00
	за повезивање са особама сличних / истих интересовања		15,69	49,02	13,73	21,57	100,00
	за посредовање			18,42	23,68	57,89	100,00
	за остваривање емотивних веза		5,00	12,50	35,00	47,50	100,00
	за проналажење посла	2,33	11,63	27,91	32,56	25,58	100,00 %
	то је део мог посла	2,44	9,76	19,51	19,51	48,78	100,00
	за „убијање времена“	10,53	24,56	35,09	22,81	7,02	100,00
45-60	за зближавање са члановима породице	12,90	16,13	32,26	12,90	25,81	100,00
	за зближавање са пријатељима	11,76	11,76	29,41	23,53	23,53	100,00
	за проналажење „изгубљених“ рођака, пријатеља и познаника	6,90	17,24	31,03	24,14	20,69	100,00
	за упознавање што више особа	3,85	11,54	15,38	11,54	57,69	100,00

	У које сврхе користите ове сајтове?	Увек	Често	Понекад	Ретко	Никад	Тотал
		%	%	%	%	%	%
	за повезивање са особама сличних / истих интересовања	6,90	13,79	20,69	13,79	44,83	100,00
	за посредовање	4,76	4,76			90,48	100,00
	за остваривање емотивних веза		4,55	4,55	13,64	77,27	100,00
	за проналажење посла		8,00	24,00	16,00	52,00	100,00
	то је део мог посла		13,64	4,55	18,18	63,64	100,00
	за „убијање времена“		25,00	25,00	21,43	28,57	100,00

Табела 15. Крамерови V коефицијенти и мере значајности веза за укрштање питања „У које сврхе користите ове сајтове?“ са старосним групама

У које сврхе користите ове сајтове?	Старосне групе без 60+		
	x^2	V	p
за зближавање са члановима породице	19,491	0,09	0,077
за зближавање са пријатељима	27,772	0,11	0,006
за проналажење „изгубљених“ рођака, пријатеља и познаника	13,515	0,08	0,333
за упознавање што више особа	27,135	0,12	0,007
за повезивање са особама сличних / истих интересовања	14,033	0,11	0,020
за посредовање	18,946	0,10	0,090
за остваривање емотивних веза	10,503	0,08	0,572
за проналажење посла	17,393	0,10	0,135
то је део мог посла	12,943	0,09	0,407
за „убијање времена“	24,797	0,10	0,016

За наше истраживање је од битног значаја разумевање сврхе коришћења друштвених мрежа. Из тог разлога смо им и поставили питање у које сврхе их користе. Пошли смо од претпоставке да већина власника профила најчешће користи друштвене мреже за зближавање са члановима породице, за зближавање са пријатељима, за проналажење „изгубљених“ рођака, пријатеља и познаника, за упознавање што више особа, за повезивање са особама сличних или истих интересовања, за разне врсте посредовања, за остваривање емотивних веза, проналажење посла, зато што је коришћење друштвених мрежа део њиховог посла или напросто за „убијање времена“. Претпоставили смо и овде стандардну динамику коришћења истих кроз одговоре увек, често, понекад, ретко и никад.

На основу вредности Крамерових V коефицијената утврдили смо да само четири ставке, од посматраних десет, имају статистички значајну везу са генерацијском припадношћу ако посматрамо комплетан узорак пунолетних. Реч је о ставкама, за зближавање с пријатељима, за упознавање што више особа, за

повезивање са особама сличних или истих интересовања и за убијање времена. Међутим, ако из разматрања искључимо старије од 60 година, добијамо још две ставке које исказују статистички значајну везу (за посредовање и за проналажење посла). У свим случајевим веза је веома слаба, готово занемарљива. На основу ових налаза можемо закључити да не постоји битна веза у разлозима за посећивања наведених сајтова међу припадницима различитих генерација. Расподеле које су се показале кроз табеле у већини случајева имају случајан карактер и представљају тенденције у назнакама.

Показало се да млађи од 30 година ове мреже највише користе за зближавање са пријатељима (57,0%), а да их велики број редовно користи за „убијање времена“ односно за зближавање са члановима породице и рођацима. Занимљиво је да су прилично учестали одговори да млади друштвене мреже понекад користе ради зближавања са пријатељима (57%), разбијања досаде (или „убијања „времена – нешто мало мање од половине њих), а и ради зближавања са члановима породице (42,17%). Око половине припадника генерације 30-45 година друштвене мреже такође учестало користи ради зближавања са пријатељима и родбином, док трећина њих то чини да би превазишла досаду или проналазила „изгубљене“ пријатеље и рођаке. Висока учесталост повременог коришћења друштвених мрежа је због повезивања са особама истих или сличних интересовања, које практикује половина испитиване популације, док трећина њих покушава да пронађе изгубљене пријатеље, познанике и рођаке или напросто да прекрати време. На основу одговора које дају припадници старосне скупине од 45 до 60 година, можемо закључити да они генерално слабо користе друштвене мреже. Када то чине, чине то најчешће ради одржавања контаката са члановима породице и родбином (29,03% њих који их користе увек или често на шта можемо додати и трећину оних који то чине повремено, што у укупном збиру износи нешто више од три петине оних који редовно или повремено користе друштвене мреже са овом намером). Понекад се одговор у овој генерацији јавља као модални одговор на прве три ставке из посматране табеле и у сва три случаја се налази негде испод нивоа трећине испитане популације.

Млади најмање користе друштвене мреже за посредовања, зато то је то „део њиховог посла“, за остваривање емотивних веза и за проналажење посла. По свим ставкама, друштвене мреже ретко или никад користи око три четвртине испитане популације млађих од 30 година. Занимљиво је да се на том списку налази и упознавање што више особа (трећина младих), али и повезивање са особама истих и сличних интересовања (половина). Такође и генерација од 30 до 45 година нема обичај да друштвене мреже користи ради посредовања и остваривања емотивних веза. Код ових ставки одговоре ретко и никад даје више од четири петине испитаника из ове генерације. Две трећине њих не користи мреже ради упознавања што више особа нити зато што то извире из потреба њиховог посла, а више од половине њих ни за проналажење посла. Ни најстарији део радног контигента нема значајно другачију структуру одговора којима се исказује слабо или никакво коришћење друштвених мрежа. Једина разлика у односу на млађе групе је у томе да сада преко 90% њих не користи ове мреже ради посредовања или налажења емотивних партнера, док нешто мање њих то не доживљава као потребу и саставни део свог посла. Треба напоменути да ни две трећине њих не покушава на овај начин да тражи посао или да упознаје велики број људи.

Само се неколико припадника најстарије генерације (један до троје), старијих од 60 година, изјаснило о својим интересовањима везаним за коришћење друштвених мрежа, тако да њихови одговори не могу водити никаквим закључцима. Такође ни мере значајности веза не одступају битно увођењем у разматрање најстарији део популације. Крамеров V коефицијент се увећава за максимално 0,03 што је за било какву анализу знемарљиво.

Генерални закључак који се може извести из приказаних података је да се друштвене мреже најчешће користе ради комуникације и остваривања блиских веза са породицом и најближим пријатељима, као и ради разбијања досаде и прекрађивања времена. Продуктивно коришћење друштвених мрежа је сведено на релативно малу меру и то најчешће код нешто старијих испитаника или, прецизније, средњег генерацијског скупа из радног контигента, односно код оних који су већ укорењени у пословним активностима и који би требало да се налазе близу врхунца своје професионалне каријере. Ово је у складу са већ констатованим налазима ранијих истраживања да они који у реалном свету већ имају шире мреже друштвене подршке сусклони да и интернет све више користе за одржаванје својих веза. Они се више друже са већ познатим пријатељима, а преко интернета и сајтова друштвених мрежа настоје да одржавају и продубљују своје контакте и јачају успостављене везе, али, ипак, нису склони ка стварању нових познанстава[54]. Изгледа да млађи још увек нису препознали да друштвене мреже могу да имају велики потенцијал у својству и са циљем изградње социјалног капитала, а да старији, зато што се налазе у последној трећини својих каријера, више и немају нарочити интерес да се прилагођавају новим инструментима како би је даље подстицали. Дакле, средњи део радног контигента је највише мотивисан да друштвене мреже инструментализује за заузимање и учвршћивање радних и, уопшт,е професионалних позиција уз ограду да ни они значајније не одступају од остатка популације. Дакле, види се могућност, али генерално изостаје акција на капитализовању друштвених мрежа зарад јачања професионалних позиција и то примарно у средњој генерацији радног контигента.

Ако пођемо од тога да социјални капитал чине мреже познанстава које се могу активирати за решавање конкретних проблема, тада је битно и то да ли се ради о активним или пасивним познанствима. Виртуелне мреже, по логици ствари, нуде пасивна познанства. Под пасивним виртуелним познанствима подразумевамо све оне повезане или умрежене „пријатеље“ који преостану иза рођака, блиских пријатеља, познаника, колега и сарадника. Дакле, ради се, у принципу, о потпуно непознатим особама са којима се власници профила повезују из најразличитијих разлога. У смислу социјалног капитала, најзначајнији су они виртуелни пријатељи са којима власници профила деле заједничке интересе, циљеве, вредности, а посебно они чије је професионално деловање на овај или онај начин комплементарно с њиховим.

Комплементарност сама по себи није довољна, мора постојати и некаква директна повезаност коју виртуелна умреженост, сама по себи, не нуди. Виртуелна умреженост има смисла само ако је резултат директног тражења пословног партнера по принципима тржишне понуде и тражње. Неке, углавним професионалне, друштвене мреже са интернета покушавају да превазиђу тај проблем тако што се, у старту усмеравају на склапање професионалних контаката.

54 Петровић, Д. (2013): Друштвеност у доба Интернета, Академска књига, Београд, стр. 238;

Linkedin, као једна од њих, директно се ослања на поверење као једну од основних компоненти социјалног капитала. Контакте на тој и њој сличним друштвеним мрежама држи у виртуелној заједници управо поверење, засновано на стручној и професионалној припадности. На бази тако утемељеног поверења, настоји се изградити лична мрежа са неодређено великим бројем сопствених контаката.

Друге мреже, попут *Facebook* и њој сличних, чију кохезију одржава шири спектар интереса и мотива за међусобно повезивање, поред стручних и професионалних интереса, често одржава мотив за припадношћу неком хетерогеном, понекад неструктурисаном и неиздиференцираном скупу особа за које бисмо могли речи, аналогно језику реалног света, да настањују једну тачку на ширем виртуелном простору, тачку коју бисмо, условно речено, могли назвати виртуелним селом. Специфичност тако замишљеног виртуелног села, у односу на реалну насеобинску тачку, била би у томе да јединка насељава велики број виртуелних села, односно да се свако виртуелно село формира и концентрише око једног корисничког профила. Практично, колико има профила толико и има и виртуелних заједница, тј. села. У том смислу виртуелни грађанин је у односу на реалног грађанина космополита који припада свуда, у мери броја контаката које је остварио на друштвеној мрежи или на друштвеним мрежама посредством свог/својих профила, али истовремено не припада нигде јер простим чином брисања свог профила, до даљњег нестаје са бројног стања свих профила и на њима заснованих виртуелних заједницама у којима се до тада налазио. Исто као што на реалној насеобинској тачки са физичког простора појединац, у мањим заједницама, може да зна скоро све чланове, иако их лично или по неком другом критеријуму близине не познаје, тако и у виртуелном селу појединац често зна или бар препознаје многе иако их лично не познаје.

Теоретичари социјалног капитала су већ констатовали да није толико битно колико нечија мрежа веза и познанстава има чланова, колико је битан број активних чланова, тј. оних који се могу покренути зарад остваривања неког појединачног циља или интереса. У виртуелним заједницама то посебно добија на значају с обзиром да се често, као пријатељи, на сопствену мрежу додају потпуно непознате особе за које се понекад претпоставља да би у ближој или даљој будућности могле бити од користи. У таквим околностима се може постулирати природна тежња сваког власника профила на друштвеној мрежи да своје контакте пресели из виртуелног у реални свет или, другим речима, да се упозна са потенцијално употребљивим виртуелним пријатељима.

Табела 16. Колико пријатеља имате на друштвеној мрежи

Колико пријатеља имате на Facebook **–у /** *Twitter*-**у...?**	**Старосне групе**		
	18-29	**30-44**	**45-59**
до 100	10,2%	25,0%	56,6%
101 - 500	47,9%	47,0%	30,2%
501 – 1000	28,5%	23,0%	11,3%
1001 - 2000	10,3%	5,0%	1,9%
преко 2000	3,1%		
Тотал %	100,0%	100,0%	100,0%
N	962	100	53
Без 60+	x^2=109,378	V=0,22	p<0,000

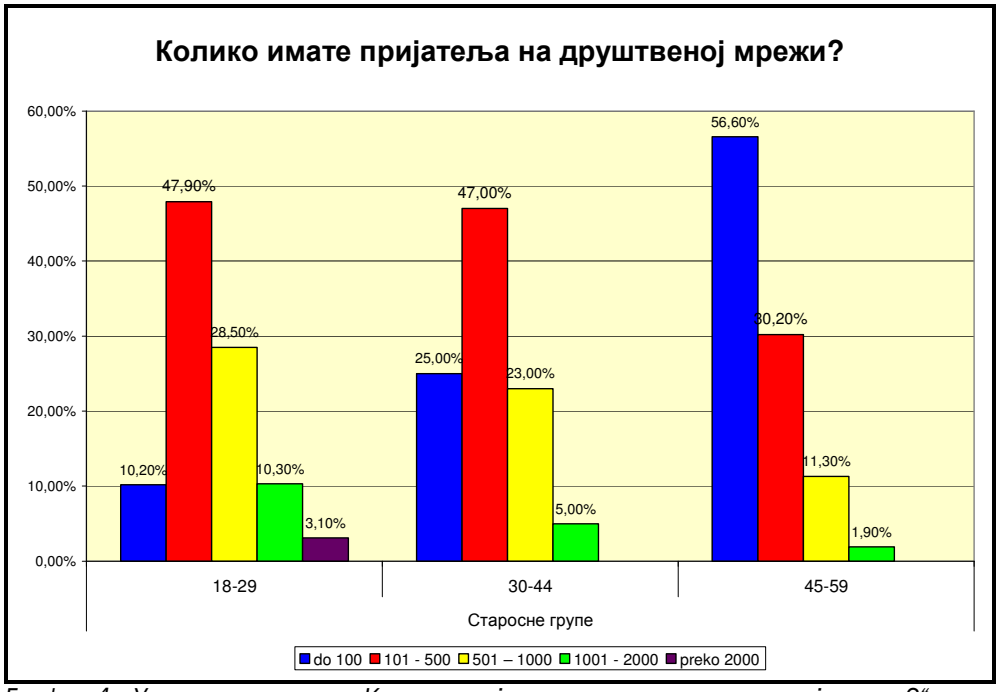


График 4. Укрштање питања „Колико пријатеља имате на друштвеној мрежи?“ са генерацијским групама

Табела 17. Колико сте он-лајн пријатеља раније познавали?

Колико сте он-лајн- пријатеља раније познавали?		Старосне групе		
		18-30	30-45	45-60
све		22,8%	21,8%	45,3%
већину		64,8%	64,4%	35,8%
неколико		8,2%	10,9%	15,1%
никога		4,2%	3,0%	3,8%
Тотал %		100,0%	100,0%	100,0%
N		960	101	53
Без 60+	x^2=21,083	V=0,10	p=0.002	

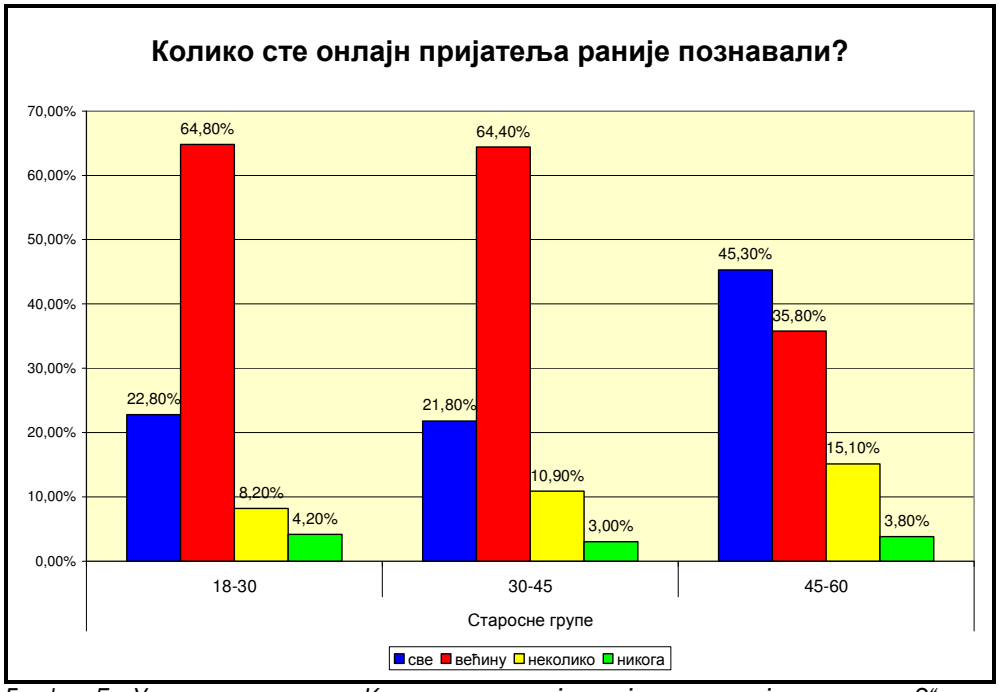


График 5. Укрштање питања „Колико сте он-лајн-пријатеља раније познавали?“ са генерацијским групама

При анализи коришћења друштвених мрежа у функцији градње социјалног капитала, свакако треба поћи од тога колико контката власници виртуелних профила имају на својим личним мрежама. Констатована је статистички значајна веза слабог интензитета између броја контаката на најчешће коришћеном интернет профилу и генерацијске припадности. Приметно је да поузданост закључка о јачини везе расте укључивањем у разматрање старијих од 60 година но, без обзирана то, она и даље остаје у границама слабе везе. Истраживањем из 2012. године дошло се до налаза да особе које имају више блиских пријатеља у реалном животу, у принципу, лакше успостављају и виртуелне контакте, те да кључну улогу за прибављање онлајн- контаката имају онлајн-платформе за друштвено умрежавање међу којима је, свакако, најзначајнији *Facebook* [55]. Већи број истраживања широм света сведочи о значају који у свакодневном животу, посебно младих, имају друштвене мреже међу којима *Facebook* сигурно предњачи. Социјални капитал се заиста на овај начин може скупљати на било ком пољу друштвеног живота[56], нпр. у

55 Петровић, Д. Томић-Петровић, Н. (2012): Интернет у функцији креирања друштвеног капитала његових корисника, XXX Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају – PosTel 2012, Саобраћајни факултет, Београд, стр. 87-96;

56 Burke, M. Kraut, R. and Marlow, C. (2011): “Social Capital on Facebook: Differentiating Uses and Users”, In Proceedings of the 29th ACM Conference on Human Factors in Computing Systems (CHI), Vancouver. p. 10;

политичком активизму[57] или друштвеној партиципацији[58], упознавању нових људи, учвршћивању задовољства животом и слично[59].

Увид у податке са табеле казује да су млађи склони да стварају широке мреже виртуелних познанстава док су старији у том погледу рестриктивнији, тако да сваки десети из скупине од 18 до 30 година старости има мање од сто контаката на својој мрежи, док је тај износ евидентиран код сваког четвртог из генерације 30-45 године и код нешто више од половине припадника генерације од 45 до 60 година. С друге стране, нешто испод половине млађих од 45 година има између 100 и 500 виртуелних контаката, док исти број има сваки трећи у генерацији од 45 до 60 година. За старије од 60 година немамо поуздане податке, с обзиром на то да је на ово питање одговарало само њих троје.

Подаци из табеле казују да старије генерације, кад већ почињу да се укључују у активности на друштвеним мрежама, показују слична интересовања као и млађи, али само слабијег интензитета. Једина разлика међу генерацијама је у склоности млађих да више времена проводе на друштвеним мрежама, па да у складу с тим тенденцијски успостављају већи број контаката. Оног тренутка када сајтови друштвених мрежа буду имали дужи „радни стаж“ на интернету моћи ћемо поузданије да тврдимо да ли се радни о тенденцији напуштања ових сајтова од стране старијих или се напросто ради о промени генерацијских образаца њиховог коришћења. За сада, друга претпоставка се чини реалнијом.

Такође, значајно питање за разумевање ове појаве је и то да ли су корисници профила на друштвеним мрежама познавали своје он-лајн пријатеље од раније. И овде се може констатовати статистички значајна веза слабог интензитета (V=0,10) са генерацијском припадношћу. С једне стране имамо млађе од 45 година од којих је сваки пети раније познавао све своје виртуелне контакте. а чак две трећине су познавале већину. Код старијих од 45 година је слика нешто другачија. Око половине њих је склапало виртуелна познанства само са онима које је познавала из реалног живота. док је сваки трећи у своју виртуелну мрежи примио и по неког непознатог. Генерално, врло мали број власника профила на друштвеним мрежама виртуелне контакте остварује са претежно непознатим особама.

---

57 Bor, S. E. (2013): Using Social Network Sites to Improve Communication Between Political Campaigns and Citizens in the 2012. Election, American Behavioral Scientist XX(X) 1–19. DOI: 10.1177/0002764213490698, http://abs.sagepub.com/content/early/2013/06/07/0002764213490698 (10.03.2014.).; Dickinson, T. (2008, March 20). The machinery of hope. Rolling Stone, 1048, 36–42; Stirland, S. L. (2007). ‘‘Open-source politics’’ taps Facebook for Myanmar protests. http://www.wired.com/politics/onlinerights/news/2007/10/myanmarfacebook (10.3.2014);

58 Valenzuela, S. Park, N. and Kee, K. (2009) “Is There Social Capital in a Social Network Site?: Facebook Use and College Students’ Life Satisfaction, Trust, andParticipation”, Journal of Computer-Mediated Communication, Vol. 14(4), pp. 875–901;

59 Ellison, N. B. Steinfield, C. and Lampe, C. (2007): “The benefits of Facebook "friends:" Social capital and college students' use of online social network sites”, Journal of Computer-Mediated Communication, Vol. 12(4), pp. 1143-1168;

Табела 18. Да ли сте се физички срели са неким кога сте упознали путем интернета?

Да ли сте се физички срели са неким кога сте упознали путем интернета?	Старосне групе		
	18-29	30-44	45-59
да	52,9%	45,3%	25,0%
не	47,1%	54,7%	75,0%
Тотал %	100,0%	100,0%	100,0%
N	980	106	60
Без 60+	x^2=18,924	V=0,13	p<0,000

Табела 19. Ако јесте, са колико?

Ако јесте, са колико?	Старосне групе		
	18-30	30-45	45-60
мање од 3	46,7%	51,0%	60,0%
3 – 20	38,9%	39,2%	25,0%
преко 20	14,3%	9,8%	15,0%
Тотал %	100,0%	100,0%	100,0%
N	552	51	20
Без 60+	x^2=2,532	V=0,05	p=0,639

На основу дистрибуције одговора, обрачунатим према старосним групама, на питање „да ли сте се физички срели са неким кога сте упознали преко интернета?“ може се закључити да постоји већа склоност млађих генерација да се лично упознају са онима са којима су претходно успоставили контакт путем интернета. Генерално, мерено Крамеровим V коефицијентом веза генерацијске припадности и склоности ка личном упознавању је слаба (V=0,13), али ипак статистички значајна.

Већина анкетираних има релативно мало искуства са упознавањем нових људи на овај начин. Од оних који су се одлучили да друге упознају на овај начин половина је то учинила једном до два пута. Више од три сусрета, али мање од двадесет остварило је око 40% њих, док је тек 10-15% испитаних који су ушли у оваква познанства остварило више од 20 контаката. Статистичка анализа казује да не постоји статистички значајна веза генерацијске припадности и броја упознатих особа.

Ранија истраживања, и у свету и код нас, казују да постоји релативно велика склоност људи да познанства из виртуелног света пренесу у реалан живот. Хоган и сарадници[60] утврђују да је то релативно универзална појава, а да се ово дешава широм света. Различите националне културе могу да дају тон динамици оваквих контаката али, у принципу, велики број корисника интернета и друштвених мрежа своје виртуелне контакте премешта у реалан живот и тиме обогаћује своје реалне (офлајн) контакте. Приказујући податке за осамнаест земаља они налазе да је најмање преношење контаката утврђено у Јапану (31,8%), а највеће у Бразилу (81,7%). У великом броју других истраживања је утврђена тенденција личног упознавања са он-лајн пријатељима која се креће у овим границама. Чак и код нас

60 Hogan, B. Li, N. Dutton,W. H. (2011):A Global Shift in the Social Relationships of Networked Individuals: Meeting and Dating Online Comes of Age. Oxford Internet Institute. http://blogs.oii.ox.ac.uk/couples/wp-content/uploads/2010/09/Me-MySpouse_GlobalReport_HoganLiDutton.pdf. (10.3.2014.);

је утврђено да се уживо[61] упознавало око три четвртине корисника сајтова, не само друштвених мрежа већ и он-лајн причаоница и сличних сајтова. Д. Петровић сматра да је овоме узрок, између осталог, и то што је физички простор Србије релативно мали тако да је код нас, за разлику од многих великих земаља, нпр. Америке, и из тог разлога могуће много лакше ступати у контакте са он-лајн-познаницима. Он наводи и чињеницу да је истраживање у Србији обављено на корисницима он-лајн-причаоница, док су у већини других земаља узорци били састављени од корисника различитих група за вести и форума где упознавање није примарни циљ виртуелне комуникације. Трећи разлог може бити везан за културолошки условљене различите обрасце друштвености на различитим просторима[62].

Намеће се закључак да је велики број људи склон ка упознавању са потпуно непознатим особама са којима је пре тога остварио контакт путем интернета. У овом можемо препознати и велики потенцијал за формирање виртуелног социјалног капитала, али и и велику опасност од злоупотреба оваквих познанстава. Релативно мали број познанстава, које је већина остварила, казује да су, и по овом критеријуму, интернет и друштвене мреже само потенцијани инструменти за изградњу социјалног капитала. Колико ће се они претворити у реалност, остаје да се види у годинама које долазе. Но, и поред различитих мишљења, реално је очекивати да ће овај начин комуникације обогатити праксу изградње социјалног капитала на различитим пољима свакодневног живата.

Табела 20. На који начин су друштвене мреже утицале на Ваш живот? (вишеструки избор)

На који начин су друштвене мреже утицале на Ваш живот?	18-30		30-45		45-60		60+	
нашао/ла сам посао	33	3,06%	3	1,89%	2	1,44%		
преселио/ла сам се у иностранство	14	1,30%	1	,63%				
нашао/ла сам животног партнера	25	2,32%	1	,63%	2	1,44%		
упознао/ла сам више партнера	74	6,86%	11	6,92%	1	,72%		
интензивнији ми је емотивни живот	51	4,73%	10	6,29%	1	,72%		
више комуницирам са пријатељима	576	53,38%	62	38,99%	24	17,27%	3	6,52%
упознао/ла сам више људи	315	29,19%	32	20,13%	10	7,19%	1	2,17%
све мање се виђам са пријатељима	106	9,82%	7	4,40%	4	2,88%	2	4,35%
прекинуо/ла сам неке контакте	71	6,58%	2	1,26%	2	1,44%		
нешто друго	99	9,18%	10	6,29%	11	7,91%		
N	1079 (1364)		159 (135)		139 (57)		46 (6)	

61 Петровић, Д. (2008): У међумрежју: Интернет и нови обрасци друштвености, Саобраћајни факултет, Институт за социолошка истраживања Филозофског факултета, Београд, стр. 140-148;

62 Петровић, Д. (2013): Друштвеност у доба интернета, Академска књига, Нови Сад, стр. 174;.

Табела 21. Крамерови V коефицијенти и мере значајности веза за питање „На који начин су друштвене мреже утицале на Ваш живот?“ са старосним групама

На који начин су друштвене мреже утицале на Ваш живот?	Старосне групе / сви			Без 60+		
	x^2	V	p	x^2	V	p
нашао/ла сам посао	3,074	0,05	0,380	1,714	0,04	0,424
преселио/ла сам се у иностранство	2,859	0,05	0,414	2,278	0,04	0,320
нашао/ла сам животног партнера	3,285	0,05	0,350	2,257	0,04	0,324
упознао/ла сам више партнера	11,373	0,09	0,010	8,064	0,08	0,018
интензивнији ми је емотивни живот	8,288	0,08	0,040	5,933	0,07	0,051
више комуницирам са пријатељима	101,356	0,27	0,000	70,283	0,23	0,000
упознао/ла сам више људи	48,200	0,18	0,000	34,181	0,16	0,000
све мање се виђам са пријатељима	12,658	0,09	0,005	11,517	0,09	0,003
прекинуо/ла сам неке контакте	15,481	0,10	0,001	12,444	0,10	0,002
нешто друго	6,001	0,07	0,112	1,575	0,03	0,455

Пун смисао коришћења друштвених мрежа у својству социјалног капитала се може препознати кроз ефекте њиховог утицаја на лични живот корисника. На бази података из табеле може се закључити да млађи од 30 година интензивније користе друштвене мреже те да код њих оне имају већи утицај на животна дешавања него код старијих. Више од половине њих више комуницира са пријатељима управо захваљујући друштвеним мрежама. Исто важи за сваког трећег припадника генерацијске кохорте 30-45 година старости. Поред овога сваки трећи сматра да му друштвени живот постаје богатији посредством упознавања нових пријатеља за шта се изјашњава и сваки пети из наредне генерацијске скупине. Исте одговоре даје и 17,27% (интензивнија комуникација са пријатељима) и 7,19% (упознавање са више људи) испитаника старости од 45 до 60 година. Старијих од 60 година, који су одговарали на ово питање, било је само шесторо те се њихови одговори не могу озбиљније искористити за аналитичку интерпретацију. Оно што се види из овако малог броја одговора јесте да друштвене мреже не остварују дубљи утицај на најстарије, већ да се он углавном оријентише ка интензивнијој комуникацији с пријатељима, односно да се отуђују од њих тако да се све мање виђају лицем у лице, што значи да се код најстаријих, највише због њихових година и слабије физичке кондиције, друштвене мреже могу појавити као вид супституције реалних сусрета виртуелном комуникацијом.

У овоме се може препознати извор потенцијалног социјалног капитала који може бити активиран у каснијим годинама. Кажемо потенцијалног јер се практична примена друштвених мрежа у функцији градње социјалног капитала само може назрети, али не и јасно препознати. Потврду овог става налазимо у чињеници да је само 3,06% млађих од 30 година успело да, захваљујући друштвеним мрежама, пронађе посао. Њима се придружује и 1,89% оних између 30 и 45 година и 1,44%

припадника најстаријег дела радног контигента. Потпуно је занемарљив број оних који су, захваљујући друштвеним мрежама, прешли у иностранство. Дакле, друштвене мреже носе велики потенцијал за решавање радних потреба својих корисника, али код нас тај потенцијал ни близу није искоришћен на адекватан начин. Тај потенцијал се користи искључиво за обликовање потенцијалног социјалног капитала посредством одржавања веза и контаката са људима са којима се те везе и контакти ионако одржавају у реалном животу.

Налази једног новијег истраживања (2012) обављеног у Србији показују да релативно велики број испитаника остварује висок виртуелни социјални капитал (39,8%)[63]. Корист од интернета је углавном била од добијања значајних информација и упознавања људи различитих професија. Разлику између ових налаза и резултата наших истраживања треба тражити у томе што је раније истраживање имало форму онлајн-истраживања, путем упитника стављеног на интернет. Уобичајено је да такве упитнике најчешће попуњавају лица која су у директном или индиректном контакту са истраживачима и да она због специфичности популације која им приступа немају репрезентативни карактер, већ пре могу послужити за тестирање методолошких инстумената.

Штавише, евидентан је значајно већи отуђујући потенцијал друштвених мрежа који је, опет, видљивији код најмлађег дела радног контигент, а с обзиром да се сваки десети изјашњава да се захваљујући њима све мање виђа са пријатељима док је њих 6,58% чак и прекинуло неке контакте. Дакле, друштвене мреже могу да остваре негативан утицај на животе својих корисника тако што ће, с једне стране, имати за последицу пребацивање социјалних интеракција из реалног у виртуелни друштвени простор и тиме смањити интензитет непосредне интерперсоналне комуникације односно, тиме што ће, с друге стране, омогућавањем већег протока информација, без обзира да ли су оне валидне или су намерно или ненамерно искривљене, довести до прекида постојећих интеракција.

Треба навести и да се један број млађих од 45 година изјашњава да им је емотивни живот на овај или онај начин постао богатији управо захваљујући контактима преко друштвених мрежа, што се може приписати њиховој релативној младости и биолошким поривима карактеристичним за тај животни период, те се ово не мора нужно повезати са изградњом социјалног капитала. Емотивно повезивање посредством друштвених мрежа је код старијих од 45 година спорадично.

И овде се може поставити питање да ли постоји значајна веза припадности старосној групи и последица које друштвене мреже могу да оставе на живот људи. Показало се да статистички значајна веза постоји код укрштања старости са следећих шест варијабли: упознавањем већег броја емотивних партнера, интензивнијим емотивним животом, већом комуникацијом са пријатељима, упознавањем већег броја људи, мањим виђањем са пријатељима и прекидањем контаката. Крамерови V коефицијенти указују на везе слабог интензитете. Највиша вредност V коефицијента је утврђена у укрштању старосне групе са више комуникације са пријатељима где је V=0,27 (у разматрање су укључени и старији од 60 година).

63 Петровић, Д. Томић-Петровић, Н. (2012): Интернет у функцији креирања друштвеног капитала његових корисника, XXX Симпозијум о новим технологијама у поштанском и телекомуникационом саобрацају – PosTel 2012, Саобраћајни факултет, Београд, стр. 87-96;

5. УМЕСТО ЗАКЉУЧКА - ФАКТОРСКА АНАЛИЗА КОРИШЋЕЊА ДРУШТВЕНИХ МРЕЖА

Пре отпочињања факторске анализе требало би проверити поузданост скале за мерење коришћења друштвених мрежа. Очекивано, нема негативних корелација међу посматраним ајтемима као што нема ни негативних бројева у табели ајтем-тотал статистика. На основу овога можемо закључити да се све посматране ставке уклапају у скалу и мере тражену релацију. То потврђује и вредност Кромбаховог коефицијента алфа) која у овом случају износи 0,87, што показује веома добру поузданост и сагласност скале за овај узорак.

Табела 22. Ајтем-тотал статистика

Item-Total Statistics	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Комуникација? са члановима породице	55,00	112,977	,412	,391	,864
Комуникација? са најближим пријатељима	55,87	114,947	,484	,450	,862
Комуникација? са дечком / девојком	55,05	110,849	,414	,279	,865
Комуникација? са *online*-пријатељима	54,50	108,580	,565	,412	,857
Комуникација? са познаницима	54,58	112,226	,533	,401	,859
Комуникација? са колегама и сарадницима	54,96	110,926	,505	,346	,860
Комуникација? са непознатима	53,28	114,801	,485	,430	,862
Сврха? (за зближавање са члановима породице)	54,39	108,656	,526	,604	,859
Сврха? (за зближавање са пријатељима)	54,83	107,442	,589	,604	,856
Сврха? (за проналажење „изгубљених“ рођака, пријатеља и познаника)	54,27	110,751	,485	,307	,861
Сврха? (за упознавање што више особа)	53,72	110,435	,590	,556	,857
Сврха? (за повезивање са особама сличних / истих интересовања)	54,00	110,049	,581	,530	,857
Сврха? (за посредовање)	53,38	114,432	,504	,454	,861
Сврха? (за остваривање емотивних веза)	53,35	113,069	,528	,501	,860
Сврха? (за проналажење посла)	53,43	115,336	,425	,323	,864
Сврха? (то је део мог посла)	53,32	114,349	,407	,321	,864
Сврха? (за „убијање времена“)	54,77	113,510	,392	,273	,865

Вредности корелираних „Item-total“ корелација, које показују степен корелације сваке ставке са укупним резултатом, веће су од 0,3. Штавише, све добијене вредности, осим за једну ставку (сврха коришћења друштвеним мрежа –

„убијање времена“), веће су од 0,4. Из исте табеле (последња колона) може се видети да се избацивањем појединих ставки из разматрања битно не мања вредност Кронбаховог алфа коефицијента и она, заокруживањем на две децимале, у сваком појединачном случају износи 0,86, што значи да су посматране ставке међусобно добро усаглашене.

С обзиром да је у вези са коришћењем друштвених мрежа анализирано седамнаест ставки, поставило се питање да ли се оне могу редуковати на мањи број фактора. Да бисмо дошли до одговора на ово питање извршили смо факторску анализу. Најјаснији резултати су добијени применом Облимин ротације. Наравно, пре уласка у факторску анализу неопходно је извршити оцену прикладности коришћених података за факторску анализу, с обзиром да је коришћени узорак био довољно велики да га можемо користити за анализу.

Табела 23. Корелациона матрица посматраних варијабли[64]

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1,00												
2	0,42	1,00											
3	0,37	0,49	1,00										
4	0,23	0,36	0,31	1,00									
5	0,18	0,29	0,25	0,46	1,00								
6	0,25	0,33	0,29	0,36	0,46	1,00							
7	0,04	0,04	0,15	0,38	0,39	0,27	1,00						
8	0,59	0,29	0,32	0,26	0,19	0,26	0,13	1,00					
9	0,46	0,47	0,38	0,34	0,30	0,35	0,11	0,72	1,00				
10	0,31	0,28	0,25	0,26	0,29	0,25	0,15	0,49	0,46	1,00			
11	0,18	0,18	0,25	0,44	0,36	0,20	0,46	0,29	0,38	0,38	1,00		
12	0,14	0,19	0,20	0,45	0,43	0,27	0,43	0,24	0,32	0,31	0,64	1,00	
13	0,10	0,10	0,18	0,29	0,28	0,20	0,43	0,18	0,19	0,26	0,51	0,55	1,00
14	0,14	0,09	0,25	0,32	0,26	0,19	0,50	0,21	0,23	0,20	0,58	0,46	0,51
15	0,17	0,08	0,11	0,18	0,21	0,23	0,38	0,16	0,17	0,21	0,34	0,37	0,43
16	0,10	0,14	0,11	0,24	0,26	0,28	0,39	0,19	0,19	0,18	0,34	0,32	0,39
17	0,11	0,31	0,23	0,37	0,35	0,27	0,21	0,11	0,30	0,22	0,26	0,30	0,18

64 Varijable uključene u faktorsku analizu su:
1. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa članovima porodice;
2. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa najbližim prijateljima;
3. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa dečkom/devojkom;
4. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa online prijateljima;
5. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa poznanicima;
6. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa kolegama i saradnicima;
7. Sa kim komunicirate putem drustvenih mreza (i koliko)? sa nepoznatima;
8. U koje svrhe koristite ove sajtove? (za zbližavanje sa članovima porodice);
9. U koje svrhe koristite ove sajtove? (za zbližavanje sa prijateljima);
10. U koje svrhe koristite ove sajtove? (za pronalaženje „izgubljenih“ rođaka, prijatelja i poznanika);
11. U koje svrhe koristite ove sajtove? (za upoznavanje što više osoba);
12. U koje svrhe koristite ove sajtove? (za povezivanje sa osobama sličnih / istih interesovanja);
13. U koje svrhe koristite ove sajtove? (za posredovanje);
14. U koje svrhe koristite ove sajtove? (za ostvarivanje emotivnih veza);
15. U koje svrhe koristite ove sajtove? (za pronalaženje posla);
16. U koje svrhe koristite ove sajtove? (to je deo mog posla);
17. U koje svrhe koristite ove sajtove? (za „ubijanje vremena“);

Табела 23а.Корелациона матрица посматраних варијабли (наставак)

	14	15	16	17
14	1,00			
15	0,35	1,00		
16	0,33	0,42	1,00	
17	0,14	0,19	0,07	1,00

На основу података из корелационе матрице се види да имамо прихватљив број интерајтемских корелација већих од 0,30, те да су податци и по овом критеријуму подобни за анализу.

Оправданост примене факторске анализе је тражена и посредством Бартеловог теста сферичности који се показао значајним (на нивоу p<0,000). Такође је и Кајзер-Мејер-Олкинов показатељ адекватности узорка потврдио адекватност података. (KMO=0,864).

Табела 24. Заједнички варијабилитети (Communalities)

Communalities	Initial	Exctraction
Са ким комуницирате путем друштвених мрежа (и колико)? са члановима породице	1,000	,591
Са ким комуницирате путем друштвених мрежа (и колико)? са најближим пријатељима	1,000	,578
Са ким комуницирате путем друштвених мрежа (и колико)? са дечком/девојком	1,000	,412
Са ким комуницирате путем друштвених мрежа (и колико)?са *online*-пријатељима	1,000	,544
Са ким комуницирате путем друштвених мрежа (и колико)? са познаницима	1,000	,577
Са ким комуницирате путем друштвених мрежа (и колико)? са колегама и сарадницима	1,000	,434
Са ким комуницирате путем друштвених мрежа (и колико)? са непознатима	1,000	,565
У које сврхе користите ове сајтове? (за зближавање са члановима породице)	1,000	,772
У које сврхе користите ове сајтове? (за зближавање са пријатељима)	1,000	,699
У које сврхе користите ове сајтове? (за проналажење „изгубљених“ рођака, пријатеља и познаника)	1,000	,441
У које сврхе користите ове сајтове? (за упознавање што више особа)	1,000	,624
У које сврхе користите ове сајтове? (за повезивање са особама сличних / истих интересовања)	1,000	,591
У које сврхе користите ове сајтове? (за посредовање)	1,000	,592
У које сврхе користите ове сајтове? (за остваривање емотивних веза)	1,000	,560
У које сврхе користите ове сајтове? (за проналажење посла)	1,000	,408
У које сврхе користите ове сајтове? (то је део мог посла)	1,000	,375
У које сврхе користите ове сајтове? (за „убијање времена“)	1,000	,473

Extraction Method: Principal Component Analysis.

На основу података из табела заједничких варијабилитета се види да ставка „у које сврхе користите ове сајтове (то је део мог посла)“ има најнижи варијабилитет (0,375). Ради се о довољно високом варијабилитету (вишем од 0,3) што нам казује

да се све посматране ставке добро уклапају у своју компоненту са осталим ставкама.

Табела 25. Објашњење укупне варијансе

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	5,658	33,283	33,283	5,658	33,283	33,283	4,358
2	2,248	13,221	46,504	2,248	13,221	46,504	3,540
3	1,330	7,823	54,327	1,330	7,823	54,327	3,660
4	,987	5,805	60,132				
5	,874	5,139	65,271				
6	,785	4,620	69,891				
7	,655	3,855	73,745				
8	,617	3,628	77,374				
9	,586	3,445	80,819				
10	,544	3,201	84,020				
11	,492	2,891	86,911				
12	,463	2,726	89,637				
13	,460	2,708	92,345				
14	,415	2,444	94,789				
15	,393	2,309	97,098				
16	,303	1,784	98,881				
17	,190	1,119	100,000				

Extraction Method: Principal Component Analysis.
a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

На бази ових показатеља смо закључили да су коришћени податци прихватљиви за факторску анализу. У следећем кораку анализом су екстрахована три фактора који задовољавају Кајзеров критеријум, тј. чија је карактеристична вредност изнад 1 и који кумулативно покривају 54,33% варијансе.

График 6. Дијаграм превоја

Потврду да су добијени фактори релевантни тражили смо посредством дијаграма превоја који се закривљује и прелази у хоризонталну линију код четврте компоненте (на X оси) чиме се потврђује да се претходне три компоненте могу сматрати валидним факторима. На основу овога смо закључили да су екстраховани фактори валидни за анализу, те да се посматрана скала може редуковати на њих.

Табела 26. Матрица компоненти „Component Matrix“

Component Matrix[a]	Component		
	1	2	3
Сврха? (за упознавање што више особа)	,724		
Сврха? (за повезивање са особама сличних/истих интересовања)	,703	-,311	
Сврха? (за зближавање са пријатељима)	,650	,488	
Комуникација (и колико)? са *online*-пријатељима	,649		,351
Комуникација (и колико)? са познаницима	,612		,448
Сврха? (за посредовање)	,607	-,435	
Сврха? (за остваривање емотивних веза)	,602	-,396	
Сврха? (за зближавање са члановима породице)	,571	,491	-,453
Комуникација (и колико)? са непознатима	,568	-,487	
Сврха? (за проналажење „изгубљених“ рођака, пријатеља и познаника)	,554		
Комуникација (и колико)? са колегама и сарадницима	,547		,336
Комуникација (и колико)? са дечком/девојком	,506	,371	
Сврха? (за проналажење посла)	,503	-,334	
Сврха? (то је део мог посла)	,501	-,316	
Комуникација (и колико)? са члановима породице	,467	,549	
Комуникација (и колико)? са најближим пријатељима	,495	,512	
Сврха? (за „убијање времена“)	,460		,505

Extraction Method: Principal Component Analysis.
a. 3 components extracted.

Табела 27. Матрица обрасца „Patern Matrix“

Pattern Matrix[a]	Component		
	1	2	3
Сврха? (за посредовање)	,774		
Сврха? (за остваривање емотивних веза)	,746		
Сврха? (за упознавање што више особа)	,701		
Комуникација (и колико)? са непознатима	,683		
Сврха? (за повезивање са особама сличних/истих интересовања)	,650		
Сврха? (за проналажење посла)	,643		
Сврха? (то је део мог посла)	,606		
Сврха? (за зближавање са члановима породице)		,887	
Комуникација (и колико)? са члановима породице		,773	
Сврха? (за зближавање са пријатељима)		,751	
Сврха? (за проналажење „изгубљених“ рођака, пријатеља и познаника)		,578	
Сврха? (за „убијање времена“)			,715
Комуникација (и колико)? са познаницима			,694
Комуникација (и колико)? са *online*-пријатељима			,619
Комуникација (и колико)? са колегама и сарадницима			,590
Комуникација (и колико)? са најближим пријатељима		,413	,566
Комуникација (и колико)? са дечком/девојком		,392	,413

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 8 iterations.

Табела 28. Структурна матрица

Structure Matrix	Component		
	1	2	3
Сврха? (за посредовање)	,769		
Сврха? (за упознавање што више особа)	,765	,333	,383
Сврха? (за остваривање емотивних веза)	,746		
Сврха? (за повезивање са особама сличних/истих интересовања)	,734		,461
Комуникација (и колико)? са непознатима	,713		,376
Сврха? (за проналажење посла)	,633		
Сврха? (то је део мог посла)	,611		
Сврха? (за зближавање са члановима породице)		,865	
Сврха? (за зближавање са пријатељима)		,818	,435
Комуникација (и колико)? са члановима породице		,767	
Сврха? (за проналажење „изгубљених“ рођака, пријатеља и познаника)	,345	,627	
Комуникација (и колико)? са познаницима	,421		,732
Комуникација (и колико)? са *online*-пријатељима	,440		,705
Сврха? (за „убијање времена“)			,683
Комуникација (и колико)? са колегама и сарадницима		,325	,648
Комуникација (и колико)? са најближим пријатељима		,560	,631
Комуникација (и колико)? са дечком / девојком		,522	,528

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

Табела 29. Табела Матрица факторских корелација

Component Correlation Matrix

Component	1	2	3
1	1,000	,211	,336
2	,211	1,000	,346
3	,336	,346	1,000

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

У структурној матрици, која је добијена Облимин ротацијом, дате су корелације посматраних варијабли са екстрахованим факторима. Ова матрица приказује добру повезаност издвојених варијабли са припадајућим факторима. Тамо где је нека ставка у значајној корелацији (изнад 0,30) са добијеним факторима, најчешће је међу приказаним корелацијама видљива значајна разлика чиме се показује да дата ставка доминантно припада једном фактору. Матрица факторских корелација указује на умерену повезаност између фактора.

Матрица компоненти не приказује на најјаснији начин структуру добијених фактора, те смо применили Облимин ротацију која је дала много јасније резултате и готово недвосмислено показала три јасно издвојена фактора. Анализом факторских тежина појединачних компоненти можемо именовати екстраховане факторе тако да смо први фактор назвали фактором секундарних веза, други смо назвали фактором примарних веза и трећи је фактор забаве или фактор опуштених комуникација.

У првом фактору, фактору секундарних веза доминирају потребе за разним врстама посредовања, тражење партнера за остваривање емотивних веза, упознавање нових људи, комуникација са непознатима, повезивање са особама истих или сличних интересовања, тражење или обављање посла. Овај фактор покрива 33,28% варијансе, те се може закључити да трећина комуникација посматране популације има као циљ успостављање секундарних веза посредством повезивања на друштвене мреже. Практично, социјални капитал има највећу вредност ако омогућава повезивање људи сличних интересовања. Секундарне везе се остварују ван круга породице и блиских пријатеља и оне, у својој позадини, најчешће имају рационалне интересе.

Равнотежу овог фактора донекле ремети компонента везана за остваривање емотивних веза која би, по логици ствари, пре требало да припада другом фактору. Међутим, можемо претпоставити да ова врста упознавања преко друштвених мрежа, због социјалног контекста обојеног релативним неповерењем у блиске контакте путем посредујућих медија типа интернета, нема усмереност ка примарним комуникацијама.

У контексту овог фактора, реч је о томе да појединци ступају у међусобне односе са другим људима да би на основу заједничких вредности остварили социјалне интеракције и на бази њих градили социјалне мреже које имају вредност, која се не огледа само на емоционалном плану већ и у врло конкретним користима које су резултат поверења, узајамности, размене информација и сарадње повезаних у друштвене мреже. Овде је испуњен услов да се социјални капитал схвата као систем социјалних мрежа и норми, насталих редовним социјалним интеракцијама, које олакшавају акцију појединаца и група унутар шире заједнице или друштва, односно као друштвени (заједнички) ресурс који олакшава/отежава приступ другим ресурсима, односно потенцијално повећава компаративну предност

у односу на оне који нису чланови мрежа. У крајњој линији, овако конципиран социјални капитал је израз личног (и друштвеног) поверења и представља везу која омогућава групну координацију и сарадњу ради постизања индивидуалне (или групне) користи. У другом фактору, фактору примарних комуникација, налазе се потреба за зближавањем и комуникацијом са члановима породице и родбином, за зближавањем са пријатељима и проналажење рођака, пријатеља и познаника са којима су се готово изгубили контакти. Овај фактор покрива 13,22% варијансе. Овде се, додуше са малом али ипак прихватљивом факторском тежином, налазе и комуникација са најближим пријатељима и емотивним партнерима, које су са нешто значајнијим факторским засићењем присутне и у трећем фактору. Други фактор се концентрише ка мање значајној форми социјалног капитала који се гради унутар примарних група и који, као своју кључну одредбу, има емоционалну, материјалну и физичку подршку унутар примарних група, односно унутар круга релативно блиских сродника и најближих пријатељима са којима се, у принципу, успоставља интеракција лицем у лице.

У контексту овог фактора се може констатовати да за социјални капитал, који се гради унутар примарних веза, није битно то да он обухвата све врсте односа међу социјално дистанцираним појединцима који, независно од присуства или одсуства међусобне блискости, деле заједничке интересе, норме и вредности у којима се акценат ставља на апстрактне нормативне и вредносне стране међусобног поверења, већ да су за њега значајне све приватне мреже и везе примарног типа као што су везе са пријатељима и породицом. У том смислу основ поверења могу бити не само пословни и слични интереси, већ и различити облици солидарности као што су породична, политичко-идеолошка, религијска, интересна, унутаргрупна у било ком значењу те речи. Овде се ради о типу социјалног капитала који се показао актуелним код нижих друштвених слојева, ниже образованог и руралног дела становништва који ослонац за разне личне и друштвене активности тражи и налази у породици, суседству или у ужој локалној заједници. Социјални капитал у овом сегменту комуникација пре има форму социјалне и емоционалне подршке блиских него интересне повезаности социјално удаљених појединаца

У трећем фактору (забава и опуштене комуникације са мање битним особама који покрива 7,23% варијансе), највећу факторску тежину има компонента потребе за „убијањем времена“. Ту се такође налазе и комуникације са мање битним особама, а са мањим факторским тежинама комуникације са блиским пријатељима и емотивним партнерима. Већ је констатовано да ове две последње компоненте имају прихватљиву факторску тежину и за други и за трећи фактор, с тим да су веће вредности у случају трећег фактора, те их првенствено треба гледати као компоненте трећег фактора.

Овај фактор генерално, није у функцији изградње и обликовања социјалног капитала, мада и необавезна комуникација може да представља потенцијал за његово формирање, посебно ако се она остварује са школским друговима, колегама са посла или из струке. Управо је ова ставка - комуникација са колегама и сарадницима показала значајно факторско засићење у трећем фактору, те се може претпоставити да се ова категорија често третира као шири круг познаника и мање актуелних пријатеља са којима се успоставља непродуктивна комуникација, непродуктивна у смислу изградње социјалног капитала ради завршавања различитих послова. Оваквом стању сигурно у извесној мери доприноси и чињеница да друштвене мреже много више користе млађе генерације него старије,

те да већина младих још увек није ушла у радни процес. Стога категорија колега и сарадника пре подразумева школске другове и мање блиске пријатеље него потенцијалне сараднике са којима се остварују везе и контакти ради задовољавања интереса, који потичу из секундарних облика груписања. Из ранијих анализа се може закључити да у овом фактору претежно учествују комуникације најмлађе посматране генерацијске скупине, и то је кључни разлог зашто се ставка комуникације са колегама и сарадницима нашла у релативно високом факторском засићењу унутар трећег, а не унутар првог фактора.

С друге стране и насупрот претходној констатацији, у оквиру овог фактора можемо наћи и елементе који указују на потенцијал за активирање тзв. тамне стране социјалног капитала. Познаници, колеге и сарадници и тзв. он-лајн пријатељи могу бити база на основу које се могу градити разне затворене групе, групе клановског типа, које имају потребу за одржавањем редовне комуникације ради обављања активности с друге стране закона. Разне криминалне групе којима су интернет и друштвене мреже потребни као инструмент повезивања са сарадницима на релативно удаљеним тачкама на терену, успевају да одрже комуникацију која и каква је до скора, из техничких разлога, била немогућа. Сада нова технолошка решења, посебно смарт телефони и мобилни интернет, активиран преко лаптоп и таблет рачунара, омогућавају брзу комуникацију, али и повећану мобилност, правовремено добијање информација о разним аспектима стања на терену. Захваљујући томе, они који се баве разним облицима кријумчарења, укључујући и кријумчарење људи, секс трафикинг, радну експлоатацију и слична кривичним делима, успевају да се лако повежу и организују, укључујући ту и обмањивање многих који им се препуштају са поверењем очекујући да ће им везе са таквим сојем људи помоћи у решавању неких егзистенцијалних проблема.

Евидентно је да скоро 18% млађих од 30 година остварује редовну или повремену комуникацију са непознатима. У контексту злоупотреба друштвених мрежа ова група корисника друштвених мрежа је потенцијално најугроженији од стране оних који друштвене мреже користе да би намамили жртве за своје криминалне намере. Посматрано према полу, овакву врсту комуникације практикује увек, често или понекад 9,8% жена и 24,1% мушкараца. Крамеров V коефицијент унутар те старосне скупине је мали, али ипак статистички значајан ($V=0,19$; $p<0,000$). Можемо претпоставити да се понекад жртве, нарочито унутар млађе женске популације, саме налазе унутар понуде на подземном тржишту људи, сексуалних услуга или лажних пословних понуда, најчешће са сасвим другачијим намерама или наивним поверењем у онлајн-пријатеље који се често укључују на велики број профила и тиме аутоматски и без икакве провере постају пријатељи пријатеља и понекад задобијају поверење без претходне провере. Мали је корак да се од безазлене игре или наивног поверења упадне у замке организованог криминала.

ЛИТЕРАТУРА

1. Baron, S. Field, J. and Schuller, T. (eds) (2000): Social Capital: Critical Perspectives, Oxford University Press.
2. Beck, U. (1992): Risk Society: Towards a New Modernity, Newbury Park, Calif; Sage Publications. London.
3. Bor, S. E. (2013): Using Social Network Sites to Improve Communication Between Political Campaigns and Citizens in the 2012 Election, American Behavioral Scientist XX(X) 1–19. DOI: 10.1177/0002764213490698 http://abs.sagepub.com/content/early/2013/06/07/0002764213490698 (10.03.2014.)
4. Bourdieu, P. (1986): „The Forms of Capital", u Richardson, J. G. (ed): Handbook of Theory and Research for the Sociology of Education, New York: Greenwoos Press, p. 241-258.
5. Boyd, D. (2008). Can social network sites enable political action? International Journal of Media and Cultural Politics, 4(2), 241–244.
6. Boyd, D.; Ellison, N. (2008): Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication. 13 (1), 210–230. http://jcmc.indiana.edu/vol13/is sue1/boyd.ellison.html (10.3.2014)
7. Brain, J.L. (1977). Sex, Incest, and Death: Initiation Rites Reconsidered, CurrentAnthropology, vol. 18, no. 2. pp. 191-208.
8. Burke, M.; Kraut, R. and Marlow, C. (2011): "Social Capital on Facebook: Differentiating Uses and Users", In Proceedings of the 29th ACM Conference on Human Factors in Computing Systems (CHI), Vancouver. p. 10.
9. Caplan, S. (2007). Relations among loneliness, social anxiety and problematic Internet use. CyberPsychology & Behavior, 10, 234– 242.; Chak, K. & Leung, L. (2004). Shyness and locus of control as predictors of Internet addiction and Internet use. CyberPsihology and Behavior, 7, 559– 570.
10. Castells, M. (2000): The Information Age: Economy, Society and Culture. Vol. 1, The Rise of the Network Society, Malden, MA: Blackwell Publishers, Inc. Oxford.
11. Castells, M. (2000a) Uspon umreženog društva, Golden marketing, Zagreb
12. Castells, M. (2004) ": A Theoretical Blueprint", in Castells M. (ed.), The Network Society: A Cross-cultural Perspective, Northampton, MA: Edward Elgar.
13. Chak, K. & Leung, L. (2004). Shyness and Locus of Control as Predictors of Internet Addiction and Internet Use. CyberPsihology and Behavior, 7, 559– 570.
14. Chambers, S. and Kopstein, J. (2001): „Bad Civil Society", Political Theory, vol. XXIX, No. 6, p. 837-865.
15. Coleman, J. (1990), Foundations of Social Theory, Cambridge, Harvard University Press.
16. Coleman, J. S. (1988), „Social capital in the creation of human capital", The American Journal of Sociology, vol. XCIV. Supllement, p. 94-120.
17. Dickinson, T. (2008, March 20). The machinery of hope. Rolling Stone, 1048, 36–42.;
18. Ellison, N. B.; Steinfield, C. and Lampe, C. (2007): "The benefits of Facebook "friends:" Social capital and college students' use of *online* social network sites", Journal of Computer-Mediated Communication, Vol. 12(4), pp. 1143-1168.
19. Eltantawy, N. Wiest, J. B. (2011), Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory, International Journal of Communication 5, pp. 1207–1224.
20. Farr, J. (2004): „Social Capital: A Conceptual History", Political Theory, Vol. 32, No. 1, pp. 6-33.
21. Foley, M. W. and Edwards, B. (1997): „Escape from Politics? Social Theory and the Social Capital Debate", American Behavioral Scientist, Vol, 40. No. 5, pp. 550-561.
22. Foley, M. W. and Edwards, B. (1998): „Beyond Tocqueville: Civil Society and Social Capital in Comparative Perspective", American Behavioral Scientists, vol. XLI No. 1. pp. 5-20.
23. Фрејзер, Џ. Џ. (1992), Златна грана: проучавање магије и религије, БИГЗ, Београд.
24. Giddens, A. (1991): The Consequences of Modernity, Cambridge: Polity, Press, Cambridge.

25. Grix, J. (2001): „Social Capital as a Concept in Social Sciences: The Current State of the Debate“, Democratization, vol.VIII, No. 3. pp. 189-210.
26. Hanifan, L. J. (1916): “The Rural School Community Center” Annals of the American Academy, of Political and Social Science No. 67. pp. 130-138.
27. Hogan, B. Li, N. Dutton,W. H. (2011):A Global Shift in the Social Relationships of Networked Individuals: Meeting and Dating *Online* Comes of Age. Oxford Internet Institute. http://blogs.oii.ox.ac.uk/couples/wp-content/uploads/2010/09/Me-MySpouse_GlobalReport_HoganLiDutton.pdf (10.3.2014).
28. Jochen, P., Valkenburg, P. M. & Schouten, A. P. (2005). Developing a model of adolescent friendship formation on the Internet. CyberPsychology and Behavior,8, pp. 423-430;
29. Kaplan, A. M. i Haenlein, M. (2010): Users of the world, unite! The challenges and opportunities of social media, Business Horizons, Vol. 53, Issue 1. pp. 59-68.
30. Lindsay, B., R. (2011): Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, CRS Report for Congress, Congressional Research Service, pp. 1-13 http://www.infopuntveiligheid.nl/Infopuntdocumenten/R41987.pdf (10.3.2014).
31. Matić, D. (2000): „Demokracija, povjerenje i socijalna pravda“, Revija za sociologiju, vol. XXXI, 3-4, str. 183-195.
32. Миладиновић, С. (1993): Вертикална друштвена покретљивост у Југославији. Социологија, vol. 35, бр. 2, стр. 263-281.
33. Миладиновић, С. (2003): Обрасци формирања и репродукције владајућих елита у бившој Југославији I - вертикална покретљивост, Социологија, вол. 45, бр. 1, стр. 33-60.
34. Миладиновић, С.: (2003) “Обрасци формирања и репродукције владајућих елита у бившој Југославији II - канали вертикалне покретљивости - образовање и политичка активност”, Социологија, вол. 45, бр. 4, стр. 347-376.;
35. Миладиновић, С. (2004): “Друштвена покретљивост као фактор глобалне друштвене конкурентности”, у Матејић, В. (ур): Технологија, култура и развој X, Удружење "Технологија и друштво", Институт "Михајло Пупин", Центар за истраживање развоја науке и технологије, Београд, стр. 147-156.
36. Миладиновић, С. (2006): „Проблем тумачења резултата истраживања друштвене (структуре и) покретљивости: идеја социјалног и културног капитала” у Немањић, М. и Спасић, И. (ур): Наслеђе Пјера Бурдијеа – поуке и надахнућа, Институт за филозофију и друштвену теорију, Завод за проучавање културног развитка, Београд, стр. 123-136.
37. Миладиновић, С. (2008): Друштво у раскораку, Нова српска политичка мисао, Београд.
38. Миладиновић, С. (2011): „Тамна страна социјалног капитала”, Нова српска политичка мисао, 3-4. вол XIX, стр. 287-316.
39. Miladinović, S. (2012): Two Faces of Social Capital in Structural Trends: Bonding and Bridging. In Cvetičanin, P. & Birešev, A. (eds): Social and Cultural Capital in Western Balkan Societies, Centre for Empirical Cultural Studies of South-East Europe and the Institute for Philosophy and Social Theory of the University of Belgrade, Belgrade, p. 59-74.
40. Милошевић, Б. (2013): Социјалне мреже и Арапско пролеће, CM: Communication Management Quarterly: Часопис за управљање комуницирањем 27 (VIII), str. 91–108.
41. Mislove, A.; Marcon, M.; Gummadi, K. P; Druschel, P.; Bhattacharjee, B.: (2007). Measurement and analysis of *online* social networks. Internet Measurement Conference 2007, October 24-26, 2007. San Diego, CA, USA. pp. 1-14. http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf (10.3.2014).
42. Montagnese, A. (2012): Impact of Social Media on National Security, Research Paper, Centro Militare di Studi Strategici, Rome. Pp. 1-36. http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Documents/Ricerche/2012/Stepi/social_media_20120313_0856.pdf (10.3.2014)
43. Петровић, Д (2007): „Од друштвених мрежа до умреженог друштва: један осврт на макро мрежни приступ у социологији“. Социологија, Вол. XLIX (2007), N° 2. стр. 174-175.

44. Петровић, Д. (2008): У међумрежју: Интернет и нови обрасци друштвености, Саобраћајни факултет, Институт за социолошка истраживања Филозофског факултета, Београд.
45. Петровић, Д. (2013): Друштвеност у доба Интернета, Академска књига, Београд.
46. Петровић, Д.; Томић-Петровић, Н. (2012): Интернет у функцији креирања друштвеног капитала његових корисника, XXX Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају – PosTel 2012, Саобраћајни факултет, Београд, стр. 87-96.
47. Portes, A. and Landolt, P. (1996): „The Downside of Social Capital“, The American Prospect, vol. VII 26, p. 18-22.; Chambers, Simone and Kopstein, Jeffrey. (2001): „Bad Civil Society“, Political Theory, vol. XXIX, No. 6, pp. 837-865.
48. Portes, A.: (1998): „Social Capital: Its Origins and Applications in Modern Sociology“, Annual Reviews of Sociology, vol. XXIV, 1. p. 1- 24.
49. Putnam, R. (1995), „Tuning In, Tuning Out: The Strange Disappearance of Social Capitalin America“, Political Science and Politics, vol. XXVIII. 4. pp. 664-683.
50. Putnam, R. (2000): Bowling Alone: The Collapse and Revival of American Community, New York: Simon and Schuster.
51. Putnam, R. D., Leonardi R. i Nanetti R. Y. (1993): Making democracy work: Civic Tradition in Modern Italy, Princeton: Princeton University Press.
52. Радовановић, Д. (2010): Интернет парадигма, структура и динамика онлајн друштвених мрежа: Фејсбук и млади у Србији, Панчевачко читалиште 17 (новембар). Стр. 21-22.
53. Републички завод за статистику, (2013), Употреба информационо-комуникационих технологија у Републици Србији, саопштење за јавност, 23 .09. 2013. стр. 3. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/14/03/PressICT2013.pdf (10.3.2014)
54. Selwyn, N (2012): 'Social Media in Higher Education', The Europa World of Learning. pp.1-10. http://www.educationarena.com/pdf/sample/sample-essay-selwyn.pdf (10.3.2014)
55. Valenzuela, S. Park, N. and Kee, K. (2009) "Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, andParticipation", Journal of Computer-Mediated Communication, Vol. 14(4), pp. 875–901.
56. Врањеш, А. (2013): Однос друштвених мрежа и грађанске партиципације на примјеру "арапског пролећа", Политеиа, vol. III, (5), str.111-119.
57. Wellman, B. (1988.). Structural analysis: From method and metaphor to theory and substance. in: Wellman,B., Berkowitz S.D. (eds), Social Structures: A Network Approach. Cambridge, UK: Cambridge University Press. pp. 19-61.
58. Widyanto, L. & McMurran, M. (2004). The psychometric properties of the Internet addiction test. CyberPsychology & Behavior, 7, pp. 443-450.
59. Wilson, C. Dunn, A. (2011), Digital Media in the Egyptian Revolution: Descriptive Analysis from the Tahrir Data Sets: International Journal of Communication 5, pp. 1248–1272.

Светлана Јовановић
Универзитет у Београду, Факултет организационих наука

ПРИВАТНОСТ И ЗАШТИТА ПОДАТАКА НА ИНТЕРНЕТУ

Садржај

Графици

Табеле

1. ПРАВО НА ПРИВАТНОСТ

1.1 Концепт приватности

У доба Интернета, смарт телефона и друштвених мрежа, једноставно је делити и пронаћи разне податке о личности. Можда и превише лако. Нечији захтев за кредит може бити одбијен јер комшилук није адекватан, фотографије објављене на мрежи често су доказ против појединца, а многобројни сајтови зарађују продајући податке својих корисника. Европска унија већ неколико година ради на изради и усаглашавању права која гарантују заштиту података о личности, како би свако могао да сачува своју приватност.

Тренутно важећа Директива о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података[65] израђена је давне 1995. године и захтева ажурирање у складу са технолошким променама. Европска комисија је предложила у јануару 2012. године нову уредбу са скупом правила за податке прикупљене на мрежи, како би се осигурала њихова безбедност и како би се обезбедило пословање са јасним оквиром за обраду тих података. Циљ је да се усвоји закон пре следећих европских избора у пролеће 2014. године.

Многа истраживања потврђују јаку привржености јавности према прописима који штите приватност. Јавност подржава принцип да је индивидуа једини власник својих приватних података и да она мора да дâ пристанак на одавање тих информација, а не обрнуто, да су подаци о личности јавне, али да индивидуа може да их ограничи. Истраживање групе *BusinessWeek/Harris Poll* из марта 2010. године показало је да 86% корисника жели да се на веб-страницама тражи дозвола од појединаца пре него што прикупе њихова имена, адресе, телефонске бројеве или финансијске информације. Исто истраживање показало је да 88% корисника подржава идеју да власници портала морају да питају корисника пре него што поделе неке његове податке са трећом страном. Друга слична истраживања потврђују ове резултате. Још 1991. године *Time-CNN* анкета показала је да 93% испитаника верује да компаније треба да добију дозволу пре него што дају приватне информације[66].

Са друге стране, појединци желе и безбедност својих података. Они желе могућност да добију надокнаду ако им се приватност наруши. Истраживање групе *Pew Internet & American Life* из августа 2012. године показало је да 94% интернет корисника мисли да се напад на нечију приватност мора санкционисати. У фебруару 2012. године *Harris Poll* је у истраживању показао да 84% испитаника сматра да се приступ информацијама мора ограничити и обезбедити.

Истраживањем које је спровео Центар за истраживање *PEW*[67] утврђено је да већина корисника мобилних телефона деинсталира или избегава апликације које угрожавају њихову приватност. Према извештају, 54% корисника мобилних телефона одлучило је да не инсталира апликацију након откривања колико се

65 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Officially Journal of the European Communities, no. L281, 1995;

66 *Public Opinion on Privacy*, Electronic Privacy Information Center, available at http://epic.org/privacy/, 03.11.2013;

67 Pew Research Center, http://www.pewinternet.org/Topics, 20.1.2014;

информација при томе чува и обрађује, а 30% корисника мобилних телефона деинсталира апликацију када схвате које све податке прикупља. Истраживање је открило да корисници постају активнији у управљању својих профила на друштвеним мрежама.

Истраживања у овој области показала су да испитаници желе јасну законску регулативу а не саморегулацију, важна им је анонимност, не слажу се са праксом праћења понашања на интернету и прављења профила корисника, нарочито када су подаци о личности повезани са профилом, не верују компанијама да ће на законит начин руковати подацима и плаше се злоупотреба од стране и приватног и јавног сектора, подржавају потребу за приватношћу, нису упознати са методама праћења корисника на интернету, као ни са пословним праксама прикупљања података о личности.

Многима је приватност веома важна. Она представља једно од основних људских права које се сме ускратити једино због безбедности и јавног добра. Али већина није упозната ни са најосновнијим правима и законима у области заштите података и приватности, па и не чуди што је некада немогуће спречити разне злоупотребе. За већину корисника интернета сам концепт приватности прилично је стран, а да би се боље разумеле мере заштите приватности, потребно је прво у основи разумети шта појам приватност означава.

1.1.1 Појам приватности

Приватност, у најширем смислу, значи могућност и право појединца или групе да се осами ако жели и да не приказује одређене податке о себи. Дакле, право приватности дозвољава појединцу да се селективно приказује свету око себе, онолико колико тај појединац жели. Границе и садржај онога што се сматра приватним податком се разликују од културе до културе, и од појединца до појединца, али постоје неке заједничке основе. Приватност се појављује као вишезначна категорија: као право појединца који се појављује као субјект података и као приватност корисника[68]. Приватност корисника обухвата: приватност тзв. "информација за укључивање одређеног терминала у систем" (позивни број, број позивне картице, тип захтеване услуге и слично), приватност говора (онемогућавање пресретања усмених комуникација), приватност података (онемогућавање пресретања података у било ком облику они били), приватност корисникове локације, приватност корисникове идентификације, приватност посебних начина укључивања и приватност његових финансијских трансакција[69].

Заштита података представља скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост и интегритет података од свих опасности које им прете[70]. Сигурност података

---

68 Wilkes J. *Privacy and Authentication Needs of PCs*, IEEE Personal Communications, vol. 2. no. 4/95, str.12;

69 Дракулић М. *Основи компјутерског права*, Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996, стр. 57;

70 Parker D. *Demonstrating the Elements of Information Security with Treats*, National Computer Security Conference, Baltimore, 1995; Heinlein E., *Principles of Information System Security*, Computer&Security, no.14/95, str. 197-199; Wolfe H., *Computer Security: For Fun and Profit*, Computer&Security, no.14/95, str. 113-115;

обухвата обезбеђење података од случајног или намерног откривања неовлашћеним корисницима или заштиту од неовлашћеног мењања, брисања и коришћења од стране овлашћених корисника[71]. Поверљивост података подразумева да се поверљиви подаци не смеју открити од стране неауторизованих појединаца и других ентитета или у неовлашћеним процесима[72]. Расположивост података претпоставља да само овлашћени корисник може благовремено доћи до података, и то одређених, без баријера или других облика ометања и спречавања[73]. Интегритет података обухвата интегритет извора и тачност, што претпоставља да се подаци неауторизовано не мењају или уништавају.

Право на заштиту од неауторизованог нарушавања приватности од стране владе, приватних компанија или индивидуа, јесте у оквиру законске регулативе већине земаља данашњице[74]. Најчешће се налази и у оквиру Устава, као једно од основних људских права.

1.1.2 Историја приватности

Још у Античкој Грчкој, Аристотел је направио разлику између јавне сфере – политике и политичке активности, **полиса** и приватне, кућне, породичне сфере живота, **оикоса**. Термин *оикос* у модерној социологији добија мало измењено значење – служи да опише социјалне групе и људе са којима се проводи највише времена. На неки начин, може се сматрати приватном сфером која обухвата и оне са којима се приватност дели. Занимљиво је да од речи оикос потиче појам економије, што у буквалном преводу значи брига о домаћинству. Аристотел је био међу првима који су разумели значај приватности и одвојили приватно од јавног.

Разлика између приватног и јавног се, такође, понекад односи на одговарајући домен ауторитета власти наспрам домена резервисаног за саморегулацију, као што је описао *John Stuart Mill*, чувени британски филозоф XIX века и отац либерализма, у свом есеју О Слободи. *Mill* је увео значајне либералне (слободарске) идеје и схватања о људским слободама која су за викторијанско доба била револуционарна, а данас се узимају здраво за готово. Један од најважнијих постулата је свакако принцип по коме сваки појединац има слободу да ради шта жели све док то не штети другом лицу. Разлика између приватног и јавног се потенцира и у делима *John Locke*-а, у његовој расправи о власништву и власничкој структури. Иако се слаже да су природа и природна богатсва свачија - јавна, он уводи и концепт приватног власништва, тако што сваки појединац поседује себе самог, па самим тим може да дође и у приватан посед улажући лични рад у њега.

---

71 Martin J, *Information Engineering*, Washington, Prentice Hall, 1990, str. 583; Edwards E, Savage N, Walden I, *Information Technology & The Law*, Basingstoke, Macmillan Publicers LTD., 1990, str. 190 - 198; Kavran D., *Laws And Regulations Of Informations Systems Development And Operation*, UN, 1987, str. 25-27; Petrovic S, Jiric V., *Zaštita podataka u automatizovanim informacionim sistemima*, Beograd, Naucna knjiga, 1986, str. 25 i dr;

72 Shirey R. op. cit., str. 325;

73 Дракулић М, *Основи компјутерског права*, Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996, стр. 58;

74 Drakulic M., Jovanovic S., 2008, *Public eq. private? Twilling of privacy in the time of online social networking*, paper presented at the conference 56th Scientific expert meeting Parliament psychologists, development and standardization in psychology, Kopaonik, 4-7.6.2008;

Margaret Mead, познати амерички антрополог културе, показала је 1949. у свом истраживању[75] полинезијских култура, „ Одрастање у Самои“, како различите културе штите приватност на различите начине, путем скривања информација, осамљења или забране приступа (нпр. забрана приступа тајним церемонијама). Адвокат *Alan Westin* наставио је проучавање приватности. Он је 1967. године обавио истраживање на животињама доказујући да жеља за приватношћу није резервисана само за људе.

У свим овим случајевима, приватност се посматра у другачијем контексту. Може се односити на сферу одвојености од власничке структуре, на домен у коме држава нема права да се меша, као и на забрањене и неприхваћене погледе на стварност и знање, на осамљеност и многе друге теме које задиру у приватност.

Почеци систематизације писаних дискусија о концепту приватности се везују за познати есеј *Samuel Warren*-а и *Louis Brandeis*-а „Право на приватност“. Цитирајући “политичке, социјалне и економске промене” и препознавање права на осамљеност, они су показали да су постојећи закони тог времена (крај XIX века) обухватали и заштиту приватности појединца, а затим су покушали да објасне природу и опсег те заштите. Углавном се фокусирајући на медије и публицитет који је омогућен изумима попут новинарске пресе и фотографије, али такође помињући и повреде у другим контекстима, нагласили су напад на приватност коју је такво време донело, у коме су приватни детаљи из живота многих доспели у јавност. *Warren* и *Brandeis* сматрали су да се већина оваквих и сличних случајева може заштитити правом на приватност, које би штитило опсег у којем нечије мисли, сентименти и емоције могу бити дељене са другима. Наглашено је да они нису покушавали да заштите саме производе или интелектуалну својину, већ слободу мишљења повезану са таквом заштитом. Право на приватност засновано је на принципу неповредљивости личности која је била део општег права на имунитет особе – права на личност. Принцип приватности, веровали су, већ је био део обичајног права, као што је и заштита нечијег дома или замка, али нове технологије довеле су до тога да је постало неопходно експлицитно и независно дефинисати посебно право, право на приватност. Предложили су да се ограничења овог права одреде аналогно Законом о клевети, да би онемогућили објављивање информација о јавним личностима, као на пример - о политичарима који се кандидују. *Warren* и *Brandeis* су поставили основе за заштиту приватности који ће постати познат као право на контролу информација о себи самом.

Иако први случајеви после издавања њиховог дела нису препознавали право на приватност, убрзо су јавност и судство гарантовали то право. У покушају да систематизује и јасније опише и дефинише ово право, *William Prosser* је 1969. године препознао четири различита интереса за приватност[76]. Не покушавајући да дâ конкретну дефиницију и признајући да и даље постоји конфузија и одсуство сагласности у развоју концепта приватности и њене заштите од стране законодавца, *Prosser* је описао четири напада на приватност и то:

- упад у нечију свесну осамљеност или приватне послове;
- јавно обелодањивање непријатних података о личности;
- јавно клеветање особе, приказивање у погрешном светлу;
- присвајање нечијег идентитета зарад користи.

75 Mead, M, *Coming of Age in Samoa*, New York: New American Library, 1949;

76 Prosser, W, 1955, *Handbook of the Law of Torts*, 2nd ed., St. Paul: West;

Prosser је нагласио да се упад у првом типу напада на приватност проширио изван опсега физичког упада и нагласио да су се *Warren* и *Brandeis* углавном бавили другим типом напада на приватност. Ипак, *Prosser* је осећао да су подједнако и физички напади и малтретирања, као и притисак јавности довели до опште прихваћености ова четири типа напада на приватност. Одговори на три главна питања, по њему, у то време још нису била дата. Није било дефинисано да ли појављивање у јавности имплицира губитак права на приватност, чињенице везане за јавни живот ипак могу да буду приватне и значајан ток времена може да утиче на деприватизовање података. Док су *Warren* и *Brandeis* писали нормативно о томе шта они осећају да треба да се заштити законом о приватности, *Prosser* је у ствари описивао оно што су судови већ штитили у протеклих 70 година, од објављивања дела *Warren*-а и *Brandeis*-а. Стога, није изненађујуће да се њихов опис приватности разликује.

1.2 Информациона приватност

Развојем науке и технике, нарочито информационо-комуникационих технологија, приватност добија нову димензију која се односи на прикупљање, обраду, чување и дељење података о појединцу. Све више аутора препознаје нови концепт приватности – информациону приватност посматрају као право појединца да контролише који подаци[77] о њему могу постати доступни другима, за кога и како.

Право на информациону приватност обухвата[78]:

- право на обавештеност, тј. право појединца да буде упознат који се подаци о њему прикупљају, обрађују и чувају, за које се сврхе и од стране кога се користе;
- право на одговарајуће коришћење података;
- право приступа и увида (право контроле);
- право исправке;
- право на правна средства.

Подаци о личности су сви они подаци који се односе на неко одређено или одредиво физичко лице, на основу којих оно може бити идентификовано, а којима се може угрозити његова приватност. То су, пре свега, подаци којима се могу угрозити живот, телесни и физички интегритет, част, углед, живот породице, идентитет и име. Ти подаци се односе на жива и на умрла лица, као и лица проглашена умрлим.

Најчешће се одређеним националним и међународним прописима дефинише који се подаци сматрају подацима о личности. У податке о личности спадају:

- подаци о чињеницама (на пример име, адреса, године, зарада, вероисповест, национална припадност, раса, број и године деце и других

---

77 Дракулић М, *Основи компјутерског права*, Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996, стр. 64;

78 Дракулић М, *Основи компјутерског права*, Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996, стр. 65;

лица под старатељством, политичке активности, коефицијент интелигенције, здравствено стање, осуђиваност и други);
- подаци о мишљењима и судовима самог појединца и других субјеката о њему (на пример о жељама за напредовање, о браку, подаци о кредитној способности, могућностима за професионално напредовање) и
- подаци о намерама (укључујући и намере корисника у вези са субјектом на кога се подаци односе).

Информационо право је релативног карактера, што значи да може бити нарушено од стране унапред одређених субјеката, у строго предвиђеним случајевима и околностима - када су у питању национална безбедност, откривање и кривично гоњење починиоца злочина и слично.

1.2.1 Приватност и контрола информација

Сужени погледи на приватност који се фокусирају на контролу информација и података о личности, које су некада подржавали *Warren* и *Brandeis* и *William Prosser*, такође подржавају и савремени теоретичари, попут *Fried*-а[79] и *Parent*-а (1983). *Alan Westin* описује приватност као могућност да се одреди када, како и до којих граница ћемо одавати податке о личности. Можда је најбољи пример савремене одбране овог става дао *William Parent* наглашавајући да се поглед на приватност брани тако да буде конзистентна са уобичајним говором и оним што приватност значи у уобичајном (народном) говору. На овај начин, неће доћи до забуне или преклапања у коришћењу неких других фундаменталних појмова. Он дефинише приватност као стање у коме не постоје недокументоване персоналне информације које знају или поседују други. *Parent* наглашава да приватност има моралну вредност за оне који вреднују индивидуалност и слободу, а не као морално или легално право на приватност. Он дефише податке о личности као чињенице (у другом случају, то би била клевета) које већина људи бира да не открије другима, као што су чињенице о здрављу, плати, телесној тежини, сексуалној оријентацији, итд. Личне информације су документоване, по Parent-у, једино када припадају јавном досијеу, тј. у новинама, судовима или другим јавним документима. Дакле, онда кад информације постану део јавног досијеа, не постоји кршење права на приватност у неким будућим јавним појављивањима тих истих информација, чак и ако их дели дуг временски период или ако се прикажу масовнијој публици, као што и надзор не дира право на приватност ако резултат нису новооткривени (до тада недокументовани) подаци. У случајевима када нови подаци нису откривени, *Parent* сматра да је упад у приватни простор небитан за само право приватности и да је боље да се онда посматра у контексту анонимности и неовлашћеног упада. Оно што је било описано као уставно право на приватност, *Parent* више посматра као утицајно за слободу избора. Све у свему, по *Parent*-у, постоји губитак приватности једино када други прибаве до тада недокументовану информацију о неком појединцу[80].

79 Fried, C, 1970, *An Anatomy of Values,* Cambridge: Harvard University Press;

80 Parent, W, 1983, *Privacy, Morality and the Law*, Philosophy and Public Affairs 12: 269-88;

1.2.2 Опсег приватности

Још једно питање око кога су настала неслагања, чак и међу оним теоретичарима који верују да је приватност кохерентни концепт, јесте питање да ли уставно право на приватност и описани случајеви у којима је оно нарушено (разне личне одлуке у вези стила живота, породице, укључујући контролу рађања, склапање брака са особама друге расе, гледање порнографије код куће, абортус, итд.) оцртавају границе нове категорије проблема приватности или се, на одређени начин, тичу слобода. *Parent* (1983) експлицитно изоставља бриге око нечије могућности да доноси одређене одлуке везане за породицу и стил живота из групе проблема приватности и каже да се уставно право на приватност односи стриктно на слободу, а не на саму приватност[81]. *Allen* (1988) описује приватност у смислу приступа и изостављања дефиницију заштите индивидуалних одлука аутономних од интервенције државе, што она сматра да је вид слободе. Ипак, она се односи ка овој заштити као ка приватности у одлучивању и каже да је одређивање њене категорије само ствар дефинисања и давања етикете. Она верује да мешање у одлуке, које се тичу трудноће и сексуалности, стварају исте оне моралне бриге као и остали напади на приватност, вређајући вредности родитељства[82]. Врховни суд данас тврди (*Whalen v. Roe*, 429 У.С. 589, 1977) да постоје две различите димензије приватности: контрола над информацијама о себи самом и контрола над способношћу појединца да без мешања других донесе одређене важне одлуке.

Следећи овакво размишљање, бројни теоретичари бране став да приватност има широк опсег, који укључује разне врсте проблема, описане од стране Врховног суда САД, јер не постоји једна дефиниција приватности. Већина њих покушава да пронађе везу између врсте интереса у приватности и сличности образложења за њихово вредновање. Неки наглашавају да је приватност неопходна да би особа развила концепт себе самог као важне и смислене особе. Приватност омогућава контролу над личним подацима, као и контролу над телом и одлукама[83]. Други наглашавају значај интиме за све теме везане за приватност и кажу да је задатак приватности да заштити интимне податке о некоме, приступ и интимне односе и одлуке[84]. Трећи се фокусирају на значај норми приватности које омогућавају лицима да забране приступ себи, као и на норме приватности које побољшавају лично изражавање и развој односа са другима. Приватност пружа заштиту против превелике друштвене контроле од стране других, путем приступа информацијама или контроле доношења одлука (*Schoeman*, 1992). Одбрана овакве контроле приступа и схватање приватности, које укључује контролу приступа телу је у томе да је она такође део концепта приватности заједно са приступом подацима[85]. Четврти сугеришу да је приватност најбоље разумети као кластер концепата који покривају интересовања у контролу над информацијама о себи самом, контролу над приступом себи самом и контролу над личном способношћу да се доносе важне одлуке о породици и стилу живота, у циљу самоизражавања и развијања различитих

81 Parent, W, 1983, *Privacy, Morality and the Law*, Philosophy and Public Affairs 12: 269-88;

82 Allen, A, 1988, *Uneasy Access: Privacy for Women in a Free Society*, Totowa, N.J: Rowman and Littlefield;

83 Kupfer, J, 1987, *Privacy, Autonomy and Self-Concept*, American Philosophical Quarterly 24: 81-89;

84 Inness, J, 1992, *Privacy, Intimacy and Isolation*, Oxford: Oxford University Press;

85 Moore, A, 1998, *Intangible Property: Privacy, Power, and Information Control*, American Philosophical Quarterly 35: 365-378;

друштвених односа[86]. Ова три интересовања су повезана зато што у сваком од та три контекста постоји нешто што нас чини рањивим и бојажљивим да ћемо постати предмет проучавања других лица или ћемо бити исмејани и искоришћени.

Приватност има моралну вредност јер нас штити у сва три контекста, пружајући нам одређене слободе и независност – слободу од посматрања, предрасуђивања, притискања ка прилагођавању, проучавања и осуђивања од стране других.

1.3 Приватност и нове технологије

Велика експанзија комуникационих технологија, као што су развој широко дистрибуираних новина и вишеструко штампаних фотографија и репродукција, у великој мери су мотивисала најјраније аргументе *Warren*-а и *Brandeis*-а за експлицитно признање заштите приватности у правном систему. Слично, заштита коју пружа 4. амандман, усмерена ка незаконитим претресима и упадима на приватну територију је касније, у XX веку, проширена на заштиту од телефонског прислушкивања и електронског надзора. Јасно је да многи и даље гледају на приватност као на веома важан аспект живота, схватајући да је сада, у јеку убрзаног технолошког напретка, угрожена више него икада. Постоје бројне базе података и забелешке на интернету препуне осетљивих података о личној, финансијској или кредитној историји, медицински картони, куповине (он-лајн и оф-лајн), телефонски позиви. Опасно је што већина не зна који подаци о њима су ускладиштени и ко све може да им приступи. Могућност других да приступе тим базама података, уз минималну контролу како они користе те податке и коме их дале, доводи до ситуације у којој је контрола приватности постала тежа него икад[87].

Постоје бројни други случајеви сукоба приватности и технолошког напретка. Узмимо у обзир следеће технологије:

- идентификација позиваоца (Caller ID) - оригинално дизајнирана да заштити људе од нежељених узнемиравајућих позива, телемаркетера, итд. стварају бригу о приватности како за позиваоца, тако и за онога ко је позван;
- широко распрострањена обавеза насумичног тестирања на дроге запослених у компанијама, а Врховни суд САД је донео одлуку да је политика која захтева од свих средњошколаца да пристану на тестирање на дроге како би могли да учествују на ваннаставним активностима није кршење 4. амандман, иако је исти суд забранио обавезно тестирање трудница на дроге, за полицијске потребе;
- фотографисање возача у жутој траци путем система за надзор је такође широко распрострањено, резултујући у казнама које возачи добијају поштом на кућну адресу. Слична техника се користи и код семафора, да би се регистровали возачи који пролазе кроз црвено светло. Скенирање лица

86 DeCew, J, 1997, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press;

87 Drakulic M, Jovanovic S., 2008, *Public eq. private? Twilling of privacy in the time of online social networking*, paper presented at the conference 56th Scientific expert meeting Parliament psychologists, development and standardization in psychology, Kopaonik, 4-7.6.2008;

је такође постало уобичајно у казинима и на спортским дешавањима широм САД, чиме се скенирана лица повезују са базом података лица осуђиваних особа. Све ово може резултовати хватањем одбеглих лица, али представља и напад на приватност осталих, невиних људи, који су фотографисани без њиховог пристанка;

- већина агенција за изнајмљивање аутомобила опремају своје аутомобиле ГПС (*Global Positioning System*) чиповима, помоћу којих сателити могу да прате кретање тих аутомобила. Ово омогућава овим агенцијама, а не полицији, да кажњава појединце за нпр. прекорачење брзине;
- људи који администрирају имиграцију у Аустралији разматрају предлог да се на избеглице у тој земљи закачи специјални чип за праћење кретања, пре него што се одреди њихов статус;
- медији су недавно открили системе за интернет-надзор Федералног бироа за истраживања (ФБИ) *Carnivore* и Америчке агенције за националну сигурност (NSA) *PRISM*-а. Они снимају и филтрирају комуникацију многих корисника интернета, без обзира да ли су осумњичени за неки злочин или не;
- *Echelon* је скривена глобална сателитска мрежа за коју се тврди да има могућност да пресеца све телефонске, фах и електронске поруке на Земљи;
- путници авионом ће ускоро моћи да прођу кроз царинску контролу са задржавањем од само 2 секунде да би се очитали биометријски подаци који потврђују идентитет мапирањем мрежњаче ока. Амерички авио-оператери чак разматрају коришћење смарт-картица које би могле да идентификују путнике користећи њихова лица, очи, отиске прстију и остале делове тела, а технологија за повезивање тих информација са разним различитим базама података напредује веома брзо.

Неке случајеве сукоба напретка технологије и приватности, могуће је објаснити. Тестирање на дроге и алкохол за пилоте авиона на послу се сматра потпуно оправданим, због јавне безбедности, иако нарушава приватност тих особа. Развојем нових, софистицираних технологија, теоретичари приватности покушавају да нађу прихватљив начин којим се поштовање приватности балансира са оправданим коришћењем технологије. *Daniel Solove* настоји да усмери законе према кохерентнијем схватању приватности, развијајући таксономију уз помоћ које се може идентификовати широк спектар проблема везаних за приватност[88]. *Moore* тврди да би нарушавање права на приватност требало да носи са собом већи значај када је у конфликту са другим друштвеним вредностима и користима. Он брани став да слободу говора и изражавања не треба гледати као важнију од приватности. Јасно је да се након терористичког напада на Светски трговински центар литература о приватности много више оријентисала на то како балансирати потребу за приватношћу са потребом за безбедношћу у доба тероризма. *Moore* тврди да ставови који трампе приватност за безбедност на многе начине потцењују и једно и друго[89]. *Etzioni* и *Marsh* пишу бројне есеје о балансирању људских права и

88 Solove, D, 2006, *A Taxonomy of Privacy*, University of Pennsylvania Law Review 154: 477-564;

89 Moore, A, 1998, *Intangible Property: Privacy, Power, and Information Control*, American Philosophical Quarterly 35: 365-378;

безбедности после 11. септембра 2001. године, наглашавајући ставове који дефинишу где ће држава морати да прошири свој ауторитет у борби против тероризма, а где ће ризиковати да прекорачи дозвољени ауторитет[90]. Праву меру није лако одредити. Због тога је важно преиспитати постојећу регулативу у једној и другој области и доносити одлуке од случаја до случаја[91].

2. ПРАВНИ ОБЛИЦИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ НА ИНТЕРНЕТУ

2.1 Међународни инструменти заштите

Право на приватност, као једно од основних људских права, штити се Универзалном декларацијом о људским правима, усвојеном у Генералној скупштини УН, 10. децембра 1948. године, којом се у члану 12 истиче да се „нико не сме изложити произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед. Свако има право на заштиту закона против оваквог мешања или напада“[92]. Савет Европе је, у складу са Декларацијом од 4. новембра 1950. године усвојио Европску конвенцију за заштиту људских права и основних слобода[93] којом потврђују право на приватност у члану 8, кроз право на поштовање приватног и породичног живота.

Заштита података о личности пратила је занимљиву путању у последњих неколико година, пратећи забринутост свих актера, како појединаца тако и правних лица. Значај политике заштите података повезан је са појавом економије података о личности, који су постали важан ресурс у светској економији. Разни примери употребе ових података наглашавају економски раст и потенцијал. Они истичу да је од општег интереса обезбедити слободан проток и аутоматску обраду података о личности како на националној основи тако и ван државних граница.

Европска унија гарантује основна права на приватност и заштиту података. Да би се она спроводила, мора бити регулисано шта је легитимна обрада података о личности и која су права појединаца у односу на ту обраду. Приступ чланица ЕУ састоји се од хоризонталног и свеобухватног регулисања, који би требало да обухвати комерцијалну страну коришћења са јасно дефинисаним ограничењима. Истовремено, прописи би требало да одржавају корак са тржишним и технолошким развојем, како би њихова примена била адекватна. Интернет је дао прилику да се утиче на јавну политику у законодавном процесу реформе заштите података ЕУ, што је условило бројним контраверзама и дебатама у он-лајн окружењу. Креатори

90 Etzioni, A, 2000, *The Limits of Privacy*, New York: Basic Books;

91 Drakulic M, Jovanovic S, 2008, *Public eq. private? Twilling of privacy in the time of online social networking*, paper presented at the conference 56th Scientific expert meeting Parliament psychologists, development and standardization in psychology, Kopaonik, 4-7.6.2008;

92 The Universal Declaration of Human Rights, 1948, The United Nations, http://www.un.org/en/documents/udhr/, 12.12.2013;

93 Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, Rome, 4.XI.1950, Council of Europe, http://conventions.coe.int/treaty/en/treaties/html/005.htm, 13.12.2013;

политика морају да избалансирају супротстављене интересе компанија и бизниса, са једне стране и појединаца са друге. У раду су представљени тренутно важећи прописи које очекује измена до марта месеца 2014. године.

2.1.1 Конвенција о заштити лица у односу на аутоматизовану обраду података о личности

Министарско веће Европског савета објавило је 17. октобра 1980. године Конвенцију о заштити појединаца у односу на аутоматизовану обраду података о личности (*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*)[94], тзв. Европску конвенцију. Доношење ове Конвенције представљало је резултат дуготрајног процеса припреме који је започео још 1960. године. Конвенција је ступила на снагу 1985. године, односно 5 година касније, јер ју је тек тада потписало пет земаља, какав је и био услов.

Конвенција дефинише бројне принципе за праведно и законито прикупљање и коришћење података. Рецимо, подаци се могу прикупљати и обрађивати само уз јасано наведену сврху обраде и не могу се користити за нешто друго. Подаци морају бити тачни, релевантни и чувани само у току временског периода у коме испуњавају сврху обраде, никако после тога. Конвенција, такође, успоставља право приступа и право исправљања података особе о чијим је личним подацима реч и налаже додатну заштиту за осетљиве податке, као на пример за религију, политичко уверење, генетске или медицинске податке неке особе.

Потписивањем и ратификовањем Конвенције, државе се обавезују да национални закони садрже принципе којима се поштују овако дефинисани начини поступања са податацима о личности. Када направе заједничку, минималну основу за заштиту података, слободан проток података о личности између држава је ауторизован за све потписнице Конвенције. Уочена су два проблема приликом примене:

- ако држава која шаље податке о личности има виши ниво протекције од државе која их прима;
- ако се трансфер података о личности обавља у држави која није потписница Конвенције.

Да би се омогућио прекогранични пренос података између држава од којих неке нису потписнице Конвенције, 1992. године је Саветодавна комисија Конвенције изнела модел уговора чија је употреба од стране приватних оператера данас широко распростањена.

У осталим одредбама предвиђено је увођење институције опуномоћника који треба да прати законодавство других земаља потписница, доставља информације о својим националним актима и пружа помоћ појединцима чије је право приватности угрожено. Поред тога, земље потписнице се обавезују да ће формирати Саветодавни комитет који има за циљ да даје предлоге и мишљења о променама, унапређењу и спровођењу ове Конвенције.

---

94 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, 19.11.2013;

Конвенција је у тадашњој СР Југославији потврђена 1992. године Законом о потврђивању Конвенције о заштити лица у односу на аутоматску обраду података о личности (Службени лист СРЈ - Међународни уговори, број 1/92 и Службени лист СЦГ - Међународни уговори, број 11/05) и представљали су основ за израду првог Закона о заштити података о личности.

2.1.2 Директива о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података

Тренутно важећа Директива, израђена давне 1995. године, захтевала је измене како би одржала корак са технолошким променама. Европска комисија је предложила у јануару 2012. године нову уредбу о једном скупу правила за све податке прикупљене на мрежи како би се осигурало њихово безбедно чување и обезбедило пословање са јасним оквиром за њихову обраду.

Директива 95/46/ЕЦ[95] је референцијални текст, на нивоу Европске уније, о заштити података о личности. Она поставља регулаторни оквир који покушава да успостави баланс између високог нивоа заштите приватности личности и слободног протока информација у оквиру Европске уније. Да би то урадила, Директива успоставља строга ограничења кад је реч о сакупљању и коришћењу података о личности. Она, такође, налаже да свака чланица Уније оснује независно национално тело које ће бити одговорно за заштиту ових података.

Ова Директива, донета 1995. године од стране Европског парламента, односи се на податке који се обрађују аутоматски (нпр, компјутерска база података) и на податке који се налазе у неаутоматском систему архивирања података или би требало да буду његов део.

Циљеви Директиве су да заштити права и слободе личности, имајући у виду обраду података о личности, и то уз давање одређених принципа и правила који одређују када је оваква обрада података законита. То се односи на:

- квалитет података: подаци о личности морају бити обрађени на фер и законит начин и морају бити сакупљени за специфичну, експлицитно наведену и легитимну сврху. Такође, морају бити тачни и, где је неопходно, ажурни;
- легитимност обраде података: подаци о личности морају бити обрађени једино ако је особа чији су подаци о личности предмет обраде недвосмислено дала своје одобрење за то. Изузетак је када је обрада података неопходна и то:
    - за испуњење обавеза из Уговора који је особа, чији су подаци о личности објекат обраде, потписала;
    - за поштовање правних обавеза;
    - да би се заштитили витални интереси особе чији су подаци о личности предмет обраде;
    - у случају постојања јавног интереса;

95 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, 18.11.2013;

- за случај легитимног интереса контролора података;

- специјалне категорије обраде: забрањено је обрађивати податке о личности које откривају расно или етничко порекло, политичко опредељење, религијско или филозофско убеђење, чланство у трговинским унијама, здравствене или сексуалне податке;
- информације које би требало дати особи чији се подаци обрађују: контролор мора да пружи особи чији се подаци сакупљају одређене информације које се односе на тог контролора и сам процес обраде (нпр, идентитет контролора, разлоге прикупљања података, кориснике података, итд).
- право приступа подацима: свака особа, чији су приватни подаци предмет обрађивања, требало би да има право да од контролора добије:
  - потврду да ли се подаци о њему обрађују;
  - измену, брисање или блокирање података чија обрада није у складу са овом Директивом, било зато што су подаци непотпуни или нетачни. Такође би требало да добије обавештење о овим променама;
- изузеци и ограничења: опсег ових принципа, који се односе на квалитет података, информације које се пружају особама које су предмет обраде или право приступа и објављивање обраде, може се ограничити ако се процени да је то неопходно да би се сачувала национална безбедност, одбрана, јавна безбедност, процес гоњења криминалаца или неки важни економски или финансијски интерес земље чланице или саме Европске уније;
- право примедбе на процес обраде података: особа чији се подаци обрађују би требало да има право примедбе, на легитимним основама, на процес обраде података о њој. Та особа би требало, такође, да има право да дâ примедбу, на захтев и без надокнаде, на обраду података о личности за које контролор сматра да се обрађују у сврху директног маркетинга. Особу чији се подаци деле са трећим лицима би требало обавестити о томе пре било каквог дељења и дати јој, експлицитино, шансу да уложи примедбу на дељење података;
- поверљивост и сигурност обраде: свака особа која је под ауторитетом контролора или обрађивача података, укључујући и самог обрађивача, која има приступ подацима о личности, не сме да их обрађује осим ако не добије инструкцију од обрађивача. Додатно, контролор мора да имплементира одговарајуће мере заштите података о личности да би се осигурао против случајног или незаконитог брисања или губитка, промене или неауторизованог откривања и приступа подацима о личности;
- обавештавање надгледајућег тела о процесу обраде: контролор мора да обавести национално тело за надгледање процеса обраде података о личности пре него што преузме било какве операције обраде. Супервизор би требало, по добијању овог обавештења, да обави иницијалну проверу и одреди специфичне ризике везане за права и слободе особа чији су подаци о личности предмет обраде.

Свака особа има право на правну заштиту у случају кршења било којег права које му је загарантовано националних законима који се односе на заштиту

података. Такође, било која особа која је претрпела штету услед незаконитог обрађивања података о личностио њој, има право на надокнаду штете.

Пренос података о личности из земље чланице Уније у неку земљу која није чланица, али има адекватан ниво заштите података, јесте ауторизован. Међутим, пренос у земље које немају адекватан систем заштите података о личности је забрањен, осим у већ наведеним изузецима.

Свака земља чланица мора да оснује једно или више независних јавних тела које су одговорне за контролу примене ове Директиве што је регулисано Додатним протоколом уз Конвенцију о заштити лица у односу на аутоматску обраду података о личности, у вези са надзорним органима и прекограничним протоком података.[96]

Централни део постојећег законодавства ЕУ о заштити података о личности, Директива 95/46/ЕЦ[97], усвојен је 1995. године са два циља: да обезбеди основно право на заштиту података и да гарантује слободан проток података о личности између држава чланица. То је била употпуњена Оквирна одлука 2008/977/ЈХА, као општи инструмент на нивоу Уније за заштиту података о личности у области полицијске сарадње и правосудне сарадње у кривичним поступцима[98].

2.1.3 Предлог измена постојећег правног оквира у ЕУ

Брз технолошки развој донео је нове изазове у смислу заштите података о личности. Обим размене података и њиховог прикупљања је драстично порастао. Технологија омогућава и приватним компанијама и јавним властима да искористе податке о личности у циљу остваривања њихових активности. Појединци све више податаке о себи чине доступним јавности и глобално. Технологија је променила како економију тако и социјални живот.

Изградња поверења он-лајн у окружењу је кључна ствар за економски развој. Недостатак поверења доводи до тога да потрошачи оклевају да купују он-лајн и усвоје нове сервисе, чиме се успорава развој, као и сама употреба иновативних технологија. Заштита података о личности стога игра централну улогу у Дигиталној агенди за Европу[99] и, уопште, у Стратегији Европа 2020[100].

Члан 16 (1) Уговора о функционисању Европске уније (УФЕУ), уведен Лисабонским уговором, утврђује принцип да свако има право на заштиту података о личности. Чланом 16 (2) Уговора о функционисању ЕУ, Лисабонски уговор увео је посебан правни основ за доношење правила о заштити података о личности. Члан 8 Повеље о основним правима ЕУ гарантује заштиту података о личности као основно људско право.

---

96 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg,8.XI.2001, http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm, 11.12.2013;

97 Direktiva 95/46/EC Evropskog parlamenta i Saveta od 24. oktobra 1995. godine o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i o slobodnom kretanju takvih podataka, OJ L 281, 23.11.1995, p.31;

98 Оквирна одлука Савета 2008/977/ЈХА од 27. новембра 2008. године о заштити личних података обрађених у оквиру полицијске и правосудне сарадње у кривичним стварима, OJ Л 350, 30.12.2008, п. 60 ('Оквирна одлука);

99 COM(2010)245 final;

100 COM(2010)2020 final;

Европски Савет позвао је Комисију да процени функционисање инструмената ЕУ о заштити података и да представи, где је потребно, даље законодавне и незаконодавне иницијативе[101]. У резолуцији о Штокхолмском програму, Европски парламент[102] је поздравио свеобухватну шему за заштиту података у ЕУ и, између осталог, позвао на ревизију Оквирне одлуке. Комисија је нагласила у свом Акционом плану за спровођење Штокхолмског програма[103] потребу да се обезбеди доследно примењивање основног права на заштиту података о личности у контексту свих политика ЕУ.

У свом саопштењу о "свеобухватном приступу о заштити података о личности у Европској унији"[104], Комисија је закључила да ЕУ треба свеобухватнију и кохерентнију политику о основном праву на заштиту података о личности.

Садашњи оквир није спречио фрагментацију у циљу заштите података о личности, која се спроводи широм Уније, правне несигурности и распрострањена мишљења јавности да постоје значајни ризици везани за активност на глобалној мрежи[105]. Због тога је важно изградити снажнији и кохерентнији оквир за заштиту података у ЕУ, којим ће појединци контролисати сопствене податаке и којим ће се ојачати правна и практична сигурност економских оператера и јавних власти.

Од 9. јула до 31. децембра 2009. године, током консултација о правном оквиру за основно право на заштиту података о личности, Комисија је примила 168 одговора, 127 од појединаца, привредних организација и удружења и 12 од јавних власти[106].

Од 4. новембра 2010. године до 15. јануара 2011. године, у оквиру консултација о свеобухватном приступу Комисије о заштити података о личности у Европској унији, Комисија је примила 305 одговора, од којих је 54 од грађана, 31 од јавних власти и 220 од приватних организација, посебно пословних удружења и невладиних организација[107] што показује колики је интерес да се ова област прецизније уреди.

У новембру 2010. године, потпредседник Европске комисије Единг је организовао округли сто о реформи заштите података. Дана 28. јануара 2011. године (Дан заштите података), Европска комисија и Савет Европе заједнички су организовали конференцију на високом нивоу како би разговарали о питањима која се односе на реформу правног оквира ЕУ, као и на потребу за заједничким стандардима заштите података широм света[108].

101 "Штокхолмски програм - отворена и безбедна Европа служи и штити грађане", OJ Ц 115, 4.5.2010, п.1;

102 Резолуција Европског парламента о саопштењу Комисије Европског парламента и Савета - подручје слобода, безбедност и правда у служби грађана - Штокхолмски програм усвојен 25. новембра 2009. године, (П7_ТА(2009)0090);

103 COM(2010)171 final;

104 COM(2010)609 final;

105 Специјални Еуробарометар (ЕБ) 359, Заштита података и електронски идентитет у ЕУ (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf., 12.5.2014;

106 Sajt Komisije: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm, 13.5.2014;

107 Sajt Komisije: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm., 13.5.2014;

108 Sajt Komisije: http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp, 14.5.2014;

Две конференције о заштити података организоване су од стране мађарског и пољског председништва Савета 16. и 17. јуна 2011. године и 21. септембра 2011. године, респективно.

Наменске радионице и семинари о специфичним питањима одржани су током 2011. године. У јануару, ЕНИСА[109] је организовала радионицу о подацима пробоја обавештења у Европи[110]. У фебруару, Комисија је реализовала радионицу са властима држава чланица, ради разматрања питања заштите података у области полицијске сарадње и правосудне сарадње у кривичним поступцима, укључујући спровођење Оквирне одлуке. Тим поводом је и Агенција за основна права одржала консултативни састанак заинтересованих страна о "заштити и приватности података". Дискусија о кључним питањима реформе је одржана 13. јула 2011. године са националним органима за заштиту података. Грађани ЕУ су консултовани путем анкете Еуробарометра, одржане у периоду новембар-децембар 2010. године[111]. Такође, покренуте су и бројне студије на ову тему[112]. Радна група Члан 29[113] обезбедила је неколико мишљења и користан допринос Комисији[114]. Супервизор за заштиту података у Европи је такође изнео мишљење о питањима покренутим у новембру 2010. године[115].

Европски парламент, својом резолуцијом од 6. јула 2011. године, одобрио је извештај којим је подржан приступ Комисије за реформу оквира за заштиту података[116]. Савет Европске уније усвојио је 24. фебруара 2011. године закључке у којима је широко подржана намера Комисије за реформу оквира за заштиту података и сагласан је са многим елементима приступа Комисије. Европски економски и социјални комитет такође је подржао циљ Комисије да обезбеди примену правила о заштити података ЕУ[117] у свим државама чланицама, одговарајућом ревизијом Директиве 95/46/ЕЦ[118].

Током консултација на свеобухватном приступу, већи део актера се сложио да општи принципи треба да остану важећи, али да постоји потреба да се прилагоди постојећи оквир, како би се боље одговорило на изазове непрекидног развоја

109 Европска мрежа и Безбедносно-информативна агенција, које се баве безбедносним питањима везаним за комуникационе мреже и информационе системе;

110 Видети http://www.enisa.europa.eu/act/it/data-breach-notification, 11.5.2014;

111 Специјални Еуробарометар (ЕБ) 359, Заштита података и електронски идентитет у ЕУ (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf;

112 Компаративне студије о различитим приступима новим изазовима приватност, јануар 2010. године http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf;

113 Радна група је основана 1996. године (према члану 29 Директиве 95/46/ЕЦ) са саветодавним статусом и састављена је од националних представника Заштита података надлежних органа (ДПАс), европских супервизора за заштиту података и комисија. За више информација о активностима видети http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm;

114 Видети следеће: "Будућност приватности" (2009, WП 168); о концептима "управника" и "извршиоца" (1/2010, WП 169); о online оглашавању (2/2010, WП 171); о принципу одговорности (3/2010, WП 173); о важећем закону (8/2010, WП 179); о сагласности (15/2011, WП 187) http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm;

115 Доступно на ЕДПС сајту: http://www.edps.europa.eu/EDPSWEB;

116 ЕП Резолуција од 6. јула 2011. године о свеобухватном приступу заштити података о личности у Европској унији (2011/2025(INI);http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-20110323&language=EN&ring=A7-2011-0244 (rapporteur: MEP Axel Voss (EPP/DE), 11.5.2014;

117 SEC(2012)72;

118 CESE 999/2011;

нових технологија (посебно на мрежи) и све већој глобализацији, задржавајући технолошку неутралност правног оквира. Критикована је тренутна фрагментација заштите података о личности у Унији, посебно од стране економских актера, који су тражили повећање правне сигурности и хармонизацију заштите података о личности. Сложеност правила о међународној размени података о личности представља значајну препреку за њихов рад, јер се редовно преносе подаци из ЕУ у друге делове света.

У складу са својом политиком "Боље уредбе", Комисија је извршила процену утицаја политичких алтернатива. Процена утицаја је заснована на политикама чији су циљеви унапређење унутрашње димензије тржишта заштите података, чинећи остваривање права на заштиту података од стране појединаца ефикаснијом у стварању свеобухватног и кохерентног оквира који покрива све области надлежности Уније, укључујући полицијску и сарадњу правосудних органа у кривичним поступцима. Разматране су и оцењиване три опције интервенције: прва опција се састојала од минималних законских измена и коришћења мера подршке као што су програми финансирања и технички алати; друга опција је обухватала низ законских одредби заснованих на адресирању сваког од идентификованих питања у анализи, док је трећа опција подразумевала централизацију заштите података на нивоу ЕУ, кроз прецизна и детаљна правила за све секторе и оснивање агенције ЕУ за праћење и спровођење одредби.

Према утврђеној методологији Комисије, свака опција је оцењена уз помоћ једне одређене групе. Оцењивање је обављено на основу њене неефикасности у постизању циљева политике, њеног економског утицаја на заинтересоване стране (укључујући буџет институција ЕУ), њеног друштвеног утицаја и утицаја на основна права. Анализа укупног утицаја довела је до развоја опције пожељне политике која се заснива на другој опцији са неким елементима из друге две опције и инкорпорирана је у предлогу. Према процени утицаја, њена примена ће довести, између осталог, до значајних побољшања у погледу правне сигурности, смањења административног оптерећења, конзистентности заштите података у Унији, могућности појединаца да остваре своја права на заштиту података и ефикасности надзора над заштитом података. Очекује се да се имплементацијом опције пожељне политике допринесе циљевима Комисије, као што су поједностављење и смањење административног оптерећења и циљевима Дигиталне агенде за Европу, Штокхолмског акционог плана и Стратегије Европа 2020.

Одбор за процену утицаја поднео је извештај о процени 9. септембра 2011. године. Извештај процене утицаја и извршни резиме публиковани су у предлозима.

У јануару 2012. године, Европска комисија предложила је реформу по питању права заштите података о личности. Реформа се састоји од нацрта Уредбе која утврђује општи правни оквир Европске уније и нацрт Директиве о заштити података о личности обрађених у сврху спречавања, откривања, истраге или гоњења кривичних дела у судским поступцима. Предлоге тренутно разматрају Европски парламент и Савет ЕУ. Да би постао важећи, предлог мора бити одобрен од стране ових заједничких законодаваца.

Дана 21. октобра 2013. године, Комитет за грађанске слободе, правосуђе и унутрашње послове (ЛИБЕ) Европског парламента подржао је предлоге Комисије са огромном већином дајући додатне предлоге у одређеним областима. Комитет је дао мандат својим известиоцима, *Philipp-y Albrecht*-у и *Dimitrios-y Drucas*-у, да уђу у преговоре са Саветом ЕУ.

Министри правосуђа постигли су договор око појединих елемената Директиве ("*one stop shop*" механизма - предлога да свака компанија која послује у јединственом тржишту треба да има јединственог регулаторног саговорника у ЕУ) на Савету у октобру 2013. године. Предлози су поново разматран на Савету у децембру и на неформалном ПУП савету у Атини 23-24. јануара 2014. године. Споразум о реформи могућ је пре краја ове године.

Очекује се да Европски парламент усвоји предлоге у првом читању на пленарној седници у априлу 2014. године. Споразум о реформи заштите података о личности ће тако бити могућ пре краја ове године.

Предлози Европске комисије за свеобухватну реформу Директиве за заштиту података 1995 ЕУ имају за циљ да ојачају права на приватност и регулишу европску дигиталну економију. Постоји јасна потреба да се затвори растући јаз између појединаца и компанија које обрађују податке о личности: девет од десет Европљана (92%) кажу да су забринути због мобилних апликација које прикупљају податке о њима без њиховог пристанка. Седам од десет Европљана забринути су због потенцијалне употребе и објављивања података од стране компанија. Реформом ће ојачати права грађана како би се обновило поверење. Појединац ће моћи да прати и контролише кретање података, нарочито на мрежи и то кроз:

- право да буде заборављен: када више не желите да се подаци о вама обрађују и не постоје легитимни разлози за даљу обраду, подаци ће бити избрисани;
- лакши приступ својим подацима, омогући ће лакши пренос пружаоцима услуга;
- омогућавање да одлучите како се користе подаци; сагласност за обраду података мора бити тражена експлицитно;
- право на информацију да су подаци компромитовани: обавештавање националног надзорног органа од стране компанија и других обрађивача података да је дошло до озбиљних повреда поверљивости и приступа подацима (у року од 24 сата), тако да и корисници могу да предузму одговарајуће мере.

Између новембра 2012. и јануара 2013. године посебна радна група анализирала је основне појмове и опште принципе приватности и заштите података о личности. У закључку је наведено да реформа политика заштите података о личности у ЕУ више одговара својој сврси и он-лине данашњем технолошком контексту. Извештај обухвата развој економије у у односу на он-лине обраду података, уводи основна права на приватност и заштиту података о личности и одговарајућег регулаторног оквира ЕУ, идентификује релевантне мере којима се процењује регулисање заштите података, и уводи економска истраживања да би образложио неке од савремених изазова за очување приватности и заштиту података на мрежи. Последњи део извештаја разматра предлог реформе и даје закључке и препоруке.

Као резултат рада донет је предлог Уредбе Европског парламента и Савета о заштити појединаца у вези са обрадом личних података и о слободи кретања таквих података[119] који дефинише основне принципе поступања са подациома о личности.

---

119 Сајт Европске комисије http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, 11.4.2014;

Да би се обезбедио доследан и висок ниво заштите појединаца, како би се уклониле препреке токовима података о личности, ниво заштите права и слободе појединаца у вези са обрадом података требало би да буде еквивалентан у свима државама чланицама.

Ефикасна заштита података о личности захтева јачање и детаљнију регулативу права физичких лица од стране оних који обрађују податке о личности, све то у складу са правилима заштите података о личности и одређивањем еквивалентне санкције за прекршиоце ових правила у држава чланицама.

Да би се обезбедио доследан ниво заштите за појединца широм Уније и да би се спречила ометања кретања података о личности у унутрашњем тржишту, неопходно је Уредбом обезбедити правну сигурност и транспарентност економских оператера, укључујући мала, средња и велика предузећа. Потребно је обезбедити могућност сарадње између надзорних органа различитих држава чланица. Органи и институције Уније и њихови надзорни органи се подстичу да увек узмимају у обзир специфичне потребе малих, средњих и великих предузећа у примени прописа.

Заштита физичких лица која се односи на обраду података о личности пружена је без обзира на њихову националност или место боравка. Уредба штити податке о личности предузећа основаних од стране правног лица, укључујући име и облик предузећа као и контакт правног лица које је оснивач. Ово би такође требало применити у случајевима кад су оснивачи фирме један или више физичких лица.

Заштита појединаца треба да буде технолошки неутрална и не треба да зависи од технике која се користи, иначе би то створило огроман ризик од заобилажења. Заштиту појединаца треба применити и на аутоматизована средства рада као и на ручне обраде, ако је у опису посла да се поделе подаци о личности.

Неопходно је дефинисати начин коришћења података о личности од стране надлежних органа за потребе превенције, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција, као и слободу кретања таквих података.

Принципи заштите треба да се примењују на било коју информацију која је у вези са идентификованом особом. Да би се утврдило о којој особи је реч, потребно је узети извештаје од руковаоца или од било које друге особе која може препознати тог појединца, а који могу бити од било какве важности. Принципи заштите података не би требало да се примењују на податке који се сматрају анонимним у смислу да се односе на особу која не може више бити идентификована.

Приликом коришћења услуга на мрежи, корисници би требало да буду упознати са идентификаторима који омогућују њихови уређаји, апликације, алати и протоколи као што је адресирање интернет протоколом или *cookie* идентификатори. Они могу оставити путању која, у комбинацији са јединственим идентификаторима и осталим информацијама добијеним са сервера, може да се искористи за креирање профила и препознавање појединца. Из тога следи да идентификациони бројеви, подаци о положају, мрежни идентификатори или било који други специфични чинилац не мора да се сматра податком о личности у свим околностима.

Сагласност треба да буде експлицитна и треба да буде дата било којом одговарајућом методом, којом се јасно виде жеље субјекта о чијим се подацима ради, нпр. изјавом или јасном потврђујућом акцијом субјекта, обезбеђујући да појединци свесно дају свој пристанак на обраду њихових података о личности, укључујући и штиклирање приликом посета интернет страницама или било којом изјавом и понашањем које јасно указује на то да појединац прихвата обраду

података о личности у овом контексту. Стога, игнорисање и неактивност не представљау пристанак. Пристанак треба да обједини све активности обраде података које служе датој сврси. Уколико је пристанак појединца дат уз пратећи електронски захтев, тај захтев треба да буде јасан, концизан и да не ремети непотребно употребу услуге за коју је предвиђен.

Заштита података о личности деце заслужује посебну пажњу, јер су она често мање свесна ризика, последица, гаранција и њихових права у вези са обрадом података о личности која мора бити усклађена са Конвенцијом Уједињених нација о правима детета.

Свака обрада података о личности треба да буде законита, фер и транспарентна у односу на појединца о коме је реч. Специфичне ситуације, у којима се подаци обрађују, треба да буду легитимне уз јасно дефинисање услова под којим се подаци прикупљају. Подаци би требало да буду адекватни, релевантни и ограничени на минимални ниво неопходности за намену на коју се односе, што захтева посебно вођење рачуна о томе да се подаци не прикупљају без преке потребе и да период чувања података буде сведен на минимум. Подаци о личности могу да се обрађују само уколико сврха обраде није могла бити испуњена другим средствима. Треба предузети сваки разуман корак како би се обезбедило да сви подаци који су нетачни буду исправљени или обрисани. Да би се осигурало да се подаци не држе дуже него што је потребно, рокови за брисање или периодичне провере би требало да буду одређени од стране руковаоца.

Да би обрада података била законита, подаци о личности се могу обрађивати на основу сагласности или на некој другој легитимној основи, утврђеној законом.

Тамо где се обрада података заснива на сагласности носиоца података, руковалац треба да буде одговоран приликом доказивања да је носилац података дао сагласност за обраду података. Посебно у контексту писане изјаве у другом случају, мере заштите треба да обезбеде да се носилац података упозна у којој мери је дао сагласност.

Да би се обезбедило да пристанак буде на бази слободне воље, треба нагласити да сагласност не подразумева важећи правни основ где појединац нема истински слободан избор и где не може да одбије и пристанак повуче накнадно, без штете.

Сагласност не би требало да обезбеди ваљан правни основ за обраду података о личности, где постоји јасна неравнотежа између носиоца података и руковаоца. Ово је посебно случај када је носилац података у ситуацији да зависи од руковаоца, на пример обрада података о личности од стране послодавца у процесу запошљавања. Уколико је руковалац особа од јавног ауторитета, постоји неравнотежа само у специфичним операцијама обраде података где јавни ауторитет може да наметне обавезу другом лицу на основу своје моћи и сагласност се не може сматрати као израз слободне воље, узимајући у обзир интерест носиоца података.

Обрада података треба да буде законски одређена тамо где је неопходно у контексту уговора или намене склапања уговора.

Тамо где је руковалац носилац података или где је неопходна обрада података за обављање задатака који су у јавном интересу или у обављању службене дужности, обрада треба да има правни основ. Такође сматрамо да би други могући основ био да се у закону државе чланице испуњавају услови из Повеље о основним правима Европске уније за било које ограничење права и слобода. Потребно је

одредити да ли руковалац обавља задатак од јавног интереса или је коришћење службених овлашћења за сврху обављања задатака јавне управе или за неки другу особу од јавног значаја.

Легитмни интереси руковаоца могу да пруже основ за обраду података, под условом да интереси или пак основа права и слобода носиоца података нису најважнији. То захтева пажљиву процену поготово тамо где је носилац података дете. Носилац права треба да има право приговора на обраду података, на основу специфичних ситуација и то без надокнаде. Да би се обезбедила транспарентност, руковалац би требало да је у обавези да експлицитно обавести носиоца података о легитимним интересима обраде података и о праву на приговор. Такође је у обавези да документује ове легитимне интересе. С обзиром да је законодавац обавезан законом да на основу јавног ауторитета обрађује податке, не би требао да тај закон користи за обраду података у име јавних власти.

Количина обраде података треба да буде строго ограничена за неопходне потребе обезбеђивања мрежа и безбедност информационих система, односно на способност мрежа или информационих система да се одупру, на датом нивоу поверења, од случајних незгода или незаконите и злонамерне радње које угрожавају могућности, аутентичност, интегритет и поверљивост чуваних или преношених података и безбедност сродних услуга које су доступне или се нуде преко ових мрежа и система, од стране јавних власти. Ово би могло, на пример, да обухвати спречавање неовлашћеног приступа електронским комуникационим мрежама и злонамерну дистрибуцију и заустављање *denial of service* напада и уништење рачунара и електронског комуникационог система.

Обраду података о личности у друге сврхе треба дозволити само када је обрада у складу са наменама за које су подаци у почетку били прикупљени, посебно тамо где је обрада неопходна за историјска, статистичка и друга научна истраживања. Тамо где друга намена обраде података није компатибилна са првобитном, руковалац мора да добије сагласност носиоца података за ту намену или на основу других легитимних основа обраде података у сврху јавних потреба.

Подаци о личности који су, по својој природи посебно осетљиви у односу на основна права или приватност, заслужују посебну заштиту. Такви подаци не би требало да буду обрађивани, осим ако носилац података на да своју експлицитну сагласност. Међутим, одступања од ове забране требало би да буду јасно предвиђена у погледу специфичних потреба, нарочито у случајевима где се обрада обавља у току легитимне активности у појединим удружењима или фондацијама којима је сврха да омогући остваривање основних слобода.

Одступање од забране обраде података који припадају осетљивој категорији треба такође да буде дозвољено ако се ради по закону и ако подлеже одговарајућим мерама заштите како би се заштитили подаци о личности и друга основна права, где су разлози од јавног интереса, а посебно у здравствене сврхе, укључујући јавну заштиту и услуге које се тичу здравља људи.

Уколико руковалац обрађује податке неке особе, а приликом те обраде није у могућности да идентификује о којој особи је реч, он није у обавези да прибавља додатне податке у циљу идентификације носиоца података. У случају захтева за приступ, руковалац има право да затражи од носиоца података додатне информације.

Принцип транспарентности захтева да било која информација упућена јавности или носиоцу података буде доступна и разумљива. Пораст улоге технологије

и технолошка сложеност отежава носиоцу података да разуме да ли ће се његови подаци прикупљати, од стране кога и у коју сврху. Због тога је неопходно да услови коришћења података буду дефинисани тако да их носилац података разуме.

Потребно је да носилац података има одговарајуће механизме за приступање, измену и брисање података без накнаде, као и право на приговор. Руковалац би требало да буде у обавези да одговори на захтеве у законом предвиђеном року и да обезбеди образложење у случају да не поступи по захтевима носиоца података.

Уколико се подаци могу легитимно дати другом примаоцу, носилац података треба да буде упознат са тиме, као и када су подаци први пут обрађивани од другог примаоца.

Једно од основних начела је право на приступ подацима који су прикупљени и који би требало да буде максимално олакшан. Појединац има право да зна на који начин се његови подаци користе, у ком периоду, ко располаже њима, кроз које врсте обраде они пролазе и када може доћи до последица овакве обраде.

Руковалац би требало да користи све разумне мере да провери идентитет носиоца података који захтева приступ, посебно у контексту он-лине услуге и он-лине идентификатора. Руковалац не би требало да задржи податке о личности ради сопствених потреба, како би био у стању да реагује на потенцијалне захтеве.

Неопходно је да свако има право да податке може да исправи као и да захтева њихово брисање уколико се више не обрађују у сврху за коју су прикупљени или уколико обрада тих података није у складу са овом уредбом. Ово право је посебно релевантно када је носилац података који је дао своју сагласност за обраду дете, које није у потпуности свесно ризика које може да носи обрада података и касније жели да уклони одређене податке са интернета (на пример на некој друштвеној мрежи). Даље задржавање података може да буде дозвољено уколико су потребни за историјска, статистичка и научна истраживања, у име јавног интереса, када постоји разлог да се обрада података ограничи уместо да се подаци обришу.

Како би се обезбедила могућност брисања података на захтев носиоца података у он-лине окружењу, право на брисање треба проширити на такав начин да је руковалац, који је учинио да подаци постану јавни, у обавези да обавести трећу страну да носилац података тражи брисање података о личности, као и брисање свих копија тих података. Да би се обезбедило ово обавештавање, руковалац треба да предузме све разумне кораке, укључујући техничке мере, у односу на податке за које је он одговоран. По питању треће стране, руковалац треба да преузме одговорност на објављивање тих података у јавности.

Како би се још више обезбедила контрола над сопственим подацима и право на приступ тим подацима, носиоци података треба да имају право, уколико се подаци обрађују електронским путем, да се то чини на најчешће коришћен начин. Носилац података такође треба да има дозволу да пренесе податке, који су подељени, са једне апликације на другу, као што је пренос података са једне социјалне мреже на другу. То се може учинити само када је носилац податка дозволио аутоматску обраду података, на основу посебног уговора.

У случајевима у којима се подаци о личности обрађују у законске сврхе, како би се заштитили интереси носиоца података, или на основу јавног интереса, интереса званичних органа и осталих легитимних интереса, сваки носилац података може да уложи приговор на обраду податка који се односе на њега. Терет

доказивања треба да буде на руковаоцу који треба да покаже да су легитмни интереси јачи од интереса или основних права и слобода појединца.

Уколико се подаци о личности обрађују за потребе директног маркетинга, носилац података би требало да има право да опозове такву обраду без додатних трошкова.

Ограничења на специфичне принципе и на право приступа, исправке и брисања, као и на право преношења података, потребно је посебно уредити националним законодавством. Та ограничења треба да буду усклађена са захтевима наведеним у повељи о основним правима Европске уније и Европске конвенције за заштиту људских права и слобода.

Заштита права и слободе носиоца података у вези са обрадом података о личности, који захтевају одређене техничке и организационе мере, како у време припреме обраде тако и у време саме обраде, регулишу се интерном политиком у складу са заштитом података у сваком смислу.

Заштита права и слободе носиоца података, као и одговорност и обавеза руковаоца и извршилаца, такође у односу на праћење и друге мере надзорних органа, захтева јасно одређивање одговорности, укључујући и намене које утврђује сам руковалац, као и услове и средства за обраду, заједно са осталим руководиоцима или где се обрада података чини у име руковаоца.

У циљу придржавања законом прописаних правила, руковалац и извршилац би требало да документују сваку операцију обраде података. Руковалац и извршилац имају дужност да сарађују са надзорним органима приликом провере рада и, на захтев, да је учине доступном, тако да сама обрада података може бити надгледана.

У циљу одржавања безбедности, како би се спречила обрада која није законита, руковалац или извршилац би требало да процене ризике карактеристичне за обраду података, као и да спроведу потребне мере за ублажавање тих ризика. Ове мере требало би да обезбеде одговарајући ниво безбедности, узимајући у обзир стање технике и трошкове примене тих мера у односу на ризик и природу личних података који су заштићени. Приликом успостављања техничких стандарда и организационих мера за гарантовање безбедности обраде, требало би заступати технолошку неутралност, интероперабилност и иновативност.

Губитак података о личности, уколико се не обавесте надлежни органи на благовремен и адкватан начин, може да резултира значајним економским губитком и социјалном штетом, укључујући крађу идентитета. Чим руковалац постане свестан да је до овакве повреде дошло, обавештава надзорни орган да је дошло до губитка, и то ако је могуће у року од 24 сата. Ако се то не може учинити у року од 24 сата, потребно је доставити објашњење којим се наводи разлог за кашњење. Појединци чији подаци о личности могу бити угрожени, морају бити обаштени без одлагања како би могли да предузму све потребне мере предострожности. Под повредом се сматра свако коришћење података о личности које негативно утиче на приватност носиоца података, идентитет, крађу, превару, физичку повреду, на значајно понижење и повреду угледа носиоца података. Обавештење би требало да описује природу података о личности који су повређени, као и препоруке за носиоца података да се ублажи негативан утицај до којег може доћи приликом повреде. Носиоци података би требало да буду обавештени у најкраћем могућем, разумно изводљивом року, у блиској сарадњи са надзорним органом и поштујући смернице које обезбеђују носиоца података и других органа (на пример: спровођење закона).

Да би се утврдило да ли је, у случају повреде приватности, у најкраћем року обавештен надзорни орган као и носилац података, требало би утврдити да ли руковалац примењује одговарајуће организационе мере и има технолошку заштиту које омогућавају правовремено утврђивање да ли је дошло до злоупотребе података. Мере би требало да омогућавају обавештење без одлагања надзорних органа и носиоца података, узимајући у обзир тежину пропуста, као и последице и негативне ефекте које проузрукује.

Приликом дефинисања правила која се односе на процедуру која се примењује у случају да дође до повреде података о личности, потребно је посветити велику пажњу околностима при којима је дошло до кршења, укључујући и то да ли су и којим мерама заштите заштићени подаци о личности, да ли ефективно онемогућавају крађу идентитета и друге облике злоупотребе. Правила и процедуре треба да буду узете у обзир уколико откривање и обавештавање о пропустима у безбедности може да отежа истрагу што захтева њихову измену.

Директивом 95/46/ЕЦ предвиђена је општа обавеза обавештавања надзорних органа о обради података о личности. Ова обавеза за собом повлачи административни и финансијски терет, иако не може у свим случајевима допринети самој заштити података о личности. Због тога обавеза неселективног обавештавања надзорних органа треба да буде укинута и замењена ефикасним процедурама и механизмима који се фокусирају, уместо на представљање операција обраде и специфичних ризика на права и слободе носиоца података на основу његове природе, на сврху постојања тих механизама. У таквим случајевима, процену утицаја заштите података треба да обави руковалац или извршилац пре обраде, која треба да обухвати посебно предвиђене мере заштите и механизме за обезбеђивање заштите података о личности као и мере за доказивање усаглашености са Уредбом.

Ово се посебно односи на системе који обрађују велику количину података о личности на регионалном, националном и међународном нивоу и који као такви утичу на велики број носилаца података.

Процене утицаја на заштиту података требало би да спроводе јавни ауторитети или јавни органи ако таква процена није већ направљења приликом усвајања националног оквира којим се дефинишу надлежности органа јавне власти и скуп операција које се обављају приликом процена.

Уколико се процени да заштита података приликом обраде података утиче на висок степен ризика и угрожавање права и слободе носиоца података, као што је искључивање појединаца из примене права, или употребом специфичних нових технологија, надзорни орган треба да буде консултован пре почетка операције, како би предложио могуће мере заштите.

Тамо где се процена обавља у јавном сектору или у случају приватних сектора у великим компанијама, или без обзира на величину привредног друштва основна активност укључује обраду података и редовно и системско праћење особа, руководилац или извршилац за праћење би требало да помогну понашајући се у складу са Уредбом. Послове заштите података би требало обављати одвојено и независно од ових процена руковалаца.

Удружења или друга тела испред којих стоји руковалац требало би да имају кодекс понашања, у границама ове уредбе, како би се олакшала и омогућила ефикасна примена Уредбе, узимајући у обзир специфичне захтеве за обрадом у појединим секторима.

У циљу подизања транспарентности, успостављање механизама којима се омогућава сертификација, креирање потписа и печата, као и посебних ознака за заштиту података, потребно је обезбедити носиоцима података да могу брзо да процене ниво заштите.

Међународна трговине и међународна сарадња захтева проток података о личности који ствара нове изазове и проблеме у погледу заштите. Пренос података о личности ка трећим земљама може се обавити само уколико је у потпуној сагласности са Уредбом.

Комисија би требало, приликом процене безбедности трећих земаља, да узме у обзир и то у којој мери се поштује владавина права, приступ правди, као и међународне норме и људска права.

Земљи, територији или сектору обраде у трећој земљи или одређеној међународној организацији која не нуди адекватан ниво заштите података, не би требало дозволити пренос података о личности. У том случају би требало дозволити консултације како би се обавила адекватна измена услова обраде података о личности.

Могућност руковаоца или извршиоца да користе стандардне клаузуле о заштити података, усвојене од стране Комисије или надзорних органа, треба да спречи могућност руковаоца и извршиоца да укључују стандардне клаузуле у општијем уговору, као и да их спречи да додају друге одредбе које су у супротности, директно или индиректно, са стандардним уговорним клаузулама усвојеним од стране Комисије или надзорних органа.

Корпоративни сектор би требало да искористи одобрена правила за међународне трансфере између Уније и организација у оквиру исте корпоративне групе, све док та корпоративна правила укључују битне принципе и применљива права како би се обезбедила одређена гаранција преноса података о личности.

Одредбе треба да се односе на могућност преноса под одређеним околностима, где је власник података дао сагласност, где је пренос неопходан због уговора или правног захтева и где пренос налаже закон, или чланови државне заједнице, или регистар који је намењен за консултације јавности или легитимних лица. У последњем случају, пренос не би требало да се односи на пренос свих података или свих категорија података који се налазе у регистру, а када се регистар односи на консултације легитимних лица, пренос је могућ само уз захтев.

Ови изузеци посебно треба да важе за пренос података, који су неопходни за заштиту података од јавног интереса, као на пример, међународни пренос података између органа, пореских или царинских управа, финансијских органа, служби надлежних за социјална питања, надлежних служби за спровођење истраге, откривање и гоњење.

Пренос који не може бити квалификован као учестали, такође може да се обави као легитиман, уколико су контролори или обрађивачи проценили све околности преноса података. Треба узети у разматрање и легитиман пренос историјских, статистичких и научно-истраживачких података.

У сваком случају, ако Комисија није донела никакву одлуку о адекватној заштити преноса података, контролор или обрађивач података треба да користи решења која гарантују да неће доћи до злоупотребе њихових података, док не дође до преноса.

Када долази до преноса података о личности ван националних граница, постоји већи ризик од злоупотребе података, као што су незаконита употреба и

откривање. У исто време, надзорни органи могу констатовати да нису у стању да прате активности везане за жалбе или истраге ван националних оквира. Њихов заједнички рад може бити отежан из различитих разлога, као што су недовољна превентивна или корективна овлашћења, противречан правни режим или практичне препреке као што је недостатак средстава. Дакле, постоји потреба да се промовише ближа сарадња између надзорних органа и међународних партнера, како би се обезбедила заштита података и размена релевантних информација приликом спровођења истрага.

Успостављање надзорних органа у државама чланицама, као и обављање функција са потпуном независношћу је суштинска компонента заштите појединаца у вези са обрадом података о личности. Државе чланице могу да успоставе више надзорних органа који ће одржавати њихову установну, организациону и административну структуру.

Сваки надзорни орган треба да обезбеди, уз адекватне финансијске и људске ресурсе, простор и инфраструктуру која је неопходна за ефикасно обављање њихових задатака, укључујући и послове који се односе на узајамну помоћ и сарадњу са другим надзорним органима широм Уније и ње.

Када се обрада података о личности, од стране контролора или обрађивача у Унији одвија у више од једне државе чланица, само један орган треба да буде надлежан за праћење активности контролора или обрађивача унутар Уније.

Иако се ова одредба односи и на активности националних судова, надлежност надзорних органа не би требало да покрива обраду података о личности, када судови делују у њиховом својству, а све то како би се очувала независност правосудних органа. Међутим, овај изузетак би требало да буде строго ограничен на праве судске активности у судским предметима и не важи за друге активности где би судије биле укључене, у складу са националним прописима.

Да би се обезбедило доследно спровођење Уредбе широм Уније, надзорни органи треба у свакој држави чланици да имају исте дужности и овлашћења, укључујући и овлашћења везана за спровођење истраге, законски обавезујуће интервенције, одлуке и санкције, нарочито у случајевима појединачних жалби. Истраживачка овлашћења треба да буду у складу са законом Уније и националним законом. То се пре свега односи на добијање судских овлашћења.

Подизање свести код јавности о активностима надзорних органа, треба да укључује и специфичне мере које спроводе контролори, укључујући микро, мала и средња предузећа, као и власнике података.

Надзорни органи треба да помогну једни другима у обављању својих дужности и да обезбеде узајамну помоћ, како би се осигурала доследна примена Уредбе на унутрашњем тржишту.

Сваки надзорни орган треба да има право да учествује у заједничким операцијама између надзорних органа. Надзорни орган који је захтеван треба да одговори на захтев у одређеном временском периоду.

Како би се осигурала доследна примена Уредбе, потребно је успоставити сарадњу између надзорних органа и Комисије. Ова сарадња је посебно значајна у ситуацијама када надзорни орган планира операције које се односе на обраду робе и услуга у неколико држава чланица, или за праћење власника података, као и за проток података о личности.

Приликом примене механизама сарадње може постојати могућност да се хитно делује, како би се заштитио интерес носиоца података, посебно када постоји

опасност од отежане примене права. Дакле, надзорни орган треба да буде у стању да усвоји привремене мере, које ће важити одређени временски период.

Примена овог механизма треба да буде предуслов за правну ваљаност приликом спровођења одговарајућег решења од стране надзорног органа. У другим случајевима ванграничне сарадње, узајамна помоћ и спровођење заједничке истраге, без примене механизама, може се обавити између одређених надзорних органа, када се ради о проблемима који имају билатералну или мултилатералну основу.

Европски одбор за заштиту подата требало би да постоји на нивоу Уније и да замени радну групу која штити лица код којих долази до обраде података о личности, што је одређено Директивом 95/46/ЕЦ. Европски одбор за заштиту података чине представници држава чланица, тако што свака поставља шефа надзорног органа који ће бити у Одбору. Комисија би требало да учествује у њеним активностима. Европски одбор за заштиту података би требало да доприноси доследној примени Уредбе широм Уније, укључујући и саветовање Комисије и промовисање међусобне сарадње. Европски одбор за заштиту података би требало да делује независно приликом обављања својих задатака.

Сваки носилац података би требало да има право на улагање жалбе код надзорног органа у било којој држави чланици, као и право на правни лек уколико сматра да су његова права повређена или уколико надзорни орган не реагује на његову жалбу како би заштитио његова права.

Сваки орган, организација или удружење који има за циљ да штити права и интересе носиоца података, а који је овлашћен националним прописима државе чланице, има право жалбе надзорном органу, право на правни лек, као и могућност независне жалбе уколико сматра да је дошло до повреде његових права.

Свако физичко и правно лице има право на правни лек против одлуке надзорног органа. Поступак против надзорног органа треба да се спроводи пред судовима држава чланица.

У циљу јачања судске заштите носиоца података, у ситуацијама када је надзорни орган основан у другој држави чланици у односу на ону у којој носилац података борави, носилац података може захтевати од било ког органа, организације или удружења, који су овлашћени од стране надзорног органа, да штити његове податке.

У ситуацијама када надзорни орган, који је овлашћен од стране државе чланице, не поступи или не предузме довољне мере приликом улагања жалбе, носилац података може захтевати од надзорног органа државе чланице у свом пребивалишту да покрене поступак против тог надзорног органа. Захтевани надзорни орган може да одлучи, на основу судског увида, да ли је прикладно да прати захтев или не.

Приликом спровођења поступка против контролора или обрађивача података, тужилац би требало да има право избора на то да ли ће мере спроводити испред судова држава чланица, где обрађивач података или контролор ради, или испред суда где носилац података има пребивалиште, осим ако је контролор јавни орган који има своја овлашћења.

Када постоји могућност да се поступак паралелно води у више држава чланица, судови имају обавезу да међусобно сарађују. Судови могу да обуставе случај који је на чекању у другој држави чланици. Државе чланице треба да

дефинишу судске радње, како би се ефикасно усвојиле мере које спречавају кршење Уредбе.

Сваку штету коју носилац података може претрпети услед незаконите обраде, треба да надокнади контролор или обрађивач података, осим у случајевима када они могу доказати да нису криви за штету или када је носилац података претрпео штету због своје грешке или због околности које се нису могле контролисати.

Казне треба да буду изречене било ком лицу које не поштује Уредбу, у складу са националним законодовством. Државе чланице треба да обезбеде да казне буду ефикасне, пропорционалне и превентивне. У циљу јачања и усклађивања санкција, сваки надзорни орган треба да има овлашћење да санкционише административни прекршај.

Обрада података о личности искључиво у новинарске сврхе или за потребе уметничких или књижевних дела, треба да се посебно регулише, како би се усагласило право на заштиту података и право на слободу говора, а нарочито право на примање и саопштавање информација, што је гарантовано чланом 11 Повеље о основним правима Европске уније. Ово посебно треба да се односи на обраду података о личности у аудиовизуелне и новинарске сврхе. Дакле, државе чланице би требало да усвоје мере које ће регулисати изузетке и одступања која су неопходна ради балансирања ових права. Такве изузетке и одступања, државе чланице треба да усвоје на основу општих принципа о правима носиоца података, о обрађивачу података и контролору, о преносу података у другу земљу или међународну организацију.

Обрада нарочито осетљивих података о личности у вези са здрављем, као посебна категорија података која заслужује већу заштиту, може често бити оправдана из бројних разлога, за добробит појединца и друштва у целини. Стога, услови за обраду података о личности у вези са здрављем, подлежу специфичним мерама заштите, како би се обезбедила адекватна заштита. Ово укључује да лице има право приступа овим подацима, као што су на пример његов картон у коме се налазе дијагнозе, резултати испитивања, напомене лекара и слично.

Обрада података о личности у вези са здрављем може бити одређена без сагласности носиоца података, ако је у питању јавни интерес из области јавног здравља. Контекст јавно здравље треба тумачити на основу Уредбе ЕЗ, бр. 1338/2008 Европског парламента и Савета[120] од 16. децембра 2008. године, што значи да се подразумевају сви елементи који се односе на здравље, односно здрастено стање, укључујући обољевања и инвалидности, факторе који имају утицај на здравствено стање, здравствене ресурсе који су неопходни, здравствену заштиту, као и на узроке смртности. Обрада здравствених података о личности не би требало да доведе до обраде података о личности од стране других лица, као што су банке, осигурања и послодавци.

Општи принципи о заштити појединаца у вези са обрадом података о личности такође треба да се примењују и на контекст запошљавања. Стога, да би се регулисала обрада података о личности запослених у контексту запошљавања, државе чланице би требало да усвоје, у границама Уредбе, посебна правила за обраду података о личности у сектору запошљавања.

120 Сајт Европске комисије http://ec.europa.eu/health/data_collection/key_documents/index_en.htm, 15.5.2014;

Обрада података о личности у историјске, истраживачке и научно-истраживачке потребе треба, да би била законита, да је у складу са националним прописима.

Научна истраживања, за потребе Уредбе, треба да укључују основна истраживања, примењена истраживања, истраживања која представљају приватно власништво, а за истраживања која су приватно финансирана треба узети у обзир и члан 179 Уговора о функционисању Европске уније за постизање европског истраживачког простора[121].

Да би се испунили циљеви Уредбе, односно, како би се заштитила основна права и слободе физичких лица и нарочито њихово право на заштиту података о личности и обезбедило слободно кретање података о личности у оквиру Уније, Комисија може да доноси акте у складу са чланом 290 Уговора о функционисању Европске уније. Делегирани акти треба да буду усвојени са становишта законитости обраде наводећи: критеријуме и услове у односу на сагласност детета; обраду посебних категорија података; критеријуме и услова за превелике захтеве и накнаде за остваривање права носиоца података; критеријуме и права за давање информација о носиоцу података; право на заборављање и брисање података; мере засноване на профитирању; критеријуме и захтеве у вези са одговорношћу контролора и подразумевану заштиту података; критеријуме и услове за документацију и безбедну обраду; критеријуме и услове за успостављање и кршење података о личности, а у околностима где долази до кршења података о личности; критеријуме и услове који се односе на операције обраде заштите података захтевају процену утицаја; критеријуме и услове који се односе на висок степен специфичног ризика захтевају претходне консултације; ознака и задатака лица задужених за заштиту података; кодекс понашања, критеријуме и захтеви за механизме сертификације; критеријуме и захтеве за трансфер; административне санкције; обраду за здравствене сврхе; обраду у контексту запошљавања и обраду за историјске, статистичке и научно-истраживачке сврхе.

Да би се обезбедили јединствени услови за спровођење Уредбе, Комисија треба да спроводи одређена овлашћења као што су: стандардна форма за обраду података о личности детета; стандардне процедуре и обрасци за остваривање права носиоца података; стандардне форме за информације на које се подаци односе; стандардне форме и процедуре у вези са правом на приступ и право на преносивост података; стандардне форме за одговорност контролора у вези са обрадом података о личности и за документацију; специфични захтеви за безбедност одбране; стандардни формат и процедуре за обавештавање лица о кршењу обраде података о личности од стране надзорних органа; стандарди и процедуре за процену утицаја на заштиту података; форме и процедуре за претходно консултовање и овлашћење; технички стандарди и механизми за сертификацију; узајамна помоћ и заједничке операције. Та овлашћења треба да се остварују у складу са Уредбом (ЕУ) 182/2011 Европског парламента и Савета[122], донетом 16.2.2011. године, која утврђује правила и опште принципе у вези

121 Lisbon Treaty, Eurostep, EEPA, http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-3-union-policies-and-internal-actions/title-xix-research-and-technological-development-and-space/467-article-179.html, 16.5.2014;

122 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, p. 13, 12.5.2014;

механизама за контролу од стране државе чланице. У том смислу Комисија треба да размотри специфичне мере за микро, мала и средња предузећа.

Комисија би требало одмах да примени одређене акте, у оправданим случајевима, на треће земље, територије или прерађивачке секторе или међународне организације које не обезбеде адекватан ниво заштите у вези са питањима од стране надзорних органа.

Како је подвучено од стране Суда правде Европске уније, право на заштиту података о личности није апсолутно право, али мора бити разматрано у односу на друге функције у друштву и у равнотежи са другим основним људским правима. У складу са принципом пропорционалности, Уредба поштује сва основна права и придржава се принципа признатих Повељом основних људских права Европске уније.

2.1.4 EU Safe Harbour програм

Интернационални *Safe Harbor* принципи приватности чине сет регулација везаних за приватност које је усвојила Европска унија као део Директиве о заштити података. Ови принципи су намењени организацијама у оквиру ЕУ или САД-а који сакупљају податке о личности. Принципи су дизајнирани тако да регулишу случајеве губитака или разоткривања оваквих података.

Листа ових принципа је:

- **нотификација** – компанија мора да пружи изјаву којом објашњава у којој мери користи податке;
- **избор** – корисник мора да има опцију да не открије ниједан податак о себи;
- **пренос података** – ако компанија изабере да уступи приватне податке неком трећем лицу, она мора да се води принципима нотификације и избора. На пример, ако се корисник одлучио да не даје другима податке, та компанија нема право да их уступа трећем лицу;
- **сигурност** – компанија мора да обезбеди своје системе и базе података од губитака, злоупотреба, разоткривања, уништавања и мењања података;
- **интегритет података** – подаци морају бити процесуирани релевантно са сврхом због које су оригинално и прикупљени;
- **приступ** – кориснику се мора омогућити да има приступ подацима, тако да може да их мења, додаје и брише;
- **примена** – компанија мора да примењује ове принципе, као и своје унутрашње полисе и процедуре, у циљу заштите случајног или намерног разоткривања или губитка података.

Према одлуци Министарства трговине Сједињених Америчких Држава *Facebook* учествује у *EU Safe Harbour* оквиру приватности, чиме је пристао на TRUSTe резолуцију за решавање спорова у оквиру приватности.

2.2 Национални инструменти заштите

2.2.1 Закон о заштити података о личности

Новим Уставом Републике Србије загарантовано је право на заштиту података о личности. Поред тога, Република Србија је потписала и Додатни протокол уз Конвенцију о заштити лица у односу на аутоматску обраду података о личности, у вези са надзорним органима и прекограничним протоком података Савета Европе. Такође, због преношења надлежности са тадашњих савезних органа на државне органе Републике Србије, одговарајућим прописима није одређен државни орган који би преузео надлежност за остваривање права по том закону, што фактички значи да се заштита на основу тог закона није ни могла остваривати у пракси[123].

Из тих разлога, донет је нови Закон о заштити података о личности[124] који је ступио на снагу 1. јануара 2009. године. Овим законом детаљно је уређена заштита података о личности, обрада и коришћење ових података, права грађана на увид у податке, као и орган надлежан за надзора над спровођењем овог закона и заштиту права грађана, у складу са Законом.

Предмет Закона је дефинисан у члану 1: Овим законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона. Заштита података о личности обезбеђује се сваком физичком лицу, без обзира на држављанство и пребивалиште, расу, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло, имовинско стање, рођење, образовање, друштвени положај или друга лична својства. Послове заштите података о личности обавља Повереник за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), као самосталан државни орган, независан у обављању своје надлежности.

Циљ закона је да, у вези са обрадом података о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода.

Закон садржи 11 делова: Основне одредбе, Услови за обраду, Права лица и заштита праве лица, Поступак по жалби, Повереник, Обезбеђење података, Евиденција, Изношење података из Републике Србије, Надзор, Казнене одредбе и Прелазне и завршне одредбе.

Чланом 5. Закона одређени су подаци о личности на које се не примењује овај закон, а то су подаци који су доступни свакоме и објављени у јавним гласилима и другим публикацијама, подаци који се обрађују за породичне сврхе и нису доступни трећим лицима, подаци о члановима политичких странака и других

123 Drakulic M. Jovanovic S. Drakulic R. 2010, *Establishment CSIRT-a in Serbia, Incorporation of Broadcaster according to Serbian Broadcasting La,w* article presented at the conference 12h International symposium FOS, SymOrg 2010, Zlatibor, 2010;

124 Закон о заштити података о личности, Службени гласник РС, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012;

удружења, када се обрађују од стране тих организација и подаци које је лице објавило о себи.

У другом делу Услови за обраду (чл. 8-18), у члану 8 Закона, уређује се недозвољеност обраде података о личности. Обрада није дозвољена без пристанка овлашћеног лица или без законског овлашћења, ако се чини у сврху која је другачија од оне за коју је одређена, ако сврха обраде није јасно одређена или је измењена, ако је начин обраде недозвољен и из других разлога прописаних законом.

Члановима 10-12 Закона уређена је обрада са пристанком, односно без пристанка. Чланом 12 Закона прописано је да је обрада без пристанка дозвољена у циљу остваривања или заштите животно важног интереса лица, у сврху извршења обавеза одређених законом и у другим случајевима који су прописани искључиво законом.

Чланом 13 Закона прописано је да државни орган може да обрађује податке без пристанка лица ако је то потребно ради остваривања интереса безбедности, вођења кривичног поступка, заштите економских интереса државе, заштите здравља, права и слобода и другог јавног интереса.

Члан 14 Закона уређује прикупљање података. Подаци се могу прикупљати од лица на које се односе, а од других лица само на основу уговора, ако је то прописано законом или другим прописом, ако је то неопходно с обзиром на природу посла, ако се подаци прикупљају ради остварења животно важних интереса лица и ако прикупљање података од самих лица на које се односе захтева прекомерни утрошак времена и средстава.

Чланом 15 Закона прописано је да је руковалац података дужан да пре прикупљања и обраде о томе упозна лице на које се подаци односе. Такође, овим чланом је уређено одступање од ове обавезе, али је прописано да је руковалац дужан да накнадно обавести лице на које се подаци односе о обради, односно прикупљању података.

Члановима 16-18 Закона прописана је обрада нарочито осетљивих података. У члану 16 Закона прописано је да су нарочито осетљиви подаци они подаци који се односе на националну припадност, расу, пол, језик, вероисповест, политичко и друго уверење, синдикално чланство, здравствено стање, сексуални живот, примање социјалне помоћи, жртву насиља и осуду за кривично дело. Прописано је да обрада ових података мора бити посебно одређена и заштићена мерама заштите.

У трећем делу Права лица и заштита права лица (чл. 19-37), у члановима 19-22 Закона, уређена су права лица поводом заштите података о личности, а то су: право на обавештење о обради, право на увид, право на копију и право поводом извршеног увида. Овде треба посебно истаћи право лица поводом извршеног увида које се остварује тако што лице има право да од руковаоца са личним подацима захтева исправку, допуну, ажурирање, брисање података, као и прекид и привремену обуставу обраде података о личности.

Чланом 23 Закона прописана су ограничења од горе наведених права. Ова права се могу ограничити ако лице злоупотребљава своје право на обавештење, увид и копију, ако би руковалац био онемогућен у обављању својих послова, ако би давање обавештења озбиљно угрозило безбедност земље, важан привредни или финансијски интерес државе и вођење кривичног поступка, ако би се обавештењем учинио доступним податак који је означен као тајна, ако би

обавештење озбиљно угрозило приватност или важан интерес лица и ако се подаци о лицу искључиво користе у научно-истраживачке и статистичке сврхе.

Чланови 27 и 28 Закона уређују остваривање права на увид и копију. Уведена је обавеза за руковаоца да све податке учини доступним подносиоцу у стању у каквом се налазе, као и да обезбеди потребну стручну помоћ ради разумевања садржине податка. Такође је прописано да право на увид не сме бити условљено плаћањем накнаде, а да подносилац захтева сноси само нужне трошкове израде и предаје податка.

Члановима 35-37 Закона прописано је чување и коришћење података у случају смрти, обавеза руковаоца података да брише податке у случају раскида уговора, односно повлачења пристанка, као и сходна примена закона којим се уређује општи управни поступак.

У четвртом делу Поступак по жалби (чл. 38-43), у члану 38 Закона, прописано је да подносилац захтева за остваривање права у вези са обрадом података може изјавити жалбу Поверенику. Прописано је да се жалба може изјавити против одлука руковаоца којом је одбијен или одбачен захтев, у случају када руковалац не одлучи о захтеву у прописаном року, ако руковалац не стави на увид податак, односно изда копију у року и на начин прописан законом, ако руковалац услови издавање копије уплатом накнаде која није прописана и ако руковалац отежава или онемогућава остваривање права.

У петом делу, који говори о Поверенику (чл. 44 и 45), у члану 44 Закона, прописана је надлежност Повереника према овом закону. Повереник има обавезу да подноси извештај Народној скупштини, који се доставља и Влади и председнику Републике и на одговарајући начин ставља на увид јавности. Повереник може имати и заменика за заштиту података о личности. У члану 45 Закона прописано је право приступа и увида Повереника у вези са заштитом података о личности, као и ограничење овог права.

У шестом делу који се односи на Обезбеђење података (чл. 46 и 47), у члану 46 Закона, прописана је обавеза чувања тајне за Повереника, његовог заменика и запосленог у стручној служби у вези са подацима које сазнају у обављању својих дужности. Обавеза чувања тајне траје и после престанка дужности или радног односа. Чланом 47 Закона прописане су организационе и техничке мере за заштиту података о личности од злоупотребе, уништења, губитка, неовлашћене промене или приступа.

У седмом делу Евиденција (чл. 48-52), у члану 48 Закона, прописано је да је руковалац дужан да образује и води евиденцију о подацима и збирка података које води, као и садржина ове евиденције.

Осми део, Изношење података из Републике Србије (члан 53), прописује да се подаци из Републике Србије могу износити у државу чланицу Конвенције о заштити лица у односу на аутоматску обраду података о личности Савета Европе, а у друге државе које нису чланице Конвенције само ако је обезбеђен степен заштите података у складу са Конвенцијом, на основу дозволе Повереника.

У деветом делу Надзор (чл. 54-56), прописано је да надзор над спровођењем и извршавањем овог закона врши Повереник преко овлашћених лица. На основу налаза овлашћеног лица у обављању надзора, Повереник може наредити да се неправилности отклоне у одређеном року, привремено забранити обраду која се обавља супротно одредбама овог закона, као и наредити брисање података

прикупљених без правног основа. Против акта Повереника у обављању надзора жалба није дозвољена, али се може покренути управни спор.

Десети део Казнене одредбе (члан 57), садржи прекршајне одредбе за повреду овог закона. Преписује се новчана казна од 50.000 до 1.000.000 динара за кршење овог закона од стране руковалаца, обрађивача или корисника који има својство правног лица.

Једанаести део се односи на Прелазне и завршне одредбе (чл. 58-63).

Чланом 59. Закона прописано је да Повереник за информације од јавног значаја, установљен Законом о слободном приступу информацијама од јавног значаја наставља са радом под називом Повереник за информације од јавног значаја и заштиту података о личности.

Права физичког лица дефинисана Законом о заштити података о личности су:

- **право на давање/недавање пристанка за обраду** – свако физичко лице има право да руковаоцу да/не да пристанак за обраду података о себи, ако руковалац не обавља обраду на основу законског овлашћења. Физичко лице може да да пуноважан пристанак и преко пуномоћника, а може пристанак и да опозове. Да би лице дало пристанак, руковалац је дужан да га претходно упозна о свом идентитету и свим осталим питањима из члана 15 Закона;
- **право на обавештење о обради** - лице има право да захтева да га руковалац потпуно и истинито обавести о томе да ли обрађује податке о њему, које и у коју сврху и по ком правном основу и од кога их прикупља; у којим збиркама података се налазе подаци о њему, ко су корисници и којих података и у које сврхе и по ком правном основу; коме и који подаци се преносе, у коју сврху и по ком правном основу, као и свим осталим питањима из члана 19 Закона;
- **право на увид** - лице има право да захтева да му се ставе на увид подаци који се на њега односе. Право на увид обухвата право на преглед, читање и слушање података, као и прављење бележака;
- **право на копију** – лице има право да од руковаоца захтева копију података који се на њега односе, при чему је дужан да сноси само нужне трошкове израде и предаје копије;
- **права поводом извршеног увида** - лице има и право да од руковаоца захтева исправку, допуну, ажурирање или брисање података, као и прекид и привремену обуставу обраде, ако су испуњени услови предвиђени чланом 22 Закона.

Руковалац подацима о личности, који може да буде физичко лице, правно лице или орган власти, прикупља податке од лица на које се односе, односно од другог лица. Руковалац је дужан да обраду података обави на основу пристанка лица или на основу закона. У случају да лице опозове пристанак, руковалац не сме након тога да обрађује податке.

Руковалац је дужан да обави обраду података у свему поштујући одредбе о дозвољености обраде (члан 8 Закона).

Руковалац је дужан да пре прикупљања, по правилу у писаном облику, упозна лице на које се подаци односе, односно друго лице, о свом идентитету и свим питањима која се односе на обраду података, све у складу са чланом 15 Закона. Руковалац је дужан да лице обавести и о измени, допуни или брисању података.

Руковалац је дужан да подносиоца захтева истинито и потпуно обавести о свим питањима у вези обраде података из члана 19 Закона, и то без одлагања, а најкасније у року од 15 дана од дана подношења захтева за обавештење о обради.

Руковалац је дужан да омогући лицу да изврши увид у податке који се на њега односе, односно да преда копију, и то без одлагања, а најкасније у року од 30 дана од пријема захтева. У случају постојања оправданих разлога ови рокови од 15, односно 30 дана, могу се продужити за 30 дана. Руковалац је дужан да подносиоцу учини доступан податак који се на њега односи, и то у разумљивом облику, односно да учини доступним све податке у стању у каквом се налазе, као и да на захтев лица пружи стручну помоћ ради разумевања садржине података. Остваривање права на увид је бесплатно, док подносилац захтева сноси само нужне трошкове израде и предаје копије података.

Такође, руковалац је дужан да без одлагања, а најкасније у року од 15 дана од дана подношења захтева, одлучи о захтеву за остваривање права поводом извршеног увида (исправка, допуна, ажурирање, брисање, прекид и привремена обустава обраде), као и да о томе обавести подносиоца захтева.

Ако руковалац не обрађује податак, проследиће захтев Поверенику, осим ако се подносилац захтева томе противи. Руковалац је дужан да поступи по решењу (налогу) Повереника, као и да овлашћеном лицу Повереника омогући несметано обављање надзора и стави му на увид и располагање потребну документацију.

Ако је збирка података успостављена уговором, односно на основу пристанка у писаном облику, у случају раскида уговора, односно повлачења пристанка, руковалац је обавезан да податке брише у року од 15 дана од дана раскида уговора, односно повлачења пристанка, осим ако је другачије прописано или уговорено.

Руковалац је дужан да предузме све потребне техничке, кадровске и организационе мере заштите података, у складу са утврђеним стандардима и поступцима, а које су потребне да би се подаци заштитили од губитка, уништења, недопуштеног приступа, неовлашћених промене, објављивања и сваке злоупотребе, као и да утврди обавезу лица која су запослена на обради, да чувају тајност података.

Руковалац је дужан да образује, води и ажурира евиденцију о обради података која садржи елементе из члана 48 Закона, све у складу са Уредбом о обрасцу за вођење евиденције о обради података о личности (Службени гласник РС бр. 50/09).

Руковалац је дужан да пре започињања обраде, односно успостављања збирке података, достави Поверенику обавештење о намери успостављања збирке података са потребним подацима (члан 49 Закона), као и о свакој даљој намераваној обради, пре предузимања обраде и то најкасније 15 дана пре успостављања збирке података, односно обраде. Руковалац доставља Поверенику и евиденцију о збирци података, односно промене у евиденцији података, најкасније у року од 15 дана од дана успостављања, односно промене. Наведена обавештења и евиденције уписују се у Централни регистар.

У складу са Законом донета је Уредба о обрасцу за вођење евиденције и начину вођења евиденције о обради података о личности, Правилник о начину претходне провере радњи обраде података о личности и Правилник о обрасцу легитимације овлашћеног лица за обављање надзора по Закону о заштити података о личности којима је прецизније уређена ова област.

Тренутни Закон не обухвата прикупљање и обраду података путем интернета. Пристанак лица на обраду захтева се у писаном облику, што је у случају он-лине регистрације немогуће. Закон не препознаје услове коришћења многобројних портала на којима корисници свакодневно остављају разне податке о личности. Коришћење друштвених мрежа и специфичан начин формирања и коришћења електронских база захтева измену постојећег Закона и увођење посебних одредби који прецизније уређују ову област.

2.2.2 Повереник за информације од јавног значаја и заштиту података о личности

Повереник за информације од јавног значаја и заштиту података о личности је самосталан државни орган, независтан у обављању своје надлежности, који обавља послове заштите података о личности и чији је широки делокруг надлежности утврђен чланом 44 Закона о заштити података о личности.

Ради остваривања послова из свог делокруга Повереник, у основи, располаже са две врсте овлашћења - оним који се односе на његово деловање као другостепеног органа који право на заштиту података о личности штити у поступку по жалби и оним који се односе на његово деловање као надзорног органа у функцији спровођења закона.

Повереник прати поштовање обавеза органа власти утврђених Законом о заштити података о личности и извештава јавност и Народну скупштину о томе; даје иницијативу за доношење или измене прописа ради спровођења и унапређења права за које је надлежан; предлаже органима власти предузимање мера у циљу унапређивања њиховог рада уређеног законом; решава по жалби против решења органа власти којима су повређена права уређена овим законом; обавештава јавност о садржини овог закона, као и о правима уређеним Законом.

Повереник доноси одлуку по жалби најкасније у року од 30 дана од дана подношења жалбе. Претходно, он жалбу доставља руковаоцу, ради одговора на жалбу односно изјашњења, а по потреби предузима и друге радње за утврђивање чињеничног стања које су неопходне ради доношења одлуке по жалби. У ту сврху Поверенику, односно лицу кога он посебно овласти, руковаоц ће омогућити увид у податке, односно у збирку података, у своје опште акте и просторије и опрему које користи.

Одлучујући по жалби, Повереник може одбацити наблаговремену и неуредну жалбу, односно одбити неосновану жалбу. Кад утврди да је жалба основана Повереник ће решењем наложити руковаоцу да у одређеном року поступи по захтеву.

Решење Повереника по жалби је обавезујуће, коначно и извршно. У случају потребе Влада обезбеђује извршење решења Повереника.

Повереник обавља надзор над спровођењем Закона о заштити података о личности. Послове надзора Повереник чини преко овлашћених лица-инспектора. Инспектор је, при обављању надзора, дужан да покаже легитимацију, да послове надзора обавља стручно и благовремено и да о обављњном надзору сачини записник. Инспектор поступа на основу сазнања до којих је дошао по службеној дужности, од стране подносиоца жалбе или трећег лица, а лица, којима су законом утврђене обавезе у вези са обрадом и заштитом података о личности, дужна су да

инспектору омогуће несметано обављање надзора, да му ставе на увид и располагање потребну документацију. Инспектор је дужан да, у складу са законом и другим прописима којима се уређује тајност података, чува све податке које сазна у обављању надзора, осим ако је друкчије прописано. Ова обавеза траје и по престанку обављања ових послова.

Ако се приликом обављања надзора утврди да су повређене одредбе закона којима се уређује обрада података о личности, Повереник ће упозорити руковаоца на неправилности у обради. На основу налаза инспектора, Повереник може:

- наредити да се неправилности отклоне у одређеном року;
- привремено забранити обраду која се обавља супротно одредбама овог закона;
- наредити брисање података прикупљених без правног основа.

Повереник обавља надзор и у погледу изношења података о личности из Републике Србије и одбрава изношење података. Против решења Повереника жалба није дозвољена, али се може покренути управни спор тужбом Врховном суду Србије. Повереник подноси прекршајну пријаву због повреда одредаба овог закона.

2.2.3 Кривични законик Републике Србије

Кривични законик Републике Србије, у глави Кривична дела против слобода и права човека и грађанина, прописује седам дела у области повреде права на приватност и заштиту података о личности[125]. Повреда поверљивог односа лекара и пацијента или адвоката и клијента у коме се размењују чак и нарочито осетљиви подаци о личности инкриминисана је чланом 141, Неовлашћено откривање тајне, које може бити прекршено само у општем интересу или у интересу другог лица који је претежнији од интереса чувања тајне. Тиме је осигурано да информациони системи који су све више присутни у јавном сектору (здравству, судству, образовању и др.) морају бити пажљиво имплементирани са прецизно дефинисаним овлашћењима, ко има права приступа којим подацима, у складу са постојећим прописима. Чланом 146 Неовлашћено прикупљање података о личности кажњава се свако неовлашћено прикупљање, обрада, коришћење и саопштавање другом података о личности. Оно што је често спорно приликом прикупљања и обраде је избор података који се захтевају јер није јасна сврха обраде. Неопходно је преиспитивање постојећих захтева, образаца, како папирних тако и електронских, који се попуњавају без имало сумње у законитост и релевантност од стране појединца, који често нису питани ни обавештени како се ти подаци даље користе. Посебним ставом прописана је казна за службено лице које учини ово дело у вршењу службе за шта може бити осуђено на казну затвора до три године. Иста казна може бити изречена службеном лицу за кривично дело Повреда тајности писама и других пошиљки (члан 142) чиме се штити приватност писане комуникације. Овим чланом експлицитно се наглашава да радња извршења може обухватити и повреду тајности електронске поште или другог средства за

125 Кривични законик Републике Србије, Сл. гласник РС, бр. 85/2005, 88/2005 -испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012 и 104/2013;

телекомуникацију чиме се електронска комуникација изједначава са традиционалним писањем писма, телеграфа и слично. У случају да ово уради неко друго лице може се казнити новчано или затвором до две године. Повреда приватности у случају усмене комуникације дефинисана је чланом 143, Неовлашћено прислушкивање и снимање које постаје све актуелније са развојем технологија које се на једноставан начин могу злоупотребити у ову сврху. Уз аудио често се врши и видео снимање што је посебно регулисано чланом 144, Неовлашћено фотографисање интервенција Повереника да се камере за праћење саобраћаја уклоне јер нису адекватно постављене, као и поједини случајеви коришћења јавних камера намењених за уживање у панорами града у сврхе снимања и задирања у интимни живот грађана само су неки од примера кршења приватности. Инкриминишући наводи некадашњег службеника *National Security Agency*[126] *Edwarda Snowdena* да се, под окриљем националне безбедности крше основна људска права и неовлашћено снимају електронске комуникације, не само политичара и других јавних личности, већ велике групе грађана без јасног основа, сугеришу да су такве ситуације могуће и у Србији. Службено лице за неовлашћено фотографисање може добити до три године казне затвора, а за прислушкивање и снимање до пет година. Закон о електронским комуникација прописује начине обављања тајног надзора, али без регулисаног видео-надзора и информационе безбедности, генерално, не могу се прецизно одредити оквири приватности појединца који неће угрозити безбедност државе и обрнуто. У ери друштвених мрежа значајно је поменути члан 145, Неовлашћено објављивање и приказивање туђег списа, портрета и снимка без пристанка лица чије одређење, бар када је најпопуларнија мрежа у питању - *Facebook*, на којој је једна од главних активности „шеровање“ фотографија, текстова и коментара, захтева додатно преиспитивање.

Кључно је да се за сва наведена дела, којом је инкриминисана повреда приватности и постоји неки вид злоупотребе података о личности, поступак покреће по приватној тужби, сем када то учине службена лица у обављању своје дужности, када се гоњење предузима по предлогу. Тиме је држава препустила појединцу да се за остварење овог права сам бори. Поставља се питање да ли је тежина ових дела адекватно регулисана јер је за остале слободе и права човека (равноправност, право на употребу језика и писма, изражавање националне или етничке припадности, слободу кретања, исповедање вере и слично) предвиђено да држава мора да интервенише. Изменом одредби Кривичног законика порука свима који су спремни да занемаре право да „вас оставе на миру“ би била јаснија. Крађа идентитета и разни видови преузимања података о личности на интернету (нпр. *phishing*) нису посебно инкриминисана Кривичним законом Републике Србије већ се третирају као превара (члан 208), о чему ће посебно бити речи у посебном поглављу.

126 The National Security Agency/Central Security Service, USA, http://www.nsa.gov/index.shtml, 13.3.2014;

3. ИСТРАЖИВАЊЕ

Избор домена истраживања одређен је циљевима пројекта "Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије". Значајно је било испитати да ли и у којој мери коришћење информационо-комуникационих технологија (у даљем тексту ИКТ) утиче на кретање миграната и азиланата, да ли им омогућава једноставнију комуникацију и на који начин се то може спречити. Развијено је неколико упитника који су били намењени посебним групама: азилантима, ирелегуларним мигрантима, кријумчарима и слично. За сваку од ових група проверавано је да ли су у својим активностима користиле рачунаре, смарт телефоне или интернет. Да би се ти резултати јасније повезали са појавом ИКТ-а, неопходно је било на већем узорку добити одговоре на иста питања. Тако је дефинисан општи упитник са 69 питања који би требало да представи свеобухватнији и детаљнији увид у карактеристике корисника ИКТ-а, податке о фреквенцији и начину употребе, врстама активности корисника на мрежи.

Истраживање у другом делу садржи питања достављања података о личности на мрежи: који се подаци остављају, коме и на који начин. Трећи део испитује да ли су испитаници упознати са потенцијалним злоупотребама података о личности коришћењем мобилних уређаја и рачунара преко интернета, да ли познају некога ко их користи у те сврхе и какав је њихов став према њима. Наведени су различити облици високотехнолошког криминала везани за злоупотребу података, као што су крађа идентитета, хакинг и фишинг. Четврти део намењен је корисницима друштвених мрежа: које податке остављају, ко све може да види њихов профил, да ли примају различите понуде преко мреже, како реагују на те понуде, да ли су се сусрели са појединим облицима злоупотребе података како би се утврдило да ли постоји одступање у односу на злоупотребу на читавој мрежи.

Један од циљева истраживања је испитати појаву приватности на интернету: низак ниво свести и недостатак тренинга и обука који објашњавају начине на које би податке о личности требало користити на мрежи, како се могу злоупотребити, јасно дефинисање опасности коју носи одређена врста понашања на интернету. Неопходно је утврдити тренутно стање, анализирати постојеће правне и техничке мере заштите које се примењују у овој области како би се донели релевантни закључци и дефинисали кораци које би требало предузети, водећи рачуна да су деца и млади део популације која проводи највише времена на интернету.

3.1 Хипотезе

Истраживање у делу које се односи на приватност и заштиту података о личности на интернету требало би да провери следеће хипотезе:

- X_1. Већина испитаника млађих од 30 година оставља велики број својих података о личности на Интернету;
- X_2. Млади немају довољно знања о могућим злоупотребама података о личности на интернету.

3.2 Анализа резултата

Спроведено истраживање о појавним облицима компјутерског и *cyber* криминала у Србији, обухватило је, поред анкете намењене општој популацији и анкету коју су попуњавали представници надлежних органа за борбу против високотехнолошког криминала у оквиру Службе за борбу против организованог криминала, Управе криминалистичке полиције, Управе граничне полиције, Посебног тужилаштва за борбу против високотехнолошког криминала при Републичком јавном тужилаштву и неколицина судија који су водили процесе из ове области. Испитивање је било анонимно и временски није било ограничено. Прикупљени подаци су обрађивани у програмима SPSS и *Microsoft Exel*.

3.2.1 Остављање и прослеђивање података о личности на интернету

Део истраживања односио се на податке које корисници остављају на мрежи о себи. Испитаници су одговарали на питања „Да ли сте доставили некоме он-лине своје податке?“, „Коме?“ и „На који начин?“.

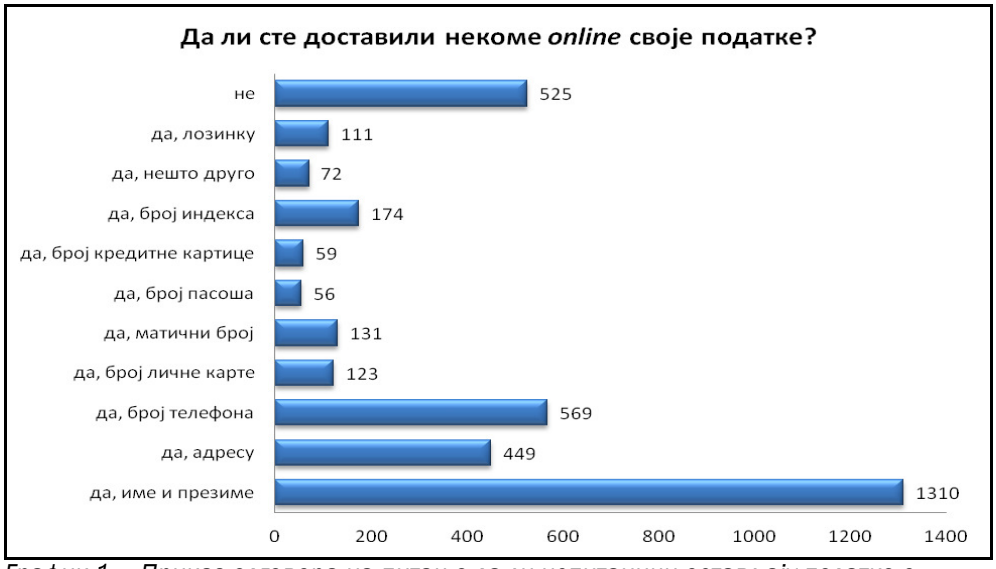


График 1. Приказ одговора на питање да ли испитаници остављају податке о личности на интернету

Проценат оних који нису достављали податке он-лине је 15%, односно већина од преко 85% испитаника је достављала податке о личности преко интернета. У највећој мери достављани су име и презиме – 71%, број телефона 31% и адреса 24%, знатно мањи број испитаника оставио је број индекса - 9%, матични број – 7%, број личне карте – 7% и лозинку – 6%, док је број кредитне картице и број пасоша доставило њих 3%. Проценат од 85%, колико износи проценат оних који су достављали податке, јесте велики, као и проценти достављања података који нису само име и презиме.

Резултати показују да податке који их јединствено одређују као што су јединствени матични број, број личне карте, које никада не би требало слати путем мреже, оставља мали број корисника интернета (3-4%), као и лозинку коју не би требало давати никоме. Забрињава података да су у питању корисници старији од 16 година, што указује да генерација која је најактивнија и има формиране навике у коришћењу интернета није свесна потенцијалних претњи и релативно је опуштена у *cyber* простору.

Које податке остављате о себи?

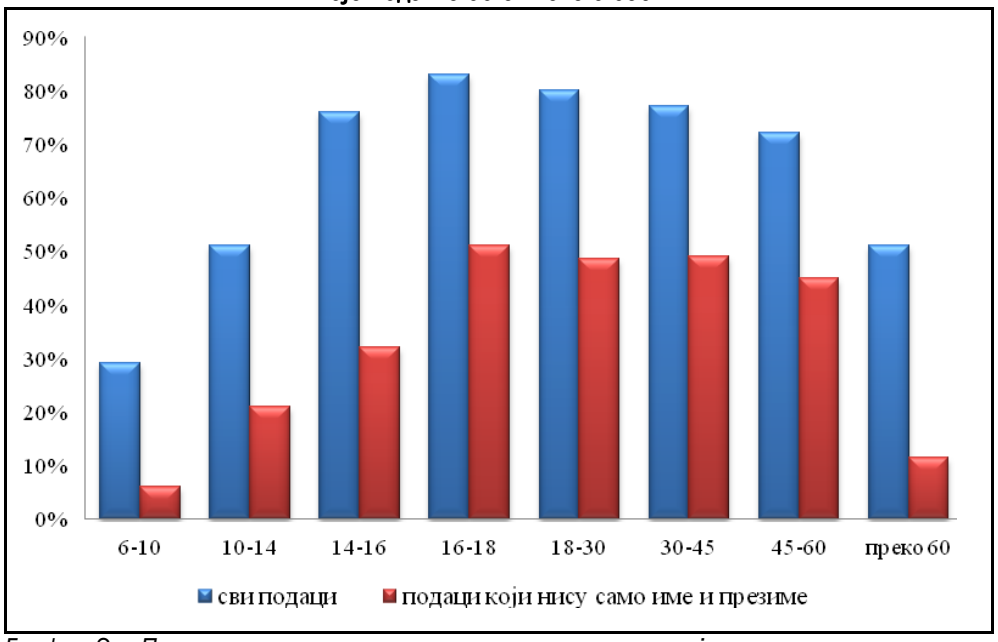


График 2. Проценат испитаника по старосним групама који су достављали податке о личности преко интернета

Највећи проценат оних који нису достављали податке преко интернета је међу младима 6-10 година старости – 59,1%, затим испитаницима старијим од 60 година – 47,8%, и од 10-14 година – 45,4%. Остале старосне групе испитаника имају проценте од 20,2%, 16,4%, 19%, 22% и 26,4% оних који нису достављали податке преко интернета за групе 14-16, 16-18, 18-30, 30-45 и 45-60 година респективно. Дакле, најмање оних који нису достављали податке је међу испитаницима 16-18 година старости, односно они су највише достављали податке – нешто мање од 85% њих је то чинило.

Најмлађи испитаници, 6-10 година старости, у највећем броју случајева су достављали име и презиме – 22,6% њих. Један испитаник је одговорио да је оставио име и презиме, адресу и број телефона, тј. 1,1% испитаника овог узраста; један је одговорио да је доставио име и презиме, адресу, број телефона, матични број, број пасоша, лозинку и нешто друго; њих двоје тј. 2,2% најмлађих испитаника је доставило име и презиме и број телефона; 1,1% је доставило име и презиме, адресу, број телефона, број личне карте и матични број; 1,1% је доставило име и презиме, адресу, број телефона и матични број. Укупно њих 6,6% је достављало податке који нису само име и презиме.

Испитаници 10-14 година старости су остављали следеће податке: у 30,9% случајева само име и презиме; у 1,5% случајева име и презиме и адресу; у 3,3% случајева име и презиме, адресу и број телефона; 1% случајева - име и презиме, адресу, број телефона и лозинку; 0,5% - име и презиме, адресу и нешто друго; 0,5% - име и презиме, адресу и лозинку; 1,9% име и презиме и број телефона; 0,5% име и презиме, број телефона и лозинку; 0,5% - име и презиме, матични број и број индекса; 0,5% име и презиме и нешто друго; 3,9% име и презиме и лозинку; 0,5% - адресу; 0,5% адресу и број телефона; 2,4% број телефона; 0,5% број телефона и лозинку; 0,5% број личне карте и матични број; по један испитаник тј. по 0,5% нешто друго и лозинку. Укупно 20,3% испитаника из ове старосне групе је достављало податке који нису само име и презиме.

Испитаници 14-16 година старости су остављали следеће податке: у 46,8% случајева име и презиме; 0,9% име и презиме и адресу; 5,5% име и презиме и број телефона; 6,4% име и презиме, адресу и број телефона; 0,9% име и презиме, адресу, број телефона, број личне карте, матични број, број пасоша, број кредитне картице, лозинку и нешто друго; 0,9% име и презиме, адресу, број телефона, број личне карте и лозинку; 0,9% име и презиме, адресу, број телефона и нешто друго; 0,9% име и презиме, адресу, број телефона и лозинку; 1,8% име и презиме, број телефона и лозинку; 0,9% име и презиме, број индекса и лозинку; 2,7% име и презиме и лозинку; 0,9% адресу; 1,8% адресу и број телефона; 1,8% број телефона; 0,9% број личне карте; 0,9% број личне карте, матични број и број кредитне картице; 0,9% лозинку. Укупно 31,2% њих је достављало податке преко интернета који нису само име и презиме.

Табела 1. Достављање података о личности одређеним институцијама / појединцима

	име и презиме	адреса	бр. тел.	бр. ЛК	ЈМБГ	пасош	кредитна картица	лозинка	индекс	друго
особи коју не познајем	112	46	58	7	17	3	5	7	13	9
на сајту приликом регистровања	810	292	327	73	81	30	43	62	115	47
продавници на њиховм сајту приликом наручивања	249	147	150	32	37	7	32	19	38	22
банци / школи / факултету	384	174	187	61	70	26	28	34	127	33
туристичкој агенцији	135	66	71	31	27	22	11	10	33	12
мобилном оператеру	171	90	101	37	37	18	21	17	36	9
интернет провајдеру	119	62	66	18	18	8	10	12	21	12
члану породице	463	179	259	58	60	27	22	67	84	36
пријатељу	728	249	380	71	71	32	32	85	124	51
познанику	244	76	136	17	21	10	10	20	34	15

Испитаници 16-18 година старости су остављали следеће податке преко интернета: 30,1% име и презиме и 50,7% њих је достављало остале податке у најразличитијим комбинацијама.

Испитаници 18-30 година старости су у 30,7% случајева достављали преко интернета само име и презиме, а у 48,6% случајева достављали су остале податке.

Старији испитаници су достављали податке који нису само име и презиме у процентима од 49,1%, 45,0% и 10,9% за старосне групе од 30-45, 45-60 и преко 60 година респективно.

Податке о личности од младих испитаника највише достављају они узраста од 16 до 30 година. Они су, такође, у највећој мери достављали податке који нису само име и презиме. Најмлађи испитаници су то радили у 6,6% случајева. Међутим, са порастом узраста испитаника проценат се значајно повећава, све до 18 године и достиже проценат и већи од 50%. Испитаници млађи од 30 година у великој мери достављају податке о личности путем интернета јер све групе испитаника, изузев најмлађих, достављају податке преко интернета у проценту већем од 50%. Старији испитаници, изузев оних најстаријих, више достављају податке него они млађи од 16 година. Ово се може објаснити чињеницом да испитаници који су млађи од 18 година још увек немају лична документа тако да не могу да проследе ништа сем евентуално броја личне карте (ако су старији од 16 година), а они најмлађи и не знају шта су поједини подаци, нпр. јединствени матични број грађана (када прослеђују те податке највероватније то чине на захтев неког старијег).

График 3. Приказ одговора на питање коме испитаници достављају податке о себи на интернету

У највећој мери подаци су достављани на сајту приликом регистровања 50% и пријатељу 48%, затим члану породице 30% и банци, школи или факултету 24%. Познанику и продавници на њиховом сајту приликом наручивања су подаци прослеђени у 16% случајева, затим следе мобилни оператери са 11%, туристичка агенција 9%, особа коју не познају 8%, интернет провајдери 7%, а у испод 5%

случајева подаци су прослеђивани органима управе, здравственим установама, страним амбасадама и невладиним организацијама.

Сви подаци наведени у питању - име и презиме, адреса, број телефона, број личне карте, матични број, број пасоша, број кредитне картице, број индекса, лозинка, нешто друго - прослеђивани су свакој од следећих страна: особи коју не познају, на сајту приликом регистровања, продавници на њиховм сајту приликом наручивања, банци/школи/факултету, туристичкој агенцији, мобилном оператеру, интернет провајдеру, члану породице, пријатељу и познанику, у проценту већем од 2,6%.

Начин на који су подаци прослеђени најчешће је преко друштвене мреже 44%, попуњавањем он-лајн формулара 43% и е-поштом у 40% случајева. Преко апликације податке је прослеђивало 7% испитаних, на неки други начин 2% и попуњавањем шерованих докумената 1% њих.

Најмлађи испитаници, старости 6-10 година, су податке прослеђивали попуњавањем он-лајн формулара у 0,8% случајева, е-поштом 0,6%, преко друштвене мреже 2,6%, преко апликације 0%, попуњавањем шерованих докумената 4,5% и на други начин двоје испитаника, односно 5,6%, од којих је један као одговор навео „претраживач“.

Испитаници узраста 10-14 година су податке прослеђивали попуњавањем он-лајн формулара у 2,9% случајева, е-поштом 5%, преко друштвене мреже 10,6%, преко апликације 10,4%, попуњавањем шерованих докумената 4,5% испитаника овог узраста и на други начин четири особе, тј. 11,1% испитаника, од чега је један дао одговор „преко Skype“ и један „рекао сам им лично“.

График 4. Приказ одговора на питање на који начин су испитаници достављали податке о себи на интернету

Испитаници узраста 14-16 година су податке прослеђивали попуњавањем он-лајн формулара у 3,7% случајева, е-поштом 3,8%, преко друштвене мреже 7,9%, преко апликације 7%, попуњавањем шерованих докумената 9,1%, на други начин 2,8%, тј. један испитаник који је додао „када се видим са неком особом“.

Испитаници узраста 16-18 година су податке прослеђивали попуњавањем онлајн формулара у 12,3% случајева, е-поштом 9,5%, преко друштвене мреже 14,2%, преко апликације 11,3%, попуњавањем шерованих докумената 13,6% и на други начин 19,4% (од чега је један одговор „лично рекао“).

Испитаници узраста 18-30 година су податке прослеђивали попуњавањем онлајн формулара у 62,1% случајева, *email*-ом 63,3%, преко друштвене мреже 58%, преко апликације 56,5%, попуњавањем шерованих докумената 59,1% и на други начин 47,2% од којих су неки одговори „позивом преко телефона“ и „личним контактом“.

Податке о личности од младих испитаника највише достављају они узраста од 16 до 30 година. Они су такође у највећој мери достављали податке који нису само име и презиме. Најмлађи испитаници су то радили у 6,6% случајева. Међутим, са порастом узраста испитаника проценат се значајно повећава, све до 18 године и достиже процентат и већи од 50%. Хипотеза „Већина испитаника млађих од 30 година доставља податке о личности путем интернета“ се прихвата, јер све групе испитаника, изузев најмлађих, достављају податке преко интернета у проценту већем од 50%. Старији испитаници, изузев оних најстаријих, више достављају податке него они млађи од 16 година. На основу датих података, хипотеза „Пунолетни испитаници више достављају податке него они млађи од 18 година“ се прихвата. Ови подаци се могу објаснити и чињеницом да испитаници који су млађи од 18 година још увек немају податке као што су број личне карте, број индекса и број кредитне картице, а они најмлађи не знају шта су поједини поадаци, као што је нпр. јединствени матични број грађана (када прослеђују те подаци највероватније то чине на захтев неког старијег).

На питање „Да ли читате услове под којим остављате податке?“, проценат испитаника који се изјаснио да пажљиво чита услове је 42,9%, само информативно чита 18,7% и понекад 18% испитаних. Услове не чита 18,7% испитаника, од чега 1,6% не разуме услове и 4,1% не зна да услови постоје.

График 5. Приказ одговора на питање да ли испитаници читају услове под којим остављају податке о себи на интернету

Највећи проценат испитаника који се изјаснио да пажљиво чита услове је 44,8% - испитаници узраста 18-30 година, 44,9% - узраста 14-16 година, 51,3% - 10-14 година, 40,2% - 16-18 гофина, а млади узраста 6-10 година 25,6%.

Проценти оних који су одговорили да их читају понекад су 12,8%, 14,9%, 15,3%, 21,1%, 18,5%, 19,2%, 17,2% и 9,1% за старосне групе респективно. Дакле, проценти испитаника који се нису изјаснили да читају услове под којим остављају податке пажљиво или информативно, односно читају их понекад или их не читају, су 71,8%, 38,3%, 34,7%, 43,2%, 35,5%, 43,1%, 43% и 36,4% за старосне групе испитаника од најмлађих до најстаријих.

Највише оних који не знају да услови постоје су испитаници узраста 6-10 година, њих 38,5%, а са годинама се тај број смањује, од 11,7% - 10-14 година, 0% - испитаници 16-18 година старости. Старији то раде: 4,6% испитаници 30-45 година, 6,5% испитаници 45-60 и преко 60 година 18,2%.

Проценти испитаника који су одговорили да не читају услове под којим остављају податке (не разумеју их, само их прихвате или не знају ни да постоје) су 59%, 23,4%, 19,4%, 22,1%, 17%, 23,8%, 25,8% и 27,3% за испитанике стросних група 6-10, 10-14, 14-16, 16-18, 18-30, 30-45, 45-60 и преко 60 година, респективно.

Проблем достављања података преко интернета дакле постоји, али не за све узрасте, јер се показало да они најмлађи далеко мање достављају податке од старијих испитаника[127]. Број оних који достављају податке о личности путем интернета је у порасту све до 18 године, када постају релативно једнаки, изузев код испитаника старијих од 60 година који пет пута мање прослеђују податке него испитаници узраста 18-60 година (што је разумљиво јер они много мање користе рачунаре и интернет генерално). Међутим, с обзиром на количину података о личности за коју испитаници млађи од 16 година уопште знају шта су и које поседују, проценти достављања података су такође високи. Ти подаци се достављају на разне несигурне начине, међу којима предњачи попуњавање он-лајн формулара.

127 Drakulic M. Jovanovic S. 2008, *Public eq. private? Twilling of privacy in the time of online social networking*, paper presented at the conference 56th Scientific expert meeting Parliament psychologists, development and standardization in psychology, Kopaonik, 4-7.6.2008;

График 6. Приказ испитаника по старосним групама који не читају услове под којим остављају податке или их читају понекад

У односу на трендове у Републици Србији интересантно је упоредити резултате са трендовима у свету, нарочито у Сједињеним Америчким Државама у којој је највећи степен коришћења интернета, као и земљама Европске уније које регулишу питања приватности на исти или сличан начин.

У септембру 2013. године *Pew Research Center* је објавио резултате истраживања о приватности на интернету међу грађанима САД-а *Anonymity, Privacy, and Security Online*[128]. Једно од питања било је и које податке о себи остављају на мрежи.

Резултати показују да су становници САД-а опуштенији по питању остављања података: фотографије оставља 66% њих, е-пошту 46%, адресу становања 30%, док број телефона чешће остављају испитаници из Србије (28% према 24%). Један од разлога за значајна одступања можда су због дужине периода и степена коришћења интернета од стране оних који су ове појаве и измислили.

Истраживање о ставовима грађана ЕУ према заштити података о личности[129] проверавало је поверење које грађани ЕУ имају у своје институције и дошло се до следећих резултата: већина Европљана има поверења у здравствене установе (78%), институције које се баве порезима и социјалним осигурањем (70%), у банке и финансијске институције (62%) и Европску комисију и Европски парламент (55%).

128 Rainie L, Kiesler S. Kang R. Madden M. Anonymity, Privacy, and Security Online, Pew Research Center's Internet & American Life Project, Washington, 2013, http://pewinternet.org/Reports/2013/Anonymity-online.aspx;

129 SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre REPORT, Publication: June 2011;

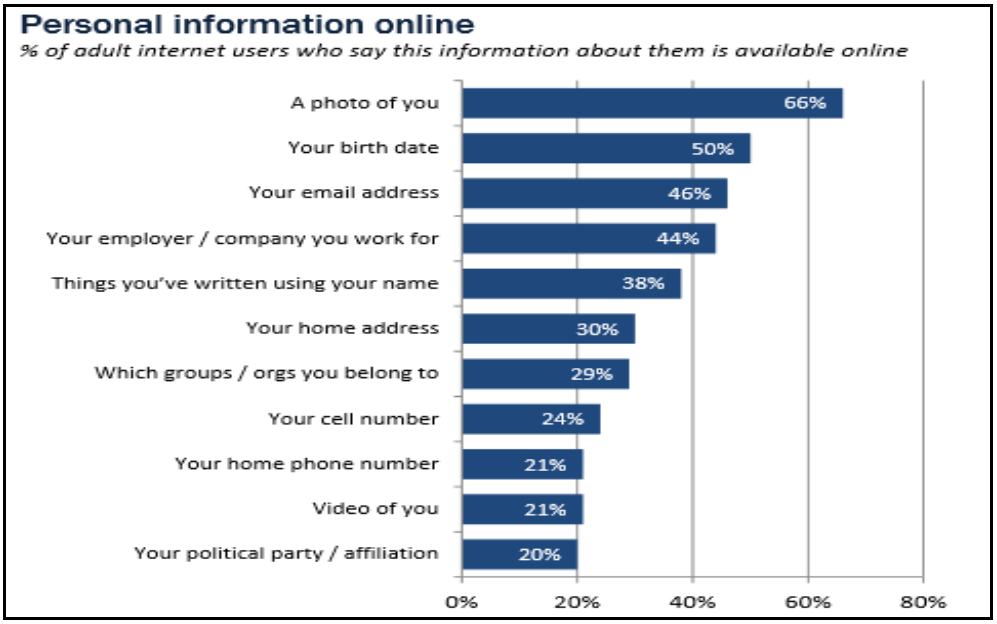


График 7. Подаци о личности које одрасли остављају он-лајн

Међутим, у мањој мери верују продавницама и робним кућама (39%), провајдерима мобилних и интернет услуга (32%), интернет претраживачима, сајтовима за друштвено умрежавање и е-пошти (22%).

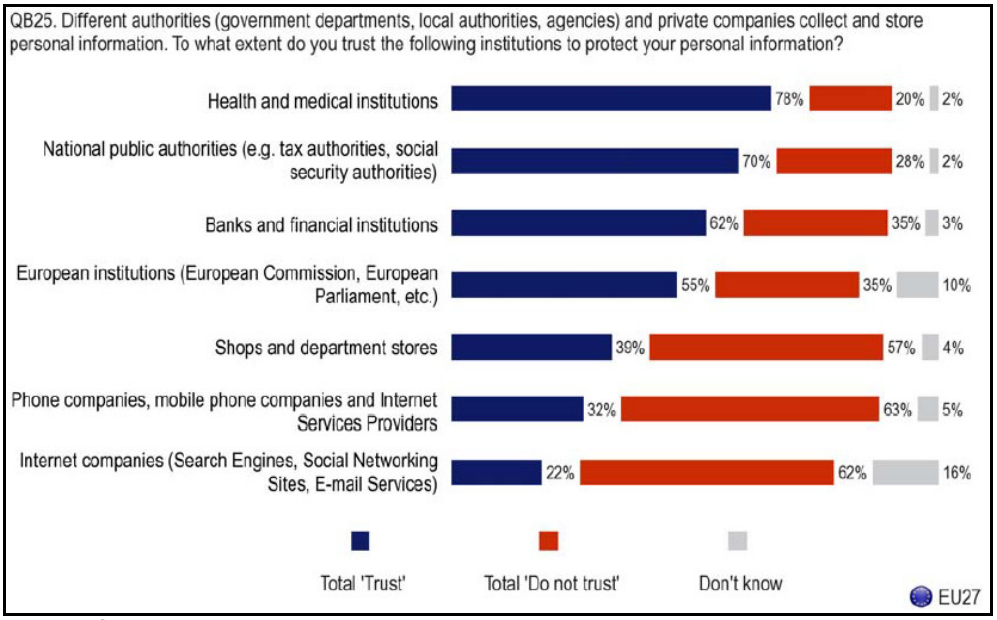


График 8. Поверење Европљана у различите организације које прикупљају податке о личности

Резултати указују да је глобализација, која је остварена у погледу коришћења интернета и односа према приватности, креирала нову генерацију корисника која слично размишља без обзира где живи. Одступања су и даље присутна у земљама у којима се интернет у мањој мери користи, али је уједначеност резултата, у погледу сигурности коју корисници имају на мрежи и према сопственом расуђивању и према компанијама које податке о њима прикупљају и обрађују, показатељ да и даље није у довољној мери развијена свест корисника бројних он-лајн услуга.

3.2.2 Злоупотребе мобилних уређаја и рачунара

На питање за шта се мобилни уређај/рачунар може користити односно - да ли мислите да се мобилни уређај/рачунар може злоупотребити, испитаници су одговорили на следећи начин: највећи број њих изјавио је да мисли да се мобилни уређаји и компјутери могу употребити за „скидање“ филмова и музике 87% и за крађу идентитета на разним мрежама 72%, следе "упад у рачунар" 57%, преузимање података о личности-54%, злоупотреба платних картица 49% и пословна шпијунажа 43%, изузев за насиље. Да се мобилни уређаји и компјутери могу користити за насиље сматра преко трећине корисника 36%. Проценат оних који су се изјаснили да сматрају да се мобилни уређаји и компјутери не могу злоупотребити је 5%.

Млађи испитаници сматрају да се мобилни уређај или рачунар може користити за крађу идентитета у 24,4% случајева, за скидање филмова/музике 33,7%, за пословну шпијунажу 22%, преузимање података о личности23,3%, за злоупотребу картица 22,3%, „упаде у рачунаре“ 25,6% и насиље 29,7%. Проценат младих испитаника који су се изјаснили да сматрају да се мобилни уређаји и компјутери не могу злоупотребити је 44,1%. Оних који су одговорили да се рачунар или мобилни телефон могу злоупотребити за све наведено је 8,6%, 14%, 10,1%, 17,4% и 20,7% за старосне узрасте од 6-10, 10-14, 14-16, 16-18 и 18-30 година, респективно.

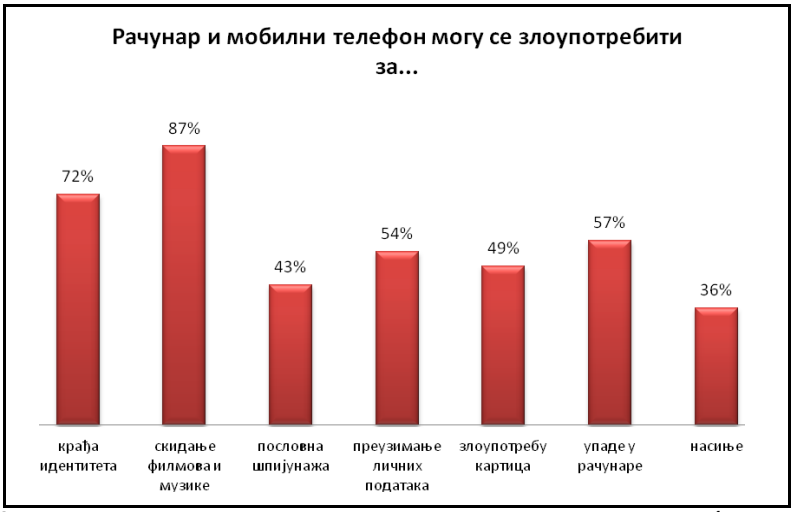


График 9. Учесталост одговора испитаника на питање за шта се мобилни уређај или рачунар може користити (злоупотребити)

С обзиром на то да ниједна старосна група није одговорила да се рачунар или мобилни телефон може злоупотребити за све наведене ставке у проценту већем од 21%, хипотеза „Већина испитаника млађих од 30 година не зна да се рачунар или мобилни телефон може користити за крађу идентитета, пословну шпијунажу, преузимање података о личности, злоупотребу картица, „упаде у рачунаре“ и за насиље“ се прихвата.

На питање „Познајете ли некога ко користи рачунар у те сврхе?“ одрично је одговорило 61% испитаника, да познају једну такву особу 6,8% и да познају неколико 22,9% испитаника.

Млади испитаници су у укупно 37,1% случајева одговорили да познају више таквих особа и 11% једну такву особу. Испитаници 6-10 година старости су у 8,9% случајева одговорили да познају неколико особа које користе рачунар у сврхе наведене у претходном питању, а 16,5% да знају једну такву особу. Испитаници 10-14 година у 30,5% случајева су одговорили да знају неколико таквих особа и 7,4% да знају једну. Испитаници 14-16 година у 36,5% случајева знају неколико таквих особа и 6,3% једну; 16-18 година – 36,4% зна за неколико особа и 9,2% за једну. Испитаници 18-30 година у 25,5% случајева знају неколико таквих особа и 6,6% зна једну. Дакле, највише оних који су потврдно одговорили на ово питање су испитаници узраста од 10 до 30 година. Међутим, ни они нису одговорили потврдно на ово питање у проценту већем од 40%.

Испитаници су затим одговарали на питање „Које је ваше мишљење о тим особама?“. Уз ово питање постоји напомена да га не попуњавају деца у основној и средњој школи, међутим неки од њих су ипак одговорили. Проценат оних који сматрају да су то позитивне активности којима би се и сами бавили („то је супер, и ја бих се тиме бавио/ла“) је 5,3%, оних који сматрају да је то у реду, али се не би бавили тиме („то је ОК, али ја то никада не бих урадио/ла“) је 5%, да је то „његова/њена ствар“ одговорило је 29% испитаних, 24,9% зна да је то забрањено и не би се тиме бавили, док је 10% испитаника одговорило да би починиоце наведених дела пријавило некоме када би знали коме.

График 10. Мишљење испитаника узраста 18-30 година о починиоцима наведених дела

Дакле, највише је оних који су индиферентни, тј. који не подржавају, али ни не осуђују особе које се баве наведеним активностима. Проценат оних који нису одговорили на ово питање је 25,2%. Испитаници узраста 18-30 година су одговарали на ово питање у 7,5% случајева са „то је супер, и ја бих се тиме бавио/ла“, у 6,8% са „то је ОК, али ја то никада не бих урадио/ла“, у 38% са „то је његова/њена ствар“, 34,2% са „знам да је то забрањено и никада то не бих урадио/ла“ и 13,5% са „пријавио/ла бих га да знам коме“.

Највећи проценат испитаника који су се изјаснили да је то „супер“ и да би се тиме бавили јесте 17,4% и они су 16-18 година старости. Испитаници узраста 18-30 година су овај одговор изабрали у проценту од 7,5%, а остали млади: 0% - испитаници 6-10 година, 8,3% - испитаници 10-14 година, и 6,9% - испитаници 14-16 година. Старији испитаници су овај одговор изабрали у процентима од 0% - испитаници старији од 60 година, 0,9% - 45-60 година и 2,7% - 30-45 година, дакле у доста нижим прцентима.

Оних који сматрају да је то „његова/њена ствар“ је од 22,9% - млади 6-10 година, до 54,3% - млади 16-18 година.

Оних који су се изјаснили да је то забрањено и да никада то не би урадили је највише међу старијим испитаницима – 39%, 42,6% и 16,1% за испитанике 30-45, 45-60 и преко 60 година. Млади су тај одговор изабрали у процентима од 57,1%, 27,4%, 25,9%, 16,7% и 34,2%, за испитанике 6-10, 10-14, 14-16, 16-18 и 18-30 година респективно.

Оних који су се изјаснили да би пријавили починиоца али не знају коме, има највише међу старијим испитаницима, 54,8% испитаника преко 60 година, 21,7% - 45-60 и 15,1% - 30-45 година. Млади су овај одговор изабрали у процентима од 6,9-14,5%.

Старији испитаници би пријавили починиоце наведених дела, док су млади много више индиферентни или сматрају да су то позитивне или занимљиве активности.

Једно од питања у истраживању о ставовима грађана ЕУ према заштити података о личности[130] било је: У последњих годину дана да ли сте чули за неки случај или имали искуства са губитком података о личностии крађом идентитета.

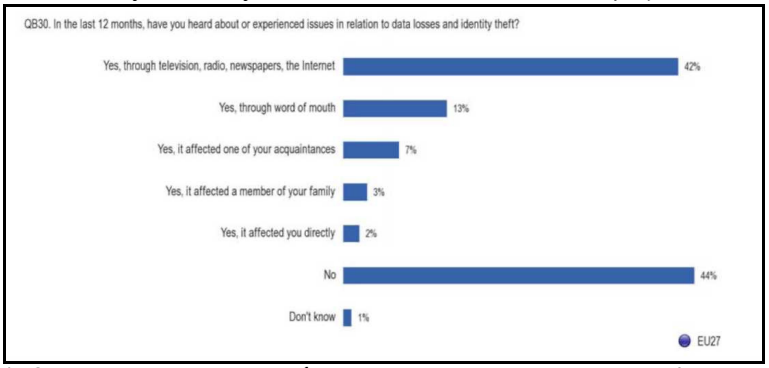


График 11. Одговори на питање губитка података о личности и крађе идентитета на интернету

130 SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre REPORT, Publication: June 2011;

44% испитаника одговорило је одрично, 42% њих је чуло нешто о овом питању путем телевизије, радија, новина и интернета, а 13% је чуло преко неког другог. Неколицина испитаника (7%) изјавила је да се то догодило њиховим познаницима, 3% њих каже да су се са крађом идентитета суочили чланови њихових породица или су директно они били жртве (2%).

Земље у којима су се испитаници изјаснили да нису чули ништа о томе су Летонија (26%) , Шведска (27%), Ирска (28%), Данска (29%), Финска (31%) и Велика Британија (34%). Преко телевизије, радија, новина и интернета су у највећој мери чули грађани Летоније (69%), Шведске (62%), Данске (61%) и Финске (59%).

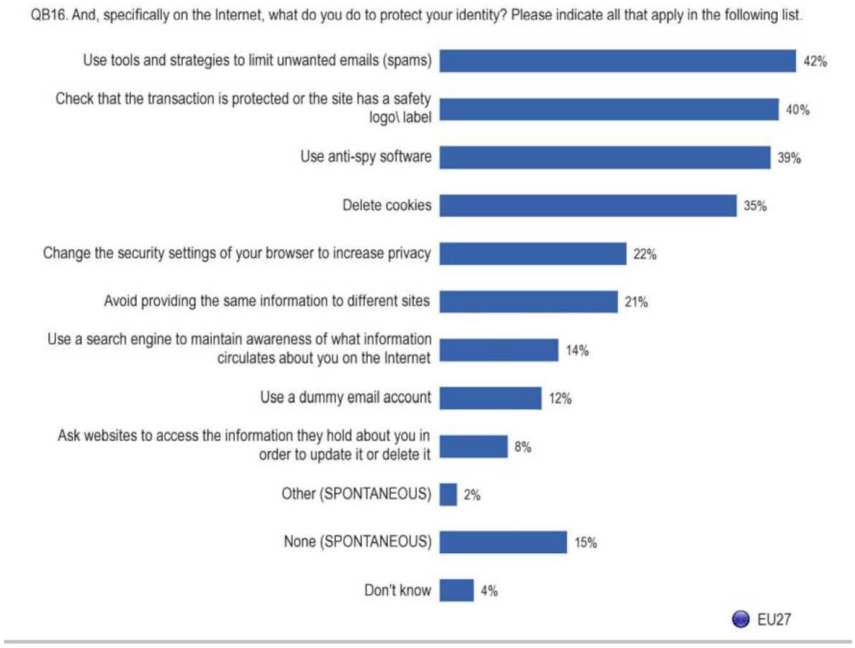


График 12. Одговори на питање шта корисници интернета чине да заштите свој идентитет [131]

Поредећи ове резултате закључује се да је у значајној мери присутније сазнање о крађи идентитета међу испитаницима у Србији. Поставља се питање да ли узрок лежи у деведесетим годинама у којима је владала посебна клима и када је степен злоупотребе података о личности био изражен или је у питању релативно висок степен коришћења интернета и друштвених мрежа на овом подручју.

131 SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre REPORT, Publication: June 2011, QB16 And, specifically on the Internet, what do you do to protect your identity?;

Можда је одговор у додатним заштитама које користе грађани ЕУ. На питање: Шта радите да заштитите свој идентитет на интернету, 42% европских интернет - корисника има посебне алате против нежељених порука е-поште (енг. *spam*), 40% њих проверава да ли сајтови за финансијске трансакције имају посебну ознаку да су безбедни, 39% користи антишпијун софтвер, а трећина испитаника редовно брише колачиће (енг. *cookies*). Петина корисника мења безбедносна подешавања претраживача како би повећали своју приватност или избегли пружање истих информација на различитим локацијама (21%).

Коначно, интересантно је напоменути да значајна мањина (15%) спонтано кажу да не чине ништа да заштите свој идентитет на интернету.

3.2.3 Друштвене мреже и злоупотреба података о личности

Полиса приватности на *Facebook*[132], једној од најпопуларнијих друштвених мрежа, дефинише два основна начела:

1. корисник треба да има контролу над подацима које оставља. *Facebook* помаже корисницима да поделе информације са пријатељима. У профилу одређује контакт и одређене податке о себи, слике, интересе и групе којима приступа. „Контролише“ са ким ће делити те информације преко поставки приватности на страници Приватност;
2. корисник треба да има приступ подацима које други желе да поделе.

Политика приватности одређује начин на који *Facebook* прикупља и користи податке о личности које корисници остављају. *Facebook* је лиценцирао *TRUSTe* програм приватности (*TRUSTe Privacy Program*[133]). TRUSTe је независна, непрофитна организација чија је мисија изградња поверења корисника у интернет, промовишући поштену и транспарентну употребу информација[134].

Facebook у полиси приватности објашњава које податке и на који начин прикупља и користи, објашњава политику према малолетницима (лицима испод 13 година је забрањено да се региструју), дељење информација са трећим странкама, везе, оглашавање трећих странака, мењање и одстрањивање података, физичку сигурност података (ССЛ), као и правила коришћења, обавештења и ревизије. Полиса је доступна на адреси http://www.facebook.com/policy.php.

Одређени делови полисе приватности свакодневно наилазе на оштру критику јавности. На пример, користећи *Facebook* корисник пристаје на пренос и обраду података у Сједињеним Америчким Државама – „Ми делимо информације с трећим странама само у ограниченим околностима где верујемо да је такво деловање: разумно нужно у виду пружања услуге, од нас захтевано од стране закона или

---

132 Facebook Data Use Policy, http://www.facebook.com/policy.php , datum poslednjeg pristupa 20.2.2014;

133 TRUSTe, Privacy Program Requirements, http://www.truste.com/privacy-program-requirements/ datum poslednjeg pristupa 20.2.2014;

134 Јовановић С. 2008, *Коришћење друштвених мрежа на универзитетима у Србији*, 16. телекомуникациони форум ТЕЛФОР 2008: Комуникација на друштвеним мрежама, Друштво за телекомуникације - Београд, Телеком Србија а.д., ЈП ПТТ саобраћаја Србија, Електротехнички факултет Универзитета у Београду, IEEE Serbia & Montenegro Com Chapter, Београд;

одобрено с ваше стране“[135]. Тиме је дата могућност да свако дође до података о кориснику који се деле на овој мрежи.

„Можемо користити информације о вама које сакупимо из других извора, укључујући, али не ограничавајући се, на новине, интернет изворе попут блогова, сервис за инстант-поруке, програмере *Facebook*-платформе и друге кориснике *Facebook-a* како би допунили ваш профил“ - што се може интерпретирати као покушај *Facebook-a* да додатно профилише кориснике, чиме је значајно угрожено право на приватност.

Остављањем било ког садржаја, корисник аутоматски даје дозволу да користи, копира, јавно приказује, реформатира, преводи, преписује (у целини или деловима) и дистрибуира тај садржај из било ког разлога, комерцијалног, за оглашавање, или неког другог, што значи да је *Facebook* власник укупног садржаја постављеног на својим серверима и може да ради било шта са њим, па и да га прода трећим лицима[136].

Приликом ажурирања података, чува се копија претходне верзије током неког периода што значи да корисник не може да контролише који подаци се чувају колико дуго.

Facebook не одговара ако било ко пробије безбедносне мере и стекне увид у приватне податке корисника[137] јер у једном делу наводи: „не можемо контролисати акције других корисника са којима одлучите да делите своје странице и информације. Због тога и не гарантујемо да кориснички садржај који објавите на страницама неће гледати неауторизоване особе. Нисмо одговорни за заобилажење било којих поставки приватности или сигурносних мера на овој страници“.

Због свега тога забрињавају одговори испитаника на сет питања који се односи на остављање података на друштвеним мрежама. На питање „Које податке приказујете?“ корисници су на првом месту навели име, презиме и датум рођења 91% њих, интересовања 39%, фотографије 61%, адресу 7%, контакт-телефон 5%, е-адресу 19%, статус везе (сам/а, у вези, ожењен/удата итд.) 26%, а податке измишља 4% испитаника.

Мушкарци у већој мери остављају име, презиме и датум рођења (48,8%) за разлику од жена које то чине у 51,2% случајева. Интересовања оставља на мрежи 53,3% мушкараца и 46,7% жена, фотографије мушких испитаника 50% жена - 50%.

На питање "да ли сте покушали да деактивирате налог?" мушки део испитаника је потврдно одговорио у 36,2% случајева, а женски део испитаника у 43% случајева.

Испитаници од 6 до 10 година су то покушали у 12%, од 10 до 14 у 18,5%, од 14 до 16 у 34,8%, од 16 до 18 у 51%, од 18 до 30 у 44,3%.

---

135 Facebook Data Use Policy, http://www.facebook.com/policy.php , datum poslednjeg pristupa 20.2.2014;

136 Јовановић С. 2008, *Коришћење друштвених мрежа на универзитетима у Србији*, 16. телекомуникациони форум ТЕЛФОР 2008: Комуникација на друштвеним мрежама, Друштво за телекомуникације - Београд, Телеком Србија а.д., ЈП ПТТ саобраћаја Србија, Електротехнички факултет Универзитета у Београду, IEEE Serbia & Montenegro Com Chapter, Београд;

137 Јовановић С. 2008, *Коришћење друштвених мрежа на универзитетима у Србији*, 16. телекомуникациони форум ТЕЛФОР 2008: Комуникација на друштвеним мрежама, Друштво за телекомуникације - Београд, Телеком Србија а.д., ЈП ПТТ саобраћаја Србија, Електротехнички факултет Универзитета у Београду, IEEE Serbia & Montenegro Com Chapter, Београд;

Од испитаника млађих од 30 година, они чије профиле на друштвеним мрежама могу да виде сви и који притом остављају неке од наведених података на свом профилу је 22,8%, а оних чије профиле могу да виде пријатељи пријатеља и притом на профилу објављују наведене податке је 13%. Проценат од 3,2% младих испитаника има преко 2000 пријатеља на некој од друштвених мрежа и истовремено остављају наведене податке, 11,2% њих има од 1000 до 2000 пријатеља и оставља наведене податке, а 25,8% њих има од 500 до 1000 пријатеља и притом остављају податке наведене у овом питању. Укупно 35,8% испитаника млађих од 30 година остављају податке о личности на друштвеним мрежама на веома несигуран начин, тј. на начин да их свако може видети (а самим тим и сакупити и злоупотребити). Дакле, хипотеза „Више од трећине испитаника млађих од 30 година податке о личности на друштвеним мрежама оставља на несигуране начине“ се прихвата.

На питање „Да ли Вас брине могућност злоупотребе података које сте оставили?“ проценат оних који су одговорили потврдно је 57,4%, 56,4%, 59,8%, 72,6%, 75,6% за групе испитаника 6-10, 10-14, 14-16, 16-18,18-30 година респективно. Оних који су се изјаснили да мисле да то није могуће је 9,3%, 7%, 6,9%, 3,4%, 2,1% за групе испитаника 6-10, 10-14, 14-16, 16-18,18-30 година респективно. Оних који су се изјаснили да нису забринути и да им то није битно је 33,3%, 36,6%, 33,3%, 24%, 22,3% за групе испитаника 6-10, 10-14, 14-16, 16-18,18-30 година респективно. Дакле, највише оних који су забринути је међу испитаницима 16-30 година – близу 73% њих, док су млађи испитаници у већем проценту одговарали да нису јер то није могуће или није битно. Што су испитаници старији, то је већи проценат оних који су забринути за своје податке, а мањи проценат оних који сматрају да је то немогуће.

Када су у питању проблеми са злоупотребом података, 7,7% испитаника се изјаснило да јесте имало неких проблема. Проценти младих испитаника по старосним групама који су одговорили потврдно су редом 5,8%, 13,5%, 12%, 7,4% за старосне групе 10-14, 14-16, 16-18 и 18-30 година, односно највише њих из група 14-16 и 16-18 година старости.

Најчешћа злоупотреба је добијање нежељених порука (енг. *spam*), затим крађа идентитета и он-лајн узнемиравање. Најмањи проценат испитаних изјавио је да је злоупотреба података подразумевала физичко узнемиравање – 0,4%, док су проценти осталих видова узнемиравања између 0,7% и 0,8% (крађа платних картица, дистрибуција података о личностии сексуално узнемиравање) и мање од 0,5% њих је одговорило да су то били неки други видови узнемиравања.

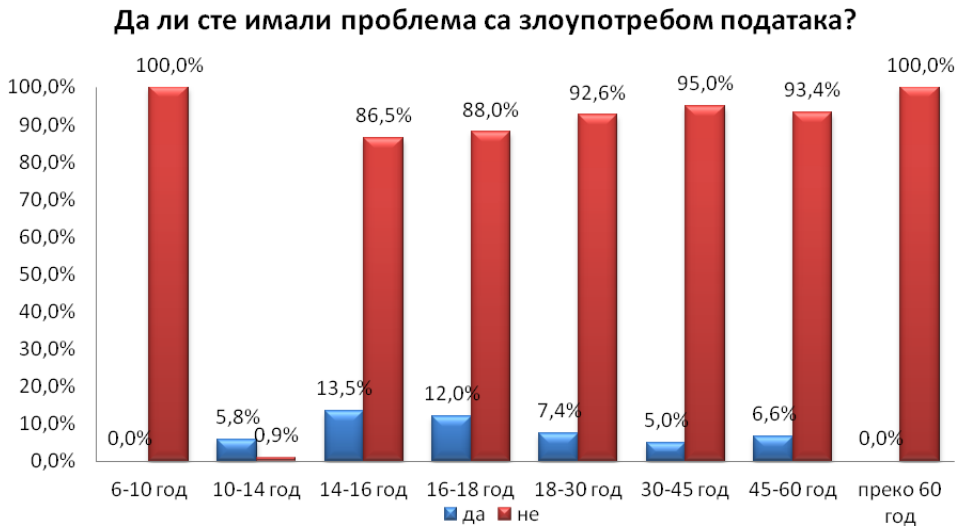


График 13. Проценти испитаника по старосним групама у вези проблема са злоупотребом података

Испитаници узраста 10-14 година су у 4% случајева одговорили да је то била крађа идентитета, 0,6% крађа платних картица, 0,6% дистрибуција података о личности, 2,3% добијање нежељених порука (*спам*), 0,6% он-лајн узнемиравање, 0,6% физичко узнемиравање и 0,6% сексуално узнемиравање.

Испитаници узраста 14-16 година су у 6,9% случајева одговорили да је то била крађа идентитета, 2,9% крађа платних картица, 2% дистрибуција података о личности, 8,1% добијање нежељених порука (*спам*), он-лајн узнемиравање 1%, 2% сексуално узнемиравање и 1% остали видови узнемиравања.

Испитаници узраста 16-18 година су у 10,2% случајева одговорили да је то била крађа идентитета, 2% крађа платних картица, 2,4% дистрибуција података о личности, 6,4% добијање нежељених порука (*спам*), 5,3% он-лајн узнемиравање, 2,5% сексуално узнемиравање, физичко узнемиравање 0,5%, 1,4% остали видови узнемиравања.

Испитаници узраста 18-30 година су у 4,1% случајева одговорили да је то била крађа идентитета, 1,1% крађа платних картица, 1,2% дистрибуција података о личности, 4,6% добијање нежељених порука (*спам*), 2,4% он-лајн узнемиравање, 0,7% физичко узнемиравање, 1,1% сексуално узнемиравање, 0,4% остали видови узнемиравања.

Крађа идентитета је или најчешћи вид злоупотребе података на друштвеним мрежама или на другом месту (после добијања нежељених порука). Дакле, хипотеза "Крађа идентитета је један од најчешћих облика злоупотребе података на друштвеним мрежама" се прихвата.

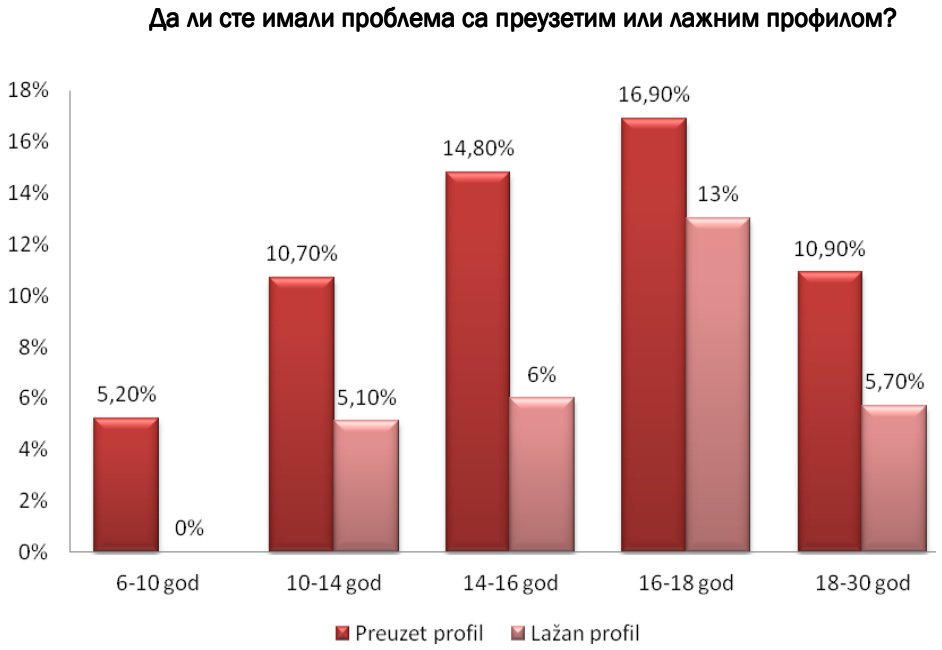


График 14. Број млађих испитаника по старосним групама којима је неко преузео профил и испитаници за које је неко отворио лажан профил представљајући се као они

Проценат испитаника који су се на друштвеној мрежи суочили са тиме да им је неко преузео профил је 10,7%, да је „неко је отворио лажан профил представљајући се као ја“ – 5,3%, са постављањем њихових фотографија без питања и таговањем 17,2%, са тиме да их непознати зову на број телефона који су оставили на профилу 2,5%, да су добијали разне „сексуалне“ понуде 6%, пословне понуде 4,9% и са „нешто друго“ је одговорило 5,1% испитаника.

Испитаници 6-10 година су одговорили да им је неко преузео профил у 5,2% случајева, постављају њихове фотографије без питања и тагују их у 13,8% случајева, добијали су разне „сексуалне“ понуде 1,7% и добијали су пословне понуде у 3,4% случајева.

Испитаници 10-14 година су одговорили да им је неко преузео профил у 10,7% случајева, неко је отворио лажан профил представљајући се као они 5,1%, постављају њихове фотографије без питања и тагују их 17,6%, непознати зову на број телефона који су оставили на профилу 1,5%, добијали су разне „сексуалне“ понуде 1,2%, добијали су пословне понуде 3%.

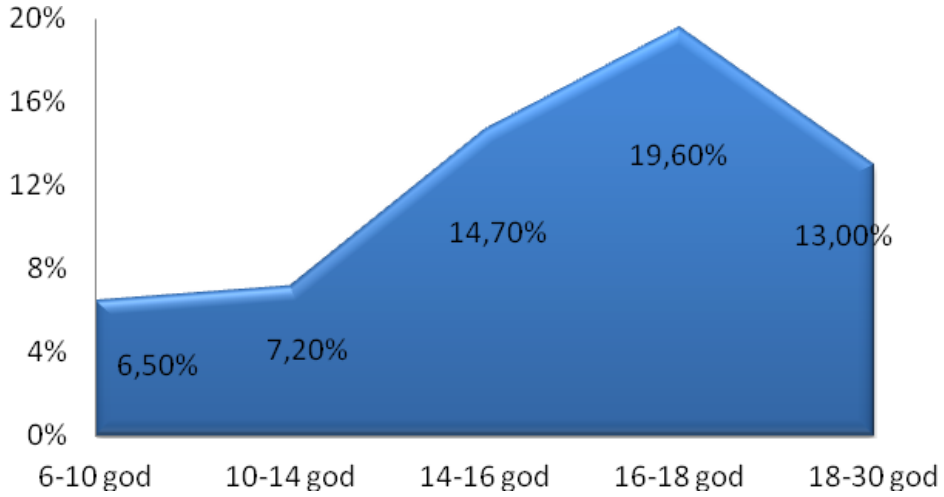


График 15. Приказ испитаника којима је преузет идентитет на друштвеној мрежи

Испитаници 14-16 година су одговорили да им је неко преузео профил у 14,8% случајева, неко је отворио лажан профил представљајући се као они 6%, постављају њихове фотографије без питања и тагују их 28,4%, непознати зову на број телефона који су оставили на профилу 7,3%, добијали су разне „сексуалне“ понуде 9,1%, добијали су пословне понуде 3,7%.

Испитаници 16-18 година су одговорили да им је неко преузео профил у 16,9% случајева, неко је отворио лажан профил представљајући се као они 13%, постављају њихове фотографије без питања и тагују их 23,5%, непознати зову на број телефона који су оставили на профилу 3,4%, добијали су разне „сексуалне“ понуде 6,6%, добијали су пословне понуде 3,8%.

Испитаници 18-30 година су одговорили да им је неко преузео профил у 10,9% случајева, неко је отворио лажан профил представљајући се као они 5,7%, постављају њихове фотографије без питања и тагују их 18,8%, непознати зову на број телефона који су оставили на профилу 1,2%, добијали су разне „сексуалне“ понуде 6%, добијали су пословне понуде 5,8%.

У односу на укупан број испитаника, проценат оних који су изјавили да им је некада неко преузео идентитет на некој друштвеној мрежи је 11,3%, да им се то није десило 71,5% и да не знају да ли им се то десило 14%.

Највише испитаника који су одговорили потврдно је међу онима 16-18 година старости 19,6%, а осталих 6,5%, 7,2%, 14,7% и 13% за узрасте 6-10, 10-14, 14-16 и 18-30 година респективно. Највише оних који су одговорили да не знају да ли им се то десило је међу младима 6-10 година је 21,5%, а осталих од 8,3% узраст 16-18 година, до 14% узраст 10-14 година.

У односу на број оних који поседују друштвене мреже, 10,3%, 8,4%, 15,7%, 20,5% и 13,5% испитаника узраста 6-10, 10-14, 14-16, 16-18 и 18-30 година респективно је доживело да им неко преузме идентитет на друштвеној мрежи (ови проценти дупло су већи од одговора на питање које злоупотребе података су испитаници доживели, међу којима је један од понуђених одговора био и крађа идентитета).

Истраживање *9 Things You Need To Know About Teens, Technology & Online Privacy*[138] које је *Teens & Technology Mary Madden, Senior Researcher Pew Research Center* реализовао 2013. године у САД-у, потврђује да је интернет медиј где се млади осећају сигурно и на коме остављају значајан број података о себи.

Резултати показују да 91% средњошколаца поставља своје фотографије на мрежи, 71% њих име школе у коју иду и град у коме живе, преко половине њих своју е- адресу, а петина број телефона.

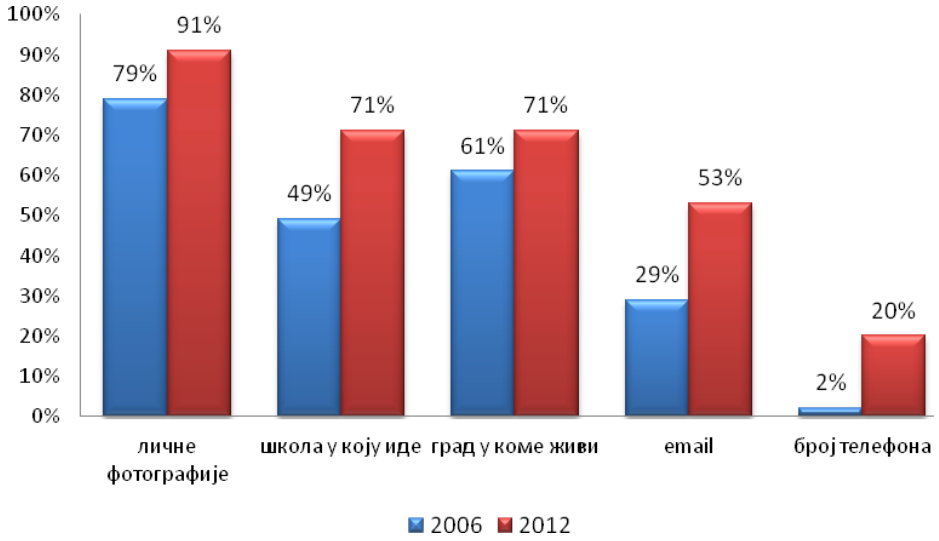


График 16. Постављање података о личности на мрежи средњошколаца у САД

Иста студија представила је тренд коришћења друштвених мрежа тинејџера и одраслих у периоду од 2006. до 2012. године, који показује значајни пораст укључивања одраслих и да се разлика значајно смањила у односу на почетне године коришћења овог вида комуникације.

138 Lenhart A. 9 Things You Need To Know About Teens, Technology & Online Privacy, Teens & Technology Mary Madden, Senior Researcher Pew Research Center, Family Online Safety Institute, 2013., http://www.pewinternet.org/Presentations/2013/Nov/9-Things-About-Teens-Technology-Online-Privacy.aspx, 26.1.2014;

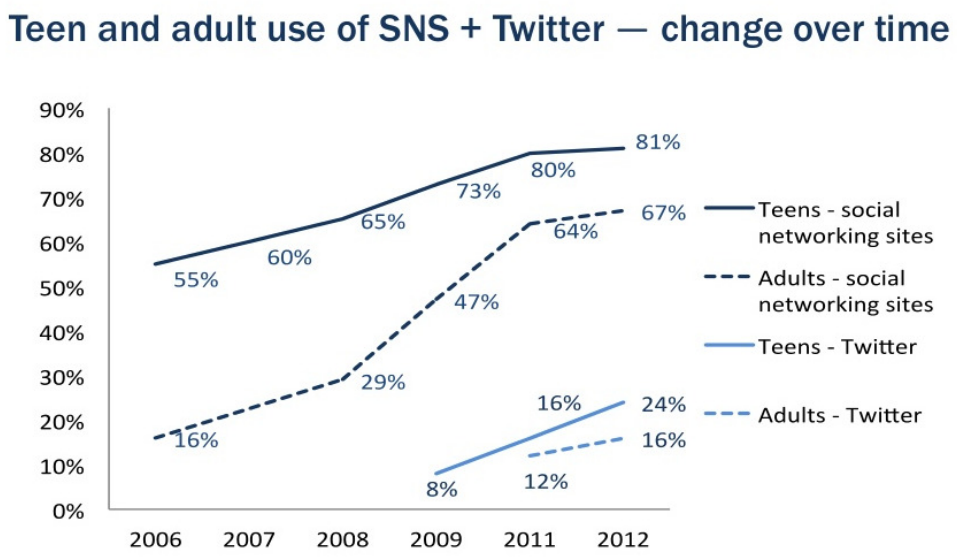


График 17. Коришћење друштвених мрежа тинејџера и одраслих у периоду 2006-2012.[139]

Када се упореде са резултатима исте старосне групе у Србији, јасно је да грађани САД-а отвореније и у већој мери користе интернет и друштвене мреже, делимично јер су све ове појаве тамо и настале.

На основу истраживања о ставовима грађана ЕУ према заштити података о личности које су спровели *TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre*[140] дигитални "староседеоци" су рођени и одрасли са дигиталном технологијом. Они су млађи Европљани узраста 15-24 и студенти. Око 94% од 15-24 користи интернет. 84% њих су користили друштвене мреже, а 73% њих су користили сајтове за размену фотографија, видео-снимака и филмова.

Откривање података о личностима сматра проблемом 43% испитаника, своје податке приликом коришћења бесплатних услуга на мрежи и то најчешће е-адресу оставља њих 48%. Њих 41% осећа се обавезним да обелодани поједине податке о себи на интернету. Четвртина испитаника поставља разне врсте података о личностима на сајтовима за друштвено умрежавање и дружење (26%). 31% не чита изјаве о приватности на интернету, али се осећају довољно информисани о условима под којим се прикупљају подаци о њима и на који начин се користе. Након регистрација за услугу на мрежи, 62% испитаника је променило своје профиле у

139 Lenhart A. 9 Things You Need To Know About Teens, Technology & Online Privacy, Teens & Technology Mary Madden, Senior Researcher Pew Research Center, Family Online Safety Institute, 2013., pp.4 http://www.pewinternet.org/Presentations/2013/Nov/9-Things-About-Teens-Technology-Online-Privacy.aspx, 26.01.2014.

140 SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre REPORT, Publication: June 2011;

односу на подразумевана подешавања на друштвеној мрежи и верују да су компаније одговорне за безбедно руковање подацима.

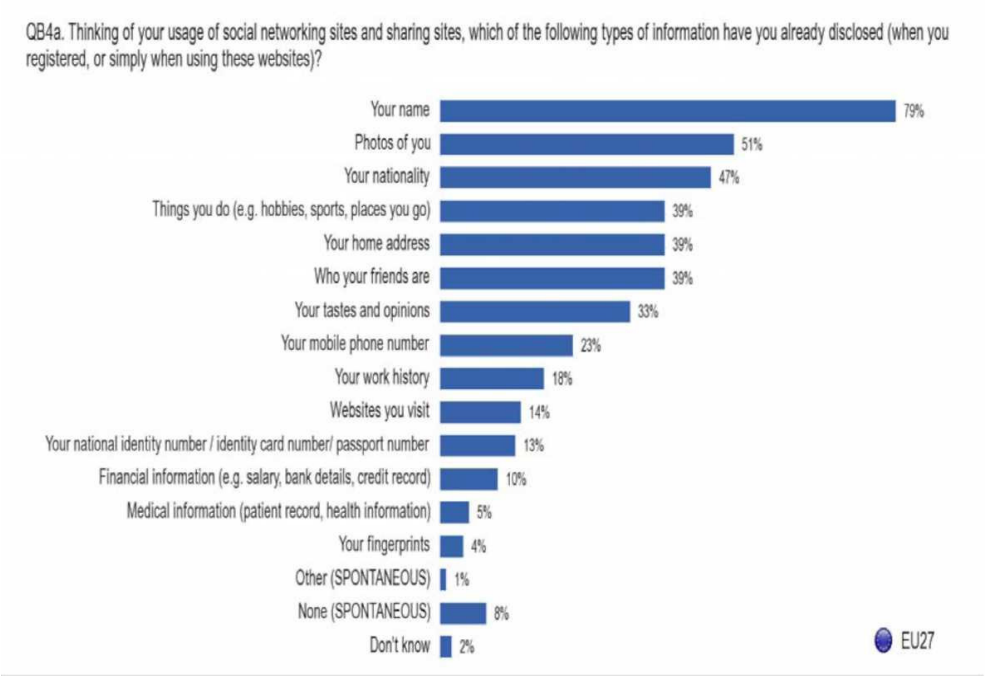


График 18. Подаци које грађани ЕУ остављају о себи на сајтовима за друштвено умрежавање и дељење садржаја[141]

Већина испитаника (84%) верују да имају контролу над подацима које објављују на друштвеним мрежама и другим сајтовима за дељење садржаја. Две трећине њих сматра да се подаци које остављају могу користити за сврху другачију од оне за коју су прикупљени.

Ако се посматрају одговори по земљама ЕУ примећује се да податке као што су име (95%) и адреса (56%) највише остављају Швеђани, а фотографије (67%) становници Велике Британије. Број телефона дели готово половина Литванаца (47%), а идентификациони број (број личне карте или пасоша) 43% Швеђана. Најопрезнији су када су медицински подаци у питању (3-13%) и отисак прста (до12%).

На питање да ли читају услове коришћења шест од десет Европљана каже да (58%); трећина наглашава да их и разуме (34%); четвртина да их чита, али не да их у потпуности разуме (24%); четвртина их не чита (25%), 8% игнорише услове, а један од двадесет каже да не зна где да их пронађе (5%).

141 SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre REPORT, Publication: June 2011, QB4a Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?, pp. 39;

Табела 2. Подаци које грађани ЕУ остављају о себи на сајтовима за друштвено умрежавање и дељење садржаја приказано по земљама ЕУ

QB4a Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?

	Your name	Photos of you	Your nationality	Your home address	Things you do (e.g. hobbies, sports, places you go)	Who your friends are	Your tastes and opinions	Your mobile phone number	Your work history	Websites you visit	Your national identity number / identity card number/ passport number	Financial information (e.g. salary, bank details, credit record)	Medical information (patient record, health information)	Your fingerprints
EU27	79%	51%	47%	39%	39%	35%	33%	23%	18%	14%	13%	10%	5%	4%
BE	82%	52%	60%	42%	42%	44%	31%	20%	23%	17%	11%	8%	7%	5%
BG	76%	54%	47%	25%	42%	34%	31%	18%	8%	17%	14%	5%	3%	5%
CZ	82%	39%	39%	52%	42%	29%	30%	38%	10%	19%	15%	10%	8%	3%
DK	91%	64%	65%	44%	44%	56%	28%	40%	33%	13%	23%	11%	3%	1%
DE	78%	44%	55%	50%	43%	34%	29%	22%	20%	16%	6%	11%	3%	2%
EE	87%	57%	46%	44%	41%	45%	23%	39%	16%	18%	37%	17%	13%	6%
IE	85%	54%	61%	49%	52%	44%	39%	26%	16%	22%	9%	11%	9%	3%
EL	75%	46%	34%	41%	27%	31%	29%	19%	8%	18%	15%	10%	4%	5%
ES	80%	46%	57%	40%	42%	27%	46%	22%	13%	13%	31%	20%	9%	10%
FR	75%	53%	44%	38%	37%	43%	34%	22%	33%	11%	4%	6%	1%	1%
IT	69%	46%	49%	24%	41%	38%	36%	15%	17%	13%	17%	11%	8%	9%
CY	89%	52%	56%	42%	28%	42%	29%	22%	15%	13%	13%	10%	3%	2%
LV	90%	58%	36%	41%	36%	24%	24%	47%	20%	16%	29%	15%	4%	3%
LT	78%	55%	40%	32%	36%	32%	21%	18%	11%	25%	6%	4%	5%	2%
LU	82%	59%	66%	28%	52%	54%	40%	13%	30%	22%	6%	7%	1%	1%
HU	81%	47%	32%	53%	37%	34%	27%	26%	22%	17%	13%	15%	8%	7%
MT	85%	61%	78%	46%	49%	44%	45%	16%	13%	22%	13%	10%	6%	1%
NL	84%	58%	51%	36%	52%	42%	31%	20%	20%	12%	8%	8%	4%	1%
AT	82%	56%	62%	53%	48%	47%	44%	40%	26%	28%	12%	21%	12%	6%
PL	84%	35%	36%	52%	24%	23%	19%	34%	6%	12%	13%	5%	4%	2%
PT	67%	40%	42%	32%	29%	22%	37%	18%	14%	13%	18%	11%	7%	12%
RO	64%	44%	45%	38%	34%	29%	27%	18%	21%	14%	17%	13%	12%	8%
SI	90%	53%	35%	56%	37%	38%	29%	29%	7%	21%	12%	8%	5%	2%
SK	82%	52%	37%	57%	44%	45%	28%	40%	15%	20%	20%	10%	6%	2%
FI	88%	53%	62%	38%	38%	30%	38%	29%	17%	13%	16%	8%	3%	1%
SE	95%	64%	68%	55%	49%	54%	37%	45%	29%	17%	43%	13%	3%	0%
UK	79%	67%	36%	25%	36%	53%	35%	13%	10%	12%	4%	6%	3%	2%

Highest percentage per country / Highest percentage per item — *Lowest percentage per country* / Lowest percentage per item

Резултати до којих је дошла *Amanda Lenhart* са својим тимом[142] указују да је тинејџерима веома значајан углед који имају на друштвеним мрежама и да много времена и енергије посвећују управљању подацима које остављају:

- 74% тинејџера редовно брише пријатеље на мрежи;
- 59% су избрисали или променили нешто што су постављали у прошлости;
- 53% брише коментаре других на свом профилу или налогу;
- 45% уклања своје име са фотографија на којима су означени;
- 31% је обрисало или деактивирало цео профил или налог;
- 19% су послали исправке на коментаре, фотографије, видео-записе.

Истраживање *Anonymity, Privacy, and Security Online* обухватило је и групу питања о различитим "издувним подацима" који се генеришу као резултат свакодневне он-лајн комуникације, сурфовања и употребе апликација. Испитаници су питани колико им је значајно да имају контролу над подацима које остављају на мрежи. Постојало је одступање у у одговорима у зависности од врсте података. Садржај е-поште и особе са којима комуницира на тај начин осетљивији су делови информација у поређењу са другим он-лајн активностима и подацима.

142 Lenhart A. 9 Things You Need To Know About Teens, Technology & Online Privacy, Teens & Technology Mary Madden, Senior Researcher Pew Research Center, Family Online Safety Institute, 2013., part 1 http://www.pewinternet.org/Presentations/2013/Nov/9-Things-About-Teens-Technology-Online-Privacy.aspx, 26.1.2014;

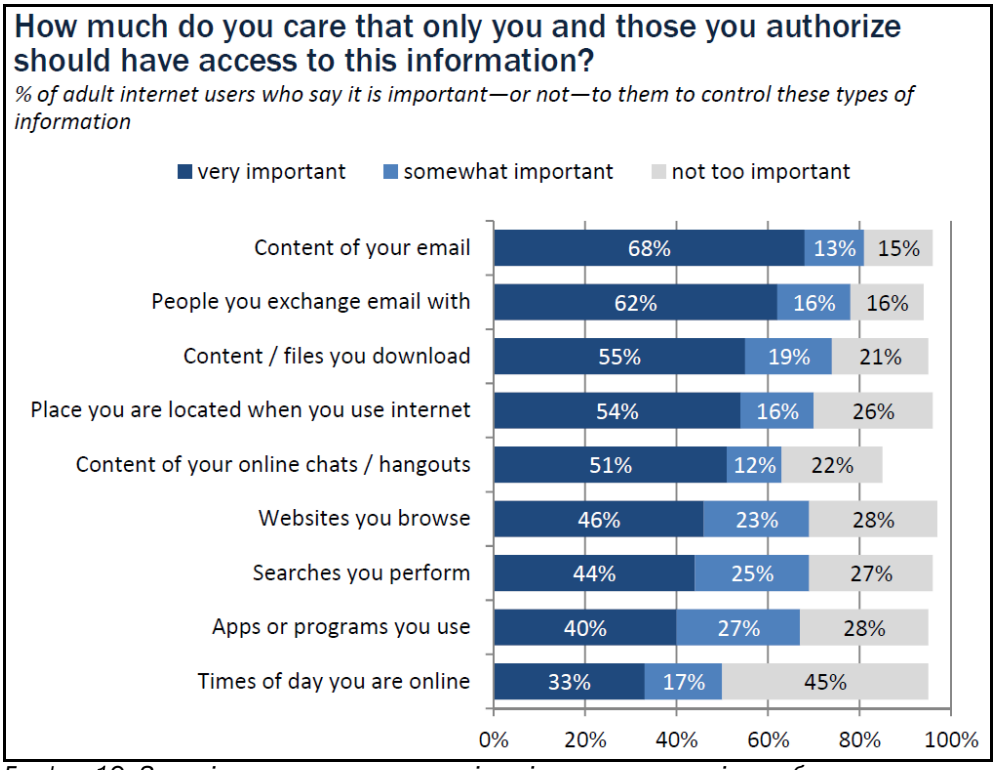


График 19. Значај контроле података које појединци остављају о себи на интернету[143]

Део истраживања односио се на питања безбедност података на интернету. Извесни број корисника имао је проблема са крађом података: *email* налога, броја социјалног осигурања или других информација о кредитној картици; ухођењем или узнемиравањем, губитком угледа, виктимизацијом од стране превараната. Неки од резултата показују следеће[144]:

- од 21% корисника *email* налог је преузет од стране неког другог без дозволе;
- 13% корисника је имало проблема са породицом или пријатељима због нечега што су објавили на мрежи;
- 12% корисника је прогањано и малтретирано на мрежи;
- 11% корисника је имало проблема са крађом социјалног броја, броја кредитне картице или информација о банковном рачуну;
- 6% корисника су били жртва он-лајн преваре и изгубили су новац;

143 Pew Research Center's Internet & American Life Project Omnibus Survey, conducted July 11-14, 2013, on landline and cell phones. N=792 for internet users and smartphone owners. Interviews were conducted in English on landline and cell phones. The margin of error on the sample is +/- 3.8 percentage points pp. 7;

144 Rainie L, Kiesler S. Kang R. Madden M. *Anonymity, Privacy, and Security Online, Pew Research Center's Internet & American Life Project, Washington, 2013.*, http://pewinternet.org/Reports/2013/Anonymity-online.aspx, pp.2;

- 4% корисника је било у физичкој опасности због нечега што се десило на мрежи;
- 1% корисника је изгубило прилику за посао или образовање због нечега што су сами или је неко други поставио о њима на мрежи.

68% корисника сматра да садашњи закони нису довољно добри у заштити приватност на мрежи док 24% њих верују у овај вид заштите.

Већина корисника интернета зна да су подаци о њима доступни он-лине, фотографије и видео-снимци, њихове е- адресе, датум рођења, број телефона, кућна адреса, групе којима припадају. Половина каже да је забринута због количине података која је о њима доступна другима.

Када су у питању млађи корисници, студија *9 Things You Need To Know About Teens, Technology & Online Privacy*[145] показује да је 9% тинејџера који користе друштвене мреже "веома" забринуто да би неким подацима које деле на сајтовима за друштвено умрежавање могла приступити трећа лица, као што су оглашивачи и друге компаније без њиховог знања. Са друге стране, иста студија указује на значајну забринутост родитеља: 81% њих је забринуто због тога што оглашивачи могу, захваљујући подацима које деца остављају, да сазнају доста тога о он-лајн понашању њихове деце; 72% родитеља брине како њихово дете реагује на мрежи у комуникацији са непознатима; 70% њих сматра да он-лајн активност њиховог детета могу негативно утицати на њихове будуће академске и професионалне каријере; 69% њих брине дететова репутација на мрежи.

Да старији ипак имају неки утицај на понашање млађих на интернету говори исто истраживање и податак да је 70% тинејџера потражило савет о подешавању приватности на мрежи: 42% је питало пријатеља или некога на интернету, 41% њих је тражило савет од родитеља, 37% је помоћ затражило од рођака, 13% је посетило сајт за подешавање приватности на друштвеној мрежи, 9% се обратило наставнику, 3% је њих негде другде потражило помоћ.

Интересантно је које стратегије корисници користе да би заштитили своју приватност на мрежи. У највећој мери редовно бришу историју кретања на интернету и *cookies*, бришу некадашње поруке, ибегавају сајтове на којима морају да се региструју или користе привремено или лажно име и е-адресу [146].

Поредећи резултате са узрастом испитаника, јасно је да су млађи корисници сналажљивији у брисању трагова и контроли садржаја који остављају на мрежи.

Одговори корисника у Србији указују на недовољно познавање различитих система заштите и чињеницу да не воде подједнако рачуна о контроли садржаја који остављају на друштвеним мрежама. Ово указује на проблем едукације, нарочито најмлађих корисника. Иако се интернет у Србији у великој мери користи више од једне деценије, култура понашања не постоји, па самим тим ни адекватан однос према видљивости података који се остављају.

---

145 Lenhart A. 9 Things You Need To Know About Teens, Technology & Online Privacy, Teens & Technology Mary Madden, Senior Researcher Pew Research Center, Family Online Safety Institute, 2013, part 2 http://www.pewinternet.org/Presentations/2013/Nov/9-Things-About-Teens-Technology-Online-Privacy.aspx, 26.1.2014;

146 Pew Research Center's Internet & American Life Project Omnibus Survey, conducted July 11-14, 2013, on landline and cell phones. N=792 for internet users and smartphone owners. Interviews were conducted in English on landline and cell phones. The margin of error on the sample is +/- 3.8 percentage points pp. 9;

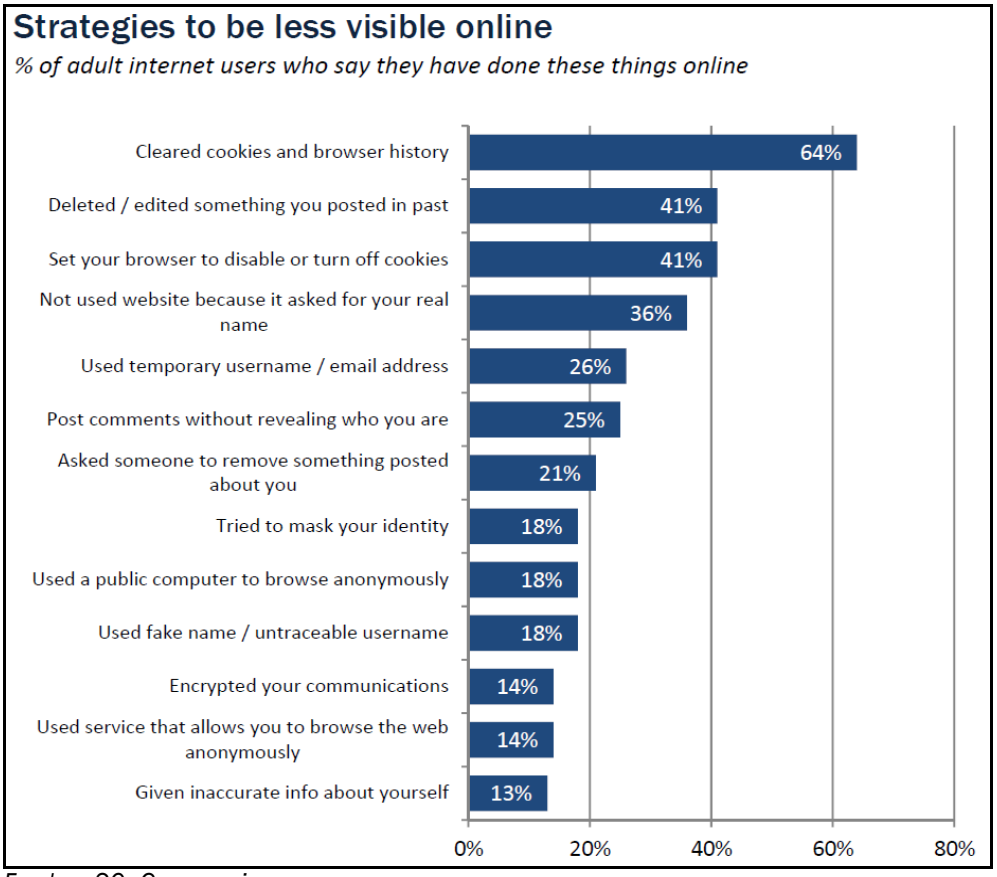


График 20. Стратегије заштите приватности на интернету

Још једна студија показује да забринутост за приватност у ери смарт телефона расте из дана у дан. *American Life Project and the Pew Internet* је објавио студију: *Cloud Computing Raises Privacy Concerns*[147] по којој 90% испитаника изјављује да их брине могућност да компаније у којима се њихови подаци чувају продају те податке, 80% сматра да њихове фотографије и друге податке користе у маркетиншке сврхе, 68% њих сматра да најмање једна од шест *cloud* апликација анализира податке, а затим приказује огласе на њима на основу њиховог понашања на мрежи.

Разлог за забринутост постоји ако се погледају резултати истраживања у Србији који говоре да се трећина оних који су остављали име и презиме, адресу и број телефона суочила са крађом идентитета на интернету, сваки десети је имао проблема са он-лине узнемиравањем. Петини корисника који су оставили матични број на мрежи преузет је идентитет, а исти број је претрпео сексуално узнемиравање. Интересантно је да ни један корисник који је оставио број платне картице није имао проблем са преузимањем идентитета, али је претрпео неки вид

147 American Life Project and the Pew Internet: Cloud Computing Raises Privacy Concerns. Pugh, Sept. 12, 2012;

узнемиравања. Крађу идентитета доживело је 36% испитаника који су дали своју лозинку. Проблем је што већину тих корисника (40%-64%) не брине могућност злоупотребе података које су оставили.

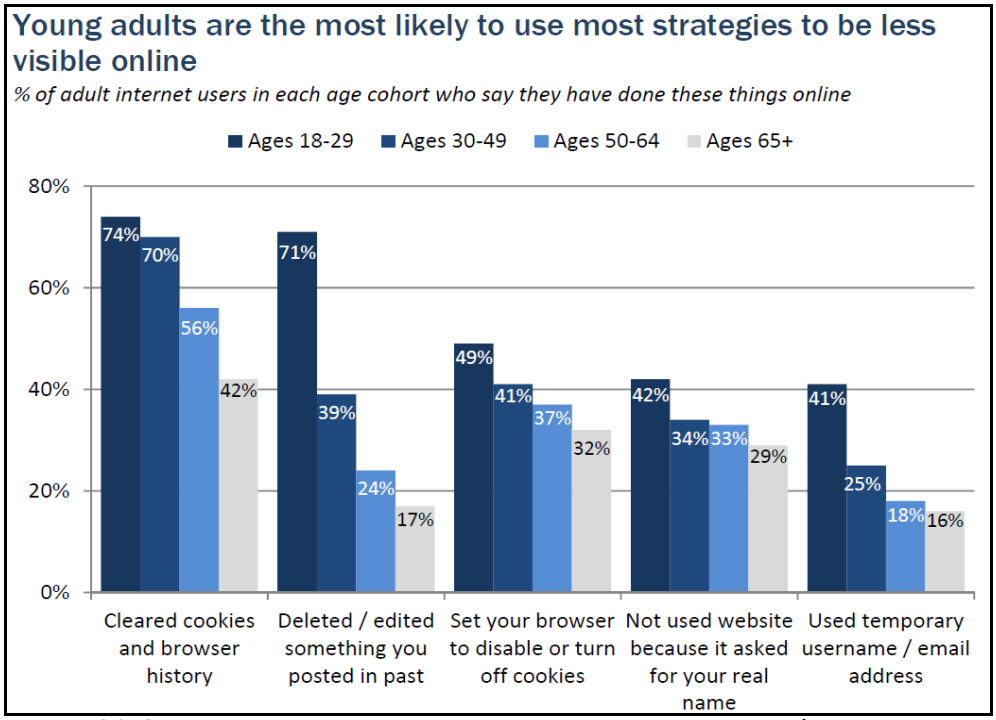


График 21. Значај контроле података које појединци остављају о себи на интернету[148]

Истраживање у Србији није обухватило питања заштите, али је значајно да се светски трендови анализирају и узму у обзир приликом дефинисање нових стратегија заштите приватности на интернету.

3.2.4 Он-лајн понуде

Половина корисника друштвених мрежа изјавила је да добија он-лајн понуде (50,2%). Највише их добијају старији малолетници - 52,5%, затим они од 18 до 30 година - 51,4% и 37% млађих малолетника, док је испитаника који добијају понуде узраста 10-14 година 34,7% и 6-10 година 14,8%.

Испитаници добијају најчешће понуде за туристичка путовања – 21%, и позиве за чланство у групу или организацију – 17%. Затим следе: школовање – 11%,

148 Pew Research Center's Internet & American Life Project Omnibus Survey, conducted July 11-14, 2013, on landline and cell phones. N=792 for internet users and smartphone owners. Interviews were conducted in English on landline and cell phones. The margin of error on the sample is +/- 3.8 percentage points pp. 10;

уручивање новчаних награда – 9%, пословне понуде – 7%, заједничка летовања/зимовања – 6%, запошљавање – 12%, лечење 5%, брачне понуде 4% и заједнички викенди и помоћ за добијање боравишне или радне дозволе са по 3%.

Највећи број испитаних те понуде добија повремено – 19,7% њих. Често их добија 13,2% испитаника, ретко – једанпут 5,8% и веома често 5,5% свих испитаника.

Највећи број испитаника је обрисао понуду без читања – 16,6%, затим следи број оних који су прочитали и нису реаговали на примљене понуде – 15,3% и они који су прочитали и обрисали понуду – 12,1%. Проценат оних који су одговорили на понуду је 4,2. Они који су одговорили на понуду је 7,7%, 4,5%, 11,5%, 6,2% и 5,6% за старосне групе 6-10, 10-14, 14-16, 16-18 и 18-30 година, респективно.

Иако половина испитаника прима он-лајн понуде, проценти оних који су на понуде одговарали нису велики. Уколико се неко није добровољно пријавио да жели да прима понуде, а понуде му стижу, значи да је тај који понуде шаље или на неки начин прикупио податке о особи којој шаље понуду, или то ради насумично. У оба случаја понуда може бити лажна, односно представља мамац који би послужио у сврху преваре неке особе, што може бити веома опасно јер постоје случајеви трговине људима који се заснивају на овом принципу, као и разни други облици кривичних дела.

4. ЗАКЉУЧАК

Приватност и интернет на први поглед делују као супротности. У доба друштвених мрежа, инсистирање на приватности делује неосновано. Ипак, сва истраживања потврђују потребу корисника за контролом података које остављају на мрежи. Застарела регулатива у области заштите података о личности у којој нису препознате специфичности прикупљања, обраде, чувања и дељења података на интернету захтева хитну измену и допуну. Предлози Европске комисије за свеобухватну реформу Директиве за заштиту података 1995 ЕУ имају за циљ да ојачају права на приватност и регулишу европску дигиталну економију. Постоји јасна потреба да се затвори растући јаз између појединаца и компанија које обрађују податке о личности. Очекујући нову Директиву у наредним месецима Канцеларија Повереника за приступ информацијама од јавног значаја и заштиту података о личности припрема нови закон о овој области, који ће пратити савремене токове и прилагодити се понашању појединца, штитећи једно од основних људских права - право на приватност.

Усклађивање правних мера заштите мора пратити и измена у наставним плановима и програмима који ни на који начин не обрађују питања информационе приватности и генерално понашања корисника на интернету. Наравно, не треба чекати да се надлежне институције одазову и предузму одговарајуће мере. Постоје разни видови неформалног учења који у великој мери могу утицати на подизање свести корисника.

Нет-патрола је механизам за пријаве нелегалних и непримерених садржаја и понашања на Интернету и пример је добре праксе у Србији. Центар за безбедни интернет Србије води електронски механизам за подношење пријава о нелегалним, штетним и непримереним садржајима и понашању на интернету, назван Нет-патрола, постоји од августа месеца 2013. године. Посебно обучени оператери

примају, обрађују и прослеђују пријаве грађана Јединици за високотехнолошки криминал Министарства унутрашњих послова Републике Србије и другим надлежним службама и организацијама у складу са утврђеном оперативном процедуром. Тежиште у раду механизма за пријаве јесте спречавање ширења материјала који садрже представе сексуалне злоупотребе деце, сексуално искоришћавање и физичке и психичке нападе на децу, али се могу пријавити и материјали који садрже говор мржње, материјали расистичке и ксенофобичне природе и други непримерени садржаји и облици понашања на интернету. Поменути садржаји могу се пријавити потпуно анонимно, попуњавањем он-лајн формулара за пријаву на сајту *www.netpatrola.rs* или слањем пријаве путем електронске поште.

У новембру 2013. године Нет-патрола је постала члан Међународног удружења оператора интернет механизама за пријаве недозвољеног и штетног садржаја на интернету *INHOPE*. Од тада, Нет-патрола активно учествује у раду ове организације, посебно у размени информација и осмишљавању најефикаснијих метода за уклањање нелегалних и штетних материјала са интернета. Током првих пет месеци рада, Нет-патрола је примила 378 пријава и захваљујући напорима њених оператера уклоњени су разни непримерени он-лајн садржаји.

Крајем септембра 2013. године започет је нови циклус едукативних активности у основним и средњим школама широм Србије у сарадњи са четири партнерске невладине организације: Центром за превенцију девијантног понашања код младих – „Таргет" из Новог Сада, Ц31 – Центром за развој културе дечјих права из Београда, Друштвом за развој деце и младих – „Отворени клуб" из Ниша и Тимочким омладинским центром из Зајечара. У оквиру овог циклуса, у школама је за ученике организовано143 предавања, 55 радионица, обука за вршњачке едукаторе и две фокус-групе које су чинили основци и средњошколци, као и 47 радионица и предавања за родитеље. Све поменуте едукативне активности, посебно прилагођене различитим узрастним групама корисника, имале су за циљ да пруже што више релевантних информација о различитим аспектима безбедне употребе интернета и информационо-комуникационих технологија, опасностима и ризицима за кориснике, као и о предностима и различитим могућностима примене ИКТ-а у процесу наставе и учења. Предавања и радионице обухватају смернице за тзв. „нетикецију" (правила понашања у он-лајн комуникацији), људска права, заштиту података о личности, неопходним техничким подешавањима у циљу заштите приватности корисника и безбедном коришћењу друштвених мрежа. Ученици и наставници су позитивним примерима и најсавременијим могућностима подстицани да на безбедан начин користе расположиве он-лајн садржаје и ресурсе. Планирана је и реализација акредитованих семинара за школске психологе и педагоге од којих се очекује да реагују у свим ексцесним ситуацијама, али и превентивно, пре него што до проблема дође.

Непрекидном едукацијом може се утицати на пораст свести корисника о могућим злоупотребама података које свакодневно остављају на мрежи. Тиме се смањује опасност од крађе идентитета и других видова повреде приватности корисника који, иако воле да шерују разне сегменте из свога живота са другима, желе да буду апсолутни господари трагова које остављају.

ЛИТЕРАТУРА

1. Abram, C., (2006) Welcome to Facebook, everyone, Facebook.
2. Agre, P. and Rotenberg, M., (eds.), (1997), Technology and Privacy: The New Landscape, Cambridge: MIT Press.
3. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8.XI2001, http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm
4. Allen, A., (1988), Uneasy Access: Privacy for Women in a Free Society, Totowa, N.J.: Rowman and Littlefield
5. Alterman, A., (2003), A Piece of Yourself: Ethical Issues in Biometric Identification, Ethics and Information Technology 5, 3:139-150
6. Pugh (2012), American Life Project and the Pew Internet: Cloud Computing Raises Privacy Concerns, 12.9. 2012.
7. Angry Facebook Users Illegally Leaked the Names of Accused Underage Murderers, (2008), Digital Journal
8. Austin, L., (2003), Privacy and the Question of Technology, Law and Philosophy 22, 2:119-166
9. Baćević, Lj. (2002), Razvoj interneta u Jugoslaviji, The European University Viadrina in Frankfurt (Oder), available at http://soemz.euv-frankfurt-o.de/media-see/newmedia/main/articles/pdf/l_bacevic.pdf
10. Batista, S., (2005), UVA Student Remembered, Charlottesville Newsplex.
11. Benschop, A., Peculiarities of Cyberspace, available at http://www.sociosite.org/index_en.php
12. Berteau, S., (2007) Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in. CA Security Advisor Research Blog
13. Bloustein, E., (1964), Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, New York University Law Review 39:962-1007
14. Bok, S., (1982), Secrets: On the Ethics of Concealment and Revelation, New York: Pantheon
15. Bork, R., (1990), The Tempting of America: The Political Seduction of the Law, New York: Simon and Schuster
16. Brin, David, (1998), The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?, Reading, MA: Addison-Wesley
17. Buckley, C., (2007) Get a life and allow your staff to use Facebook, TUC tells bosses. The Times
18. Cohen, J.,(2002), Regulating Intimacy: A New Legal Paradigm, Princeton: Princeton University Press
19. Council of Europe, (2001) Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
20. Cubrilovic, N., (2007-08-11). "Facebook Source Code Leaked", TechCrunch
21. Darnton, R., (2008), The Library in the New Age, The New York Review of Books, available at http://www.nybooks.com/articles/21514
22. DeCew, J., (1997), In Pursuit of Privacy: Law, Ethics, and the Rise of Technology, Ithaca: Cornell University Press
23. Definition of cybercrime, Webster Dictionary, available at http://www.webster-dictionary.org/definition/cybercrime, 16.4.2014.
24. Delaney, K., (2006) Facebook, Riding a Web Trend, Flirts With a Big-Money Deal, Dow Jones, pp. 1.
25. Delaney, K., (2007) Microsoft Fires Volley At Google in Ad Battle. The Wall Street Journal
26. Dempsey, L., (2006) Facebook is the go-to Web site for students looking to hook up, Dayton Daily News

27. Директива 95/46/ЕЦ Европског парламента и Савета од 24. октобра (1995) о заштити појединаца у вези са обрадом података о личности и о слободном кретању таквих података, ОЈ Л 281, 23.11.1995.
28. Дракулић, М. (2007), Основи компјутерског права, Факултет организационих наука, Београд
29. Drudi, C.,(2008). Facebook proves problematic for police. The Globe and Mail
30. Elshtain, J., (1981), Public Man, Private Woman: Women in Social and Political Thought, Princeton: Princeton University Press
31. Etzioni, A., (2000), The Limits of Privacy, New York: Basic Books
32. Европска Комисија, сајт доступан на адреси http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
33. Еуробарометар (ЕБ) 359, Заштита података и електронски идентитет у ЕУ (2011), http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
34. Fried, C., (1970), An Anatomy of Values, Cambridge: Harvard University Press
35. Freeman, L., (2006) The Development of Social Network Analysis. Vancouver: Empirical Pres, 2006;
36. Gavison, R., (1980), Privacy and the Limits of Law, Yale Law Journal 89: 421-71
37. Gerety, T., (1977), Redefining Privacy, Harvard Civil Rights-Civil Liberties Law Review 12: 233-96 Gerstein, R., 1978, Intimacy and Privacy, Ethics 89: 76-81
38. Henkin, L., (1974), Privacy and Autonomy, Columbia Law Review 74:1410-33
39. Hollander, R., (1985), Video Democracy. Lomond: Mount Airy, MD
40. Hoffman, H., (2007) Facebook's source code goes public, CNET News.com
41. How Sticky Is Membership on Facebook? Just Try Breaking Free, (2008), New York Times
42. Inness, J., (1992), Privacy, Intimacy and Isolation, Oxford: Oxford University Press
43. Iorg, E., (2005) Student Colby McLain remembered, University News
44. Jesdanun, A., (2006) Facebook offers new privacy options. Associated Press
45. Johnson, J., (1994), Constitutional Privacy, Law and Philosophy 13: 161-193
46. Jones, H. & Soltren J. H., (2005) Facebook: Threats to Privacy
47. Kelleher, K., (2007) Facebook profiles become makeshift memorials. The Brown Daily Herald
48. Компаративне студије о различитим приступима новим изазовима приватност, (2010) http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf
49. Кривични законик Републике Србије, Сл. гласник РС, бр. 85/2005, 88/2005 -испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013
50. Kupfer, J., (1987), Privacy, Autonomy and Self-Concept, American Philosophical Quarterly 24: 81-89
51. Laverdet, M., (2006) Why XSS is my favorite type of vulnerability
52. Lenhart A., (2013), Senior Researcher, Director of Teens & Technology, Mary Madden, Senior Researcher Pew Research Center, Family *Online* Safety Institute
53. Lerer, L., (2007) Why MySpace Doesn't Card. Forbes. Lacy, Sarah (2006-09-12). "Facebook: Opening the Doors Wider". BusinessWeek
54. Lerner, D., (1958), The passing of Traditional Society: Modernizing the Middle East. New York: Free Press of Glencoe
55. Lisbon Treaty, Eurostep, EEPA, http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-3-union-policies-and-internal-actions/title-xix-research-and-technological-development-and-space/467-article-179.html, 22.3.2014.
56. MacKinnon, C., (1989), Toward a Feminist Theory of the State, Cambridge: Harvard University Press
57. McLuhan, M. (1968) War and Peace in the Global Vilage. New York: Bantam Books
58. Mead, M., (1949), Coming of Age in Samoa, New York: New American Library
59. Moore, A., (1998), Intangible Property: Privacy, Power, and Information Control, American Philosophical Quarterly 35: 365-378

60. Morse, J., (2006) Facebook Responds. Cogito
61. Nadel, S.F. (1957) The Theory of Social Structure. London: Cohen and West
62. Nagel, T., (2002), Concealment and Exposure: And Other Essays, Oxford: Oxford University Press
63. Net generation grieves with Facebook postings, (2008), News Observer
64. News Corp in $580 m internet buy, (2005), BBC News
65. Оквирна одлука Савета 2008/977/ЈХА од 27. новембра 2008. године о заштити личних података обрађених у оквиру полицијске и правосудне сарадње у кривичним стварима, ОЈ Л 350, 30.12.2008, п. 60 (Оквирна одлука)
66. Parent, W., (1983), Privacy, Morality and the Law, Philosophy and Public Affairs 12: 269-88
67. Paul, J., Miller, F., Paul, E., (eds.), (2000), The Right of Privacy, Cambridge: Cambridge University Press
68. Pennock, J. and Chapman, J., (eds.), (1971), Privacy, NOMOS XIII, New York: Atherton Press
69. Peterson, C., (2006), Who's Reading Your Facebook?, The Virginia Informer
70. Posner, R., (1981), The Economics of Justice, Cambridge: Harvard University Press
71. Privacy, 123 HelpMe.com, (2008), available at http://www.123HelpMe.com/view.asp?id=82335, 21.02.2014
72. Privacy Policy, (2008), Facebook
73. Protection of personal data, (2007), The European Union On-Line, available at http://europa.eu/scadplus/leg/en/lvb/l14012.htm
74. Prott, D., (2006), Son, friend remembered as 'free spirit', College Heights Herald
75. Public Opinion on Privacy, Electronic Privacy Information Center, available at http://epic.org/privacy/survey/
76. Prosser, W., (1955), Handbook of the Law of Torts, 2nd ed., St. Paul: West
77. Rachels, J., (1975), Why Privacy is Important, Philosophy and Public Affairs 4: 323-33
78. Radcliffe-Brown, A.R., (1940), On Social Structure, Journal of the Royal Anthropological Institute: 1-12.
79. Rainie L, Kiesler S., Kang R. Madden M., *Anonymity, Privacy, and Security Online, Pew Research Center's Internet & American Life Project, Washington, (2013),* http://pewinternet.org/Reports/2013/Anonymity-*online*.aspx
80. Резолуција Европског парламента о саопштењу Комисије Европског парламента и Савета - подручје слобода, безбедност и правда у служби грађана - Штокхолмски програм усвојен 25. новембра 2009. године, (П7_ТА(2009)0090)
81. Резолуција од 6. јула 2011. године о свеобухватном приступу заштити података о личности у Европској унији (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-20110323&language=EN&ring=A7-2011-0244 (rapporteur: MEP Axel Voss (EPP/DE)
82. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011
83. Richards, J., (2007), Facebook Source Code Leaked Onto Internet, FOX
84. Romero, J., (2006), The Super Facebook Saga
85. Rosenbush, S., (2006), Facebook's on the Block, BusinessWeek
86. Rosmarin, R., 2006. Facebook's Makeover, Forbes
87. Rosmarin, R., (2006), Open Facebook, Forbes
88. Sakuma, P., (2007), The Future of Facebook, Time
89. Scanlon, T., (1975), Thomson on Privacy, Philosophy and Public Affairs 4: 315-322
90. Schoeman, F., (ed.), (1984), Philosophical Dimensions of Privacy: An Anthology, Cambridge: Cambridge University Press
91. Scott, J., (1991) Social Network Analysis. London: Sage
92. Smith, J., (2005), Big Brothers, Big Facebook: Your Orwellian Community. The Color of Infinity

93. Solove, D., (2006), A Taxonomy of Privacy, University of Pennsylvania Law Review 154: 477-564
94. Stelter, B., (2006), On Facebook, life after death. The Towerlight
95. *Штокхолмски програм - отворена и безбедна Европа служи и штити грађане*, ОЈ Ц 115
96. Sullivan, B., (2006) Facebook, Courted By Yahoo, Won't Sell, Director Says (Update3). Bloomberg L.P.
97. Swartz, J., (2007) Tech giants poke around Facebook, USA Today
98. Team Coverage: Suspect In Tiffany Souers Murder Case Captured In Tennessee, (2006), ksdk.
99. Teller, S., (2006), Investors Add $25M to Facebook's Coffers, The Harvard Crimson
100. Terms of Use, (2008), Facebook
101. The 2007 International Privacy Ranking, (2007), Privacy International, http://www.privacyinternational.org/article.shtml?cmd[347]= x-347-559597
102. Thomson, J., (1975), The Right to Privacy, Philosophy and Public Affairs 4: 295-314
103. Turkington, R., Trubow, G., and Allen, A., (eds.), (1992), Privacy: Cases and Materials, Texas: John Marshall
104. Vander Veer, E. A., (2008), Facebook: The Missing Manual, O'Reilly
105. Водинелић, В. (2006), Поводом модела закона о заштити података о личности, Херетицус, Београд, available at http://www.hereticus.org/arhiva/2006-3-4/povodom-modela-zakona-o-zastiti-podataka-o-licnosti.html
106. Wafa, T, (2008), Internet Privacy Rights - Global Internet Privacy Rights: A Pragmatic Legal Perspective, ExpressO
107. Westin, A., (1967), Privacy and Freedom, New York: Atheneum
108. Warren, S. and Brandeis, L., (1890(, The Right to Privacy, Harvard Law Review 4: 193-220.
109. Wellman, Barry and S.D. Berkowitz, eds., (1988), Social Structures: A Network Approach, Cambridge: Cambridge University Press
110. Wasserman, Stanley, and Katherine Faust, (1994), Social Network Analysis: Methods and Applications, Cambridge, Cambridge University Press
111. Why you should beware of Facebook, (2008), The Age
112. Williams, C., (2007), Facebook wins Manx battle for face-book.com, The Register
113. Закон о заштити података о личности, Службени гласник РС, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012

проф. др Мирјана Дракулић
Универзитет у Београду – Факултет организационих наука

мр Ратимир Дракулић
Универзитет у Београду – Факултет организационих наука

CYBER КРИМИНАЛ

Садржај

Табеле

Графици

Слике:

1. ЧЕТИРИ СТВАРИ КОЈЕ СУ ПРОМЕНИЛЕ СВЕТ

Глобалне рачунарске мреже, мобилна/смарт телефонија, друштвене мреже и *cloud* рачунарство створиле су могућности за нове облике криминала. Појављује се посебан, софистициран, продоран, технички поткован, бескрупулозан, опседнут, добро припремљен, понекад осветољубив, сексуално или на други начин настран, овисан појединац[149] кога је тешко зауставити[150]. Он све чешће не жели да буде сам већ му је потребно друштво, као што му је неопходна и "публика". Лакоћа "вршљања" cyber простором даје му осећај моћи и неухватљивости[151]. Ови осећаји нису без разлога, јер га је стварно изузетно тешко открити у моменту чињења дела, што, углавном, представља и "прави" тренутак за његово идентификовање и хватање. С друге стране, интернет и друштвене мреже који су толико рањиви и несигурни због огромног броја корисника, отворености и нерегулисаности су и идеално скровиште криминалацима различитог типа, којима је потребно друштво, као што му је неопходна и "публика". Лакоћа "вршљања" cyber простором даје му осећај моћи и неухватљивости[152].

Тако је, у марту 2013. године, по подацима Међународне телекомуникационе уније 38,8% корисника интернета од укупног светског становништва (број корисника интернета порастао је на скоро 3 милијарде, односно 2 милијарде 749 милиона), од тога у развијеним земљама је то 76,8%, а у земљама у развоју 30,7%. У поређењу са 2005. годином, када је било 15,8% укупног светског становништва (1 милијарда и 24 милиона корисника интернета), односно 50,9% у развијеним и 7,8% у неразвијеним земљама. Пораст говори сам по себи. Ако би се претпоставило да је само један промил од тог броја са „лошим" намерама, то би било чак око 275 хиљада учнилаца. А колико је тек потенцијалних жртава?

Ако се погледа укупан број корисника у тој истој години, по регионима, види се да их је највише у Азији, а најмање у Океанији и Аустралији[153]. Почетком 2014. године 81% интернет корисника је било у Северној Америци, 78% у Западној Европи, 63% у Океанији, а у осталим регионима проценат се креће од 12% (Јужна Азија) до 54% (Централна и Источна Европа)[154]. У Европи број интернет корисника креће се од 15,3 милиона, у Украјини, до 68 милиона у Русији. У осталих 8 водећих европских земаља корисници су милионски: Немачка, Велика Британија, Француска, Турска, Италија, Шпанија, Пољска, Холандија.

---

149 Wolak J. Finkelhor D., Mitchell J.K., Ybarra L. M., (2008), Online "Predators" and Their Victims, Myths, Realities, and Implications for Prevention and Treatment, American Psychologist, Vol. 63, No. 2, 111–128, pp. 111 - 128., http://www.apa.org/pubs/journals/releases/amp-632111.pdf;

150 Nuccitelli M. (2012), iPredator-A Global Internet Predator Theorymoreby, http://www.academia.edu/1169441/iPredator-A_Global_Internet_Predator_Theory, приступљено 23.1.2014;

151 Small P.E. (2012), Defense in Depth: An Impractical Strategy for a Cyber World, SANS Institute, http://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world- 33896, приступљено 27.1.2014;

152 Drakulić M. Drakulić R., (2005), Cyber kriminal, www.bos.org.yu/cepit/drustvo/sk/cyberkriminal.pht, приступљено 18.9.2005;

153 Inernet World Stats, http://www.internetworldstats.com/stats4.htm, приступљено 26.1.2014;

154 Social, Digital & Mobile Around The World, (2014), http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014, приступљено 25.5.2014;

У земљама кандидатима 2012. године највећи продор корисника интернета је на Исланду (97,1%), затим следе Хрватска (70,7%), Босна и Херцеговина (60%), Македонија (56,7%) и Србија (56,4%), Турска (45,7%), Црна Гора (50%), Албанија (49%) и Косово (20,5%)[155], у односу на број становника, а 48,1% је од укупног броја становника у свих 10 земаља. По посебним подацима Међународне телекомуникационе уније у Србији је те године било 48,1% интернет корисника од укупног броја становника[156].

Слика је мало другачија по подацима Републичког Министарства за унутрашњу и спољњу трговину и телекомуникације по коме више од 2,4 милиона грађана користи интернет свакодневно или скоро свакодневно, што је 300.000 више него 2012. године. У Србији интернет прикључак има 55,8% домаћинстава. Број домаћинстава која имају интернет прикључке већи је за 8,3%[157].

По истраживању спроведеном у мају 2013. године за потребе пројекта „Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије“ у коме је учествовало 2059 испитаника оба пола, различитих старосних доби (од 6 година до преко 60), занимања, економског статуса, радног статуса, нивоа обрзовања и друго, на питање „Ако користите интернет, колико често?“, испитаници су имали следеће понуђене одговоре: неколико пута месечно, једном недељно, неколико пута недељно, свакодневно до једног сата, свакодневно од један до пет сати, свакодневно преко пет сати.

По полу структура одговора је била следећа: испитаници оба пола највише свакодневно користе интернет. Разлике између полова су минималне у процентима.

Најмање у обе категорије користе једном недељно. Испитаници женског пола више користе, неколико пута недељно, а минималне су разлике и у осталим одговорима.

Млади између 16 и 18 година, проводе највише времена на интернету, свакодневно од једног до пет сати.

Резултати везани за време проведено на интернету и број становника у месту становања испитаника, показују да у свим местима, сем оним до 5000 становника, највећи проценат испитаника свакодневно проводе од једног до пет сати на интернету. У малим местима, која су изузеци, највећи број испитаника проводи до један сат на интернету.

Кад је у питању ниво образовања и време коришћења интернета, средњошколци и студенти виших школа највише времена проводе на интернету од једног до пет сати дневно. Испитаници без школе проводе више времена на интернету него што то чине основци.

Иако је пораст корисника интернета фасцинантан и стално растући још већи пораст има број претплатника мобилних телефона. Тако у 2013. години 96% укупног светског становништва су претплатници мобилних телефона (6 милијарди 834 милиона и скоро 900.000). У 2005. години то је 33,9% (2 милијарде 205 милиона

155 Inernet World Stats, http://www.internetworldstats.com/stats9.htm, приступљено 26.1.2014;

156 ITU, Percentage of Individuals using the Internet, www.itu.int/en/, приступљено 26.1.2014;

157 Расте број корисника интернета у Србији, (2013), http://mtt.gov.rs/slider/raste-broj-korisnika-interneta-u-srbiji/, приступљено 27.1.2014;

претплатника)[158]. Ако се томе додају подаци да је на светском нивоу то 95%, онда се може констатовати да је тај продор невероватних размера[159]:

У 2013. години, по подацима Међународне телекомуникационе уније, скоро је исти број мобилних претплатника колико и људи на планети, а више од половине је у азијско-пацифичком региону (3,5 милијарди од укупно 6,8 милијарди претплатника). Продор је 96% на глобалном нивоу, с тим што је 128% у развијеним земљама и 89% у земљама у развоју.

По подацима *comScore* за три месеца 2013. године (закључно са новембром), 152.5 милиона Американаца има у власништву смарт телефоне (пенетрација је 63,8% од тржишта мобилних телефона). Највише је заступљен *Apple*, потом следи *Samsung*, а иза њега *Motorola*, LG и HTC.

Подаци о броју претплатника по регионима и нивоу развијености[160] указују да становници у Африци имају најмањи раст са „свега“ 63%, док је раст највиши у земљама Заједнице независних држава (мало другачије је у осталим статистикама у којима се појављују земље Централне и Источне Европе). Раст се не поклапа са растом интернет корисника.

У спроведеном истраживању у Републици Србији испитаници су одговарали на питање да ли имају мобилне телефоне и какве.

Од укупног броја испитаника 56,7% се изјаснило да имају „обичан“ мобилни телефон, смарт има 41,1%, 2,4% се изјаснило да нема мобилни телефон, а 0,7% поседује и смарт и обичан телефон. Обичан телефон старији поседују више него млађи испитаници – у проценту од 64,2% до 77,1%, а млађи од 42,2%-56,6%. Смарт телефоне поседује 50,2% - 56% испитаника 10-18 година, 42,2% испитаника 18-30 година и 20,5% испитаника 6-10 година (старији испитаници 35,2%, 21,4% и 6,5% за испитанике 30-45, 45-60 и преко 60 година респективно). Телефон не поседује 26,9% испитаника 6-10 година старости, а остали испитаници од 0,5% до 1,9% и испитаници преко 60 година старости 23,9%. На графикону се јасно види да испитаници узраста 10-18 година у већем проценту поседују смарт телефоне него обичне, док са даљим порастом година расте разлика у поседовању смарт и обичних телефона, у корист обичних. Сви смарт телефони имају интернет који је најчешће укључен стално и њихови корисници на тај начин користе телефоне и за комуникацију преко интернета.

158 Social, Digital & Mobile Around The World, (2014), op.cit.;

159 Social, Digital & Mobile Around The World, (2014), op.cit.;

160 The World in 2013. ICT Facts and Figures, (2013), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf, приступљено 25.1.2014;

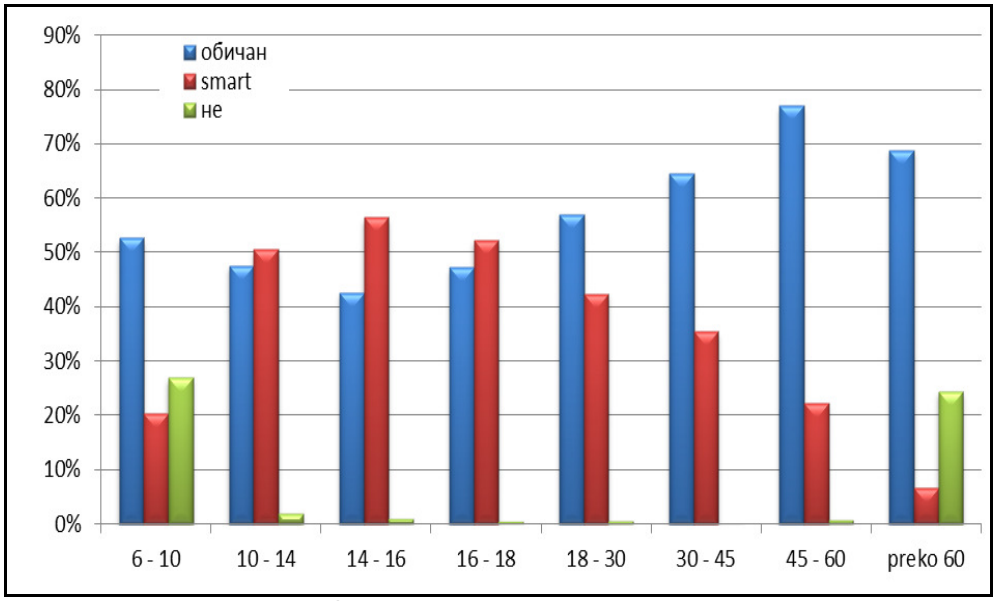


График 1. Поседовање мобилних телефона према старосним групама

Нешто већи број испитаника мушког пола поседује смарт телефоне, у односу на испитанике женског пола и то за 4,7%, док се око 1% више испитаника мушког пола изјаснило да уопште не посудеју мобилни телефон.

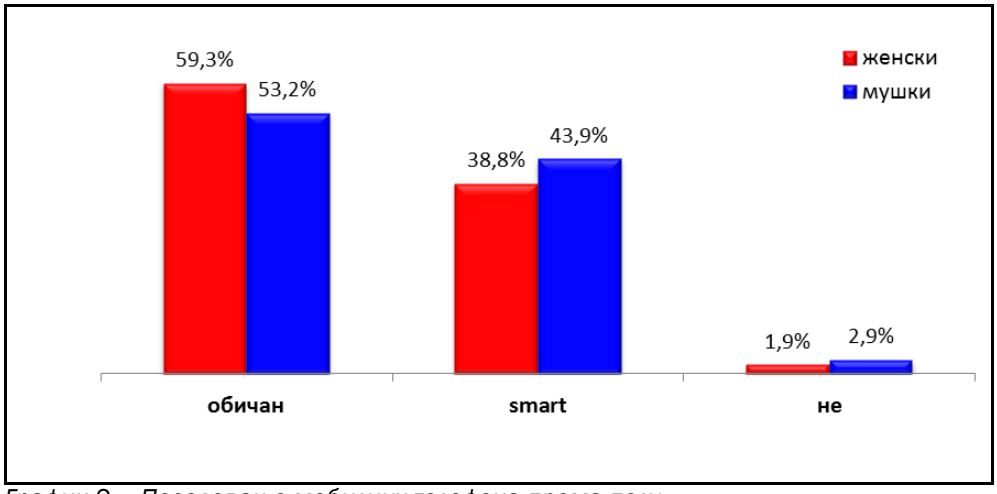


График 2. Поседовање мобилних телефона према полу

Зависно од величине места у којима живе и поседовања мобилног телефона подаци указују да обични телефони има 60,9% испитаника у местима од 20.000 до 100.000 становника, 58,4% у насељима од 100.000 до 500.000, а 51,1% од преко 500.000 становника.

Ако се посматра коришћење смарт телефона, оно је највише заступљено код испитаника из места са преко 500.000 становника као и до 5.000, а најмање местима од 20.000 до 100.000 становника.

Испитаници који не поседују телефон су најчешће из места од 5.000 до 20.000 становника, док их је најређе из места од преко 500.000 становника.

Обичан мобилни телефон је најзаступљенији код испитаника са средњим и вишим образовања. Највише смарт телефоне имају испитаници са основним и високим образовањем, при томе су основци у предности. Непоседовање мобилног телефона је најизраженије код лица без школе, што се могло и очекивати, док сви испитаници са вишим образовањем поседују мобилни телефон.

Подаци добијени на основу других истраживања указују да се мобилни телефони све више користе за комуникацију преко рачунарских мрежа. Тако, по подацима по *Europbarometer*-у, 35% смарт телефона у 2013. години се користило за интернет-везу, док је у 2012. то било знатно мање, 24%. Мада су још увек главни уређаји за приступ интернету рачунари (лаптоп и десктоп у 2013. години 62% односно 53%, а у 2012. 61% односно 63%.)[161].

У последњој деценији, аналитичари су указали да ће у наредним годинама раст броја смарт телефона и таблета бити више него уносан посао. Најновији подаци показују да је у 2013. години, широм света, продаја мобилних уређаја достигла 455.6 милиона јединица, а продаја смарт телефона прешла 250 милиона[162]. Број људи који користе ове телефоне за приступ интернету, такође, расте. Рачуна се да од скоро 7 милијарди претплатника мобилних телефона, око 1,7 милијарди, имају смарт телефоне са разноврсним могућностима. У 2012. године око 1,58 милијарди корисника користе своје мобилне телефоне за интернет, што је око 67% корисника интернета. Овај број расте тако да ће их у 2014. години бити око 79% од укупног броја корисника интернета. До 2017. године се очекује да ће око 2,97 милијарди корисника користити интернет преко својих телефона, што би било око 91% од укупног броја корисника интернета и 58% корисника мобилних телефона. У блиској будућности ови телефони ће постати примарни за повезивање на интернетом[163].

Трећи феномен који је знатно утицао на пораст претњи у cyber простору су друштвене мреже. Експлозија корисника у неколико протеклих година говори сама за себе.

Почетком 2014. године продор друштвених мрежа је био 26% код укупне светске популације, с тим што је највише било у Северној Америци (56%), у три регије је то преко 40% (две регије имају исто Западна Европа и Јужна Америка – 44%), а Источна Азија 45%. Изузетно их је мало у Централној Азији (5%).

Ако се погледају подаци о корисницима разних друштвених мрежа у јануару 2014. године, може се констатовати да је *Facebook* најзаступљенији са 1

161 Eurobarometer Special Surveys 404, Cyber security, report, Fieldwork: May - June 2013, Publication: November 2013, http://ec.europa.eu/public_opinion/index_en.htm, приступљено 28.3.2014;

162 Tiwari A. (2014), Operating System Usage Trend September – December 2013: Smartphone Operating Systems Are Driving Growth!, http://www.dazeinfo.com/2014/01/24/operating-system-usage-trend-2013-smartphone-growth/, приступљено 27.4.2014;

163 Srivastava A. (2014), 2 Billion Smartphone Users By 2015 : 83% of Internet Usage From Mobiles [Study], http://www.dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017/#ixzz2rcbChM tk, приступљено 28.3.2014;

милијардом 184 милиона[164]. Поред раста постојећих друштвених мрежа настају и нове какав је кинески микро блогинг веб-сајт *Tencent Weibo*, настао као нова друштвена мрежа 2010. године и за кратко време добио је велики број корисника који размењују фотографије, видео и текст [165].

Раст друштвених мрежа не тече баш равномерно. Тако, ако се пореди годишњи пораст, нпр. између 2010. и 2011. године, он је мањи код најзаступљенијих мрежа (*Facebook*) него код мање заступљених (*LinkedIn*)[166]. Ипак је, у том периоду *Facebook* претекао локалне конкуренте на 8 тржишта и на њима постао најпопуларнија друштвена мрежа (у 39 од 44 земље у којима компанија *comScore* функционише)[167]. Кина, Јапан, Русија, Јужна Кореја и Вијетнам имају друге друштвене мреже. И даље је, у току 2012. године, ова мрежа имала највиши пораст и била најчешће коришћена. По подацима *Statistic Brain,* 58% светске популације користи било коју друштвену мрежу, а *Facebook* чак 56%[168].

По регионима највише корисника *Facebook* те године има у Европи, за њом следе Азија, Северна Америка, Африка, Централна Америка и Мексико, Средњи Исток, Океанија са Аустралијом и на крају Кариби[169]. Пораст само за једну годину је скоро 200.000.000 корисника, а продор се са 9,6% у првом кварталу 2011. године, пење на 12,1%. Пенетрација *Facebook* друштвене мреже у периоду од 2011. до 2012. године је велика и креће се од 9,6% до 12,1% за свега годину дана[170].

По подацима добијеним истраживањем у Републици Србији испитаници су одговарали на којој друштвеној мрежи поседују налог. Понуђени су одговори: *Facebook, Twitter, YouTube, LinkedIn, Google+, Foursquare*, *Tumblr* и друге. Највећи проценат њих поседује налог на *Facebook*, затим следи *YouTube*, *Google+* и *Twitter*. Трендови се не подударају са светским.

Друштвене мреже се превасходно користе за успостављање разних врста комуникација. Међутим, лепеза циљева се све више шири. Тако корисници размењују податке, видео, P2P, гласовне поруке. Од 2008. године, када су се размењивали само подаци, до 2013, када је највише била заступљена размена видео-записа (64%) и података (19%) дошло је не само до промене у могућностима него и распоређности/заступљености[171].

---

164 Social, Digital & Mobile Around The World, (2014), op. cit;

165 Millward S. (2012), China's Forgotten 3rd Twitter Clone Hits 260 Million Users, http://www.techinasia.com/netease-weibo-260-million-users-numbers/, приступљено 28.1.2014;

166 Mobile Social Networking Audience Grew 44 Percent Over Past Year in EU5, (2011), http://www.comscore.com/Insights/Press_Releases/2011/11/Mobile_Social_Networking_Audience_Grew_44_Percent_Over_Past_Year_in_EU5, приступљено 25.1.2014;

167 Mohamud A. (2012), Facebook: Around the World in 800 Days, http://www.comscore.com/Insights/Blog/Facebook_Around_the_World_in_800_Days, приступљено 28.3.2014;

168 Social Networking Statistics, http://www.statisticbrain.com/social-networking-statistics/, приступљено 26.1.2014;

169 Facebook users in the world, Facebook Usage and Facebook Growth Statistics By World Geographic Regions, http://www.internetworldstats.com/facebook.htm, приступљено 27.1.2014;

170 Internet World Stats, www.internetworldstats.com/facebook.htm, приступљено 23.4.2014;

171 Cloud Computing Penetration into Enterprise IT Gaining Momentum WaveLength Market Analytics & Winn Technology Group Report Says Early Cloud Users and Planners Estimate 30% of IT will be Cloud-

Четврти феномен *је Cloud* рачунарство чије тржиште доживљава велики раст (са око 10% у 2012. године на 30% до 2015.)[172]. Према истраживању *WaveLength Market Analytics and Winn Technology Group* (*Five Key Themes in Enterprise Cloud Computing Migration*) 58% од средњих и великих предузећа у САД већ користе или планирају да користе *Cloud*. Око 41% тог тржишта чине она предузећа која активно користе или испробавају неку врсту C*loud* решења, а још 17% планирају да га уведу. У следеће две године очекује се још веће коришћење приватних, јавних и хибридних *cloud* сервиса/платформи (по рангу су: *Cloud, Egnyte, Google Apps, OpenDrive, Dropbox, Amazon Cloud Drive*)[173]. При томе до 2017. године више од половине пословних C*loud* сервиса ће бити хибридних[174]. Трендови појазују, наравно, највећи пораст на тржишту САД[175].

По Извештају из 2012. године о услугама везаним за *Cloud* складиштење било је преко 375 милиона интернет корисника који их је користило и очекивало се да ће бити 500 милиона до краја те године године, а до краја 2013. године око 625 милиона[176]. Нова студија[177] предвиђа да ће се до 2017. године тај број попети на 1,3 милијарде[178].

Сматра се да ће доминација персоналних рачунара у току 2014. године[179] бити замењена личним *Cloud* у центрима „дигиталног живота" корисника[180].

Колико се користе интернет, мобилни телефони, друштвене мреже и *Cloud* рачунарство?

По подацима *Statistic Brain* 11 милијарди људи месечно претражује вебсајтове само у САД, а дневно се пошаље 210 милијарди порука преко електронске поште[181].

---

based by 2015, (2011), http://www.businesswire.com/news/home/20110517005132/en/Cloud-Computing-Penetration-Enterprise-Gaining-Momentum, приступљено 28.3.2014;

172 Cloud Computing Penetration into Enterprise IT Gaining Momentum WaveLength Market Analytics & Winn Technology Group Report Says Early Cloud Users and Planners Estimate 30% of IT will be Cloud-based by 2015, (2011), op. cit;

173 2014 Best Cloud Computing Services Comparisons and Review, (2014), http://cloud-services-review.toptenreviews.com/, приступљено 28.1.2014;

174 Brown D. (2014), Is This the Year of the Hybrid Cloud?, http://www.hybridcloudforum.com/45/year-hybrid-cloud, приступљено 11.4.2014;

175 ISM Projected To Cost U.S. Cloud Computing Industry $35B, http://www.forbes.com/sites/louiscolumbus/2013/08/08/prism-projected-to-cost-u-s-cloud-computing-industry-35b/, приступљено 28.3.2014;

176 Cloud Computing Penetration into Enterprise IT Gaining Momentum WaveLength Market Analytics & Winn Technology Group Report Says Early Cloud Users and Planners Estimate 30% of IT will be Cloud-based by 2015, (2011), op. Cit;

177 Cloud Services Users Will Hit 625 Million in 2013: IHS, http://slashdot.org/topic/cloud/cloud-services-users-will-hit-625-million-in-2013-ihs/, приступљено 2.3.2014;

178 Lardinois F., Report: Cloud Storage Services Now Have Over 375M Users, Could Reach 500M By Year-End, http://techcrunch.com/2012/10/15/report-cloud-storage-services-now-have-over-375m-users-could-reach-500m-by-year-end/, приступљено 15.1.2014;

179 Gartner Special Report Examines How Businesses Must Meet Consumers' Cloud Expectations in Order to Win Customers, http://www.gartner.com/newsroom/id/1947315, приступљено 15.4.2014;

180 Personal Cloud Adoption: Steady March Towards One Billion Users by 2016, http://blog.tmcnet.com/thinking-out-cloud/2012/09/personal-cloud-adoption-steady-march-towards-one-billion-users-by-2016.html, приступљено 28.3.2014;

181 Internet Statistics, http://www.statisticbrain.com/internet-statistics/, приступљено 4.2.2014;

Подаци за Европску унију дати у специјалном издању **Извештаја о cyber сигурности**[182], на основу посебних истраживања која се понављају већ неколико година, показују да је у 2013. години 41% становника користило интернет неколико пута дневно, односно стално у току дана, једном дневно 13%, а 10% неколико пута недељно. Уопште га не користи 28%. Када се ти подаци упореде са 2012. годином виде се тенденције смањивања за поједина времена коришћења: једном недељно и никад је било више те године за 1%. Остало се поклапало између те две године. Једини пораст од 1% има категорија једном месечно.

Швеђани (85%), Холанђани (82%) и Данци (81%) највише користе интернет јер му приступају бар једном дневно. У овим земљама веома мали број испитаника каже да никада не користе интернет - 6% у Шведској, 7% у Холандији и 8% у Данској. Проценат испитаника који никада не користе интернет је највиши у Румунији (50%) и Португалији (49%). У следећим земљама је низак проценат приступа интернету, а испитаници то чине најмање једном дневно - 35% у Румунији и 36% у Португалији. Најмање корисника који приступају интернету, бар једном дневно је у Мађарској (36%)[183].

За шта се све користе мобилни телефони?

Као и интернет и мобилни, нарочито смарт телефони, имају широку употребу. Битно је истаћи да све већи број људи препознаје ове телефоне као уређај број један за комуникацију. Чак 48% Аустралијанаца их идентификују управо тако. У анализи датој у *ACMA* Извештају констатује да се смарт телефони све више користе за повезивање са мрежама[184], нарочито за претраживање информација на веб-сајтовима, за ажурирање података о спорту, о времену, вестима, за слање порука преко е- поште, добијање упутстава, препорука, за коришћење сајтова социјалних мрежа, повезивање са аудио и видео-садржајима, плаћање рачуна, "скидања" аудио и видео-садржаја, наручивња роба и услуга.

А за шта се и колико сати користе друштвене мреже? Различите су сврхе и намене[185].

Cloud рачунарство је нашло широку примену у разним областима[186]. Најзаступљеније је у пословању, државној и локалној администрацији, образовању, маркетингу, биотехнологијама, фармацији, људским ресурсима, банкама и другим финансијским институцијама, библиотекама, али и код појединаца[187].

182 Eurobarometer Special Surveys 404, op. cit;

183 Eurobarometer Special Surveys 404, op. cit.

184 ACMA, (2012), Communications report 2011. – 12 series Report 3 – Smarthphones and tablets Take –up and use in Australia, Summarz report, http://www.acma.gov.au/webwr/_assets/main/lib310665/report-3-smartphones_tablets-summary.pdf, приступљено 28.3.2014;

185 Statistic Brain, (2014), Social Networking Statistics, http://www.statisticbrain.com/social-networking-statistics/, приступљено 27.1.2014;

186 Daly J. (2013), 13 Cloud Computing Stats for CIOs, http://www.statetechmagazine.com/article/2013/09/13-cloud-computing-stats-cios, приступљено 27.1.2014;

187 Analytics, Cloud Computing Challenge Flat Growth in Forrester's Tech Market Outlook for 2012, (2012), http://socialmediatoday.com/wwwshirazdattacom/421657/analytics-cloud-computing-challenge-flat-growth-forrester-s-tech-market-out, приступљено 26.1.2014;

Међутим, интернет, мобилни телефони, друштвене мреже и *Cloud* рачунарство не користе се само ради „добрих и позитивних ствари". Често се користе за незаконите, штетне и неморалне сврхе[188]. Рачуна се да је, нпр. 40% корисника друштвених мрежа било жртве cyber криминала на њиховим платформама, 1/6 корисника ових мрежа су пријављивали да им је неко упао у профил и представљао се касније као они, 3/4 верује да су cyber криминалци поставили своје сајтове на друштвеним мрежама, 1/10 корисника друштвених мрежа су били жртве преварних и лажних линкова на њиховим платформама, а 38% корисника мобилних телефона је доживело неку од активности cyber криминала у последњих 12 месеци[189].

По истраживању спроведеном у Републици Србији ситуација је нешто другачија. Највећи број се није срео са злоупотребом сопствених података, док је 8% свих испитаника имало таквих проблема. Највише младих од 14 до 18 година старости је имало проблем са злоупотребама.

Најчешћа злоупотреба је добијање нежељених порука (*spam*), затим крађа идентитета и он-лајн узнемиравање. Најмањи проценат испитанка изјавио је да је злоупотреба података подразумевала физичко узнемиравање.

Када су у питању негативна/непријатна дешавања на друштвеним мрежама заступљено је преузимање профила, отварање лажног профила, постављање фотографија без питања и таговање, позиви непознатих особа на број телефона који су оставили на профилу, разне „сексуалне" понуде и пословне понуде. У односу на укупан број оних који поседују налоге на друштвеним мрежама до 20% младих је доживело да им неко преузме идентитет.

Cyber малтретирање/шиканирање преко друштвених мрежа је присутно. Од оних који су то доживели највећи број су старости од 18 до 30 година (јер је најзаступљенија на друштвеним мрежама).

У Европској унији, по Извештају из 2013. године, најчешћи облици злоупотреба су:

- крађа идентитета;
- преварни приступ електронској пошти или преварни телефонски позиви ради приступа шифрама, рачунару или подацима о личности;
- он-лајн превара код које се купљена роба не испоручује, фалсификује;
- приступ дечијој порнографији на интернету;
- случајни приступ материјалима који промовише расну мржњу или верски екстремизам;
- онемогућавање коришћења услуга због cyber напада;
- хаковање друштвене мреже или *e-mail* налога;
- преваре са кредитним картицама или банкарске преваре на мрежи.

188 Jaser J. (2010), Smart Phones: The Next Cyber Crime Frontier, http://www.cocc.com/smart-phones-cyber-crime.html; Cybercrime on social networks continues to climb, (2011), http://www.net-security.org/secworld.php?id=11464, приступљено 20.1.2014;

189 Norton Cybercrime Report, (2012)&(2013), go.symantec.com/norton-report-2013, приступљено 22.1.2014;

Међутим, у коришћењу *Cloud* рачунарства[190] поред великих погодности[191] појављују се и озбиљни проблеми[192]. Од 7 проблема које је идентификао *BSA* 4 су директно везано за cyber криминал: „отмица" података, нарочито о личности (информациона приватност); угрожавање сигурности; поједини облици cyber криминала (крађе, нарочито идентитета) и интелектуалне својине[193].

По Другој студији[194], објављеној у септембру 2013. године од стране *Info Pro,* испитивање је спроведено са 451 корисником, а чак њих 83% суочавало се са значајним препрекама као што су: забринутост од губитка контроле (према истраживању 179 *Cloud* провајдера 48% сматра да је **губитак контроле** највећи страх корисника[195]); **безбедност и приватност података** и **неизвесност око стварних уштеда**. Очигледно је да безбедност најпроблематичнија компонента[196].

У таквом окружењу и са таквим појединцима све се чешће покушавају изборити не само многа национална права, међународне организације и асоцијације, већ и приватни сектор и корисници не би ли се ублажиле негативне последице и смањили губици који настају због неоматаних криминалних активности. То су финансијски губици, губитак репутације, времена, угрожавање поверења корисника, потрошача, смањење продуктивности, осећај несигурности, угрожености и беспомоћности појединаца; затим губитак породичних веза, нестабилност, конфликти, психолошки породични проблеми, комуникациони проблеми. Посебан проблем је национална сигурност, здравља нације и слично. Утицаји cyber криминала су вишеструки[197]: друштвени, економски/пословни, политички, психолошки, породични, еколошки[198].

А шта је он, у ствари?

---

190 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, (2012), Unleashing the Potential of Cloud Computing in Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF, приступ-љено 28.3.2014;

191 McAfee A., (2012), Modeling the Cost of Cloud vs. On-Premise Computing, http://policybythenumbers.blogspot.com/2012/10/modeling-costs-of-cloud-vs-on-premise.html, приступљено 15.1.2014;

192 LaBarge R., McGuireT., (2012), Cloud Penetration Testing, http://arxiv.org/ftp/arxiv/papers/1301/1301.1912.pdf, приступљено 15.1.2014;

193 BSA Global cloud computing scorecard, http://cloudscorecard.bsa.org/2012/, приступљено 10.01.2014.

194 2013 Cloud Computing Outlook – Cloud Computing Wave 5, https://451research.com/report-long?icid=2831, приступљено 10.1.2014;

195 Overcoming the Fear of Cloud Computing, (2013), http://www.csc.com/cloud/publications/96289/96297-overcoming_the_fear_of_cloud_computing, приступљено 15.2.2014;

196 Angeles S., (2013), 8 Reasons to Fear Cloud Computing, http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html, приступљено 19.1.2014;

197 Amosun P.A, O Ige O.I. (2013), Impact Of An Action Cyber Crime Prevention Programme On In-School Aged Children's Attitude To Crime Prevention Concepts In Civic Education And Social Studies, Proceedings-st Annual International Interdisciplinary Conference, AIIC 2013, 24-26 April, Azores, Portugal, http://eujournal.org/index.php/esj/article/viewFile/1454/1463, приступљено 19.1.2014;

198 Petrović N. Drakulić M. Vujin V. Drakulić R. Jeremić V. (2011), Climate changes and green information technologies, Management, no 59/2011, pp. 35–45;

2. CYBER КРИМИНАЛ – ПОЈАМ И ОБЛИЦИ

Од када се појавио овај специфичан облик криминала изазвао је бурне реакције у теорији и пракси. Расправе су се водиле и још се воде око тога да ли уопште овај криминал постоји, који термин се користи, шта му је суштина, који су му облици, по чему се разликује од осталих, који му је *modus operandi,* које ће се право променњивати, шта су особености учнилаца, како га доказивати, где је место извршења, шта је објект и друго. Иако се појавио пре неку деценију, његов развој је спорaн јер се не зна тачно од када почиње његова „историја“ и да ли је уопште има. Дилеме, несугласице, проблеми и различита мишљења прате теоријско, нормативно и оперативно тумачење, што је од овог феномена створило једну од највећих „мистерија“ данашњице. Са друге стране, његова сложеност и променљивост захтевају одговарајуће одговоре. Интересантно је да је право реаговало међу првим. Још увек нејединственост појмовног одређења није спречило међународно реаговање. Наиме, међународна регулатива је била бржа и од теорије и од националне реакције. И још једна контрадикторност и неуобичајеност – Европа (тачније, Савет Европе) реагује пре свих осталих доношењем Конвенције о *cyber* криминалу којој су се придружиле и нечланице. Претходила јој је још једна необичност – предлог Стенфордске међународне конвенције. Запетљано клупко треба одмотати и доћи до другог краја. А тај други крај води до нереалног *cyber* простора у коме се реално дешавају злоупотребе и у коме су жртве, такође, реалне. Дешава се сусрет два света у чијем средишту је криминал.

2.1. Cyber криминал – термини

Појава специфичних облика понашања у специфичном окружењу изазвала је бројне недоумице, а једна од њих је његов назив, односно којим термином се он најбоље детерминише[199]. Тако су се појавили следећи термини: компјутерски криминал, криминал везан за компјутере, интернет криминал, мрежни криминал, високотехнолошки криминал, ВТК, hi-teh криминал, дигитални криминал, електронски криминал, е-криминал, информационо-технолошки криминал, криминал електронских комуникација и слично, а све у зависности од тога шта се ставља у први план. У следећој табели су дати најчешће коришћени термини на српском језику, затим објекти и термини на енглеском језику.

199 Drakulić M. (1996), Osnovi Kompjuterskog prava, Beograd, DOPIS, str.12;

Табела 1. Термини

Криминал	*Објект*	*Crime*
компјутерски криминал /криминал везан за компјутере/рачунарски криминал	**компјутери / computers**	*computer crime / computer related crime*
интернет криминал	**интернет / Internet**	*Internet crime*
мрежни криминал	**Мрежа / Network / net**	*Net crime*
високотехнолошки криминал / ВТК	**висока технологија / high technology**	*High technology crime / hi teh crime*
електронски криминал/ е-криминал	**електронски/ electronic**	*electronic crime / eCrime*
дигитални криминал	**Дигитални / digital**	*digital crime*
Информационо технолошки криминал	**информационо комуникационе технологије/ information communication technologies**	*information technology crime*
информатички криминал	**информатика**	*informatics crime*
криминал електронских комуникација	**електронске комуникације/ electronic communications**	*electronic communication crime*
cyber криминал/ сајбер криминал/ кибер криминал	**cyber/ сајбер простор/ cyberspace**	*cyber crime*

Сви ови термини се користе да опишу специфичан криминал, али они нису синоними. Напротив, пошто им је различит објекат или имају различиту улогу у криминлу, односе се на различите појмове.

У Републици Србији, у теорији и пракси, појављују се као најзаступљенија 3 термина: високотехнолошки криминал, cyber (сајбер) и компјутерски криминал. При томе под утицајем регулативе у којој је искључиво заступљен термин високотехнолошки криминал[200], поједини аутори аутоматски прихватају нормативно

200 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Službeni glasnik RS, br. 61/2005; Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu, Službeni glasnik RS, br. 19/2009;

одређење, нарочито они који су повезани са борбом против овог криминала[201]. Овај термин се налази и у преводу Конвенције о cyber (сајбер) криминалу која је ратификована као Конвенција о високотехнолошком криминалу, чиме се показало непознавање суштине и ишло на „сопствена“ решења увођењем језичке збрке. Да се хтело да се акт Савета Европе назове под тим именом није било никакве сумње да би се то и десило, али у свим документима и анализама које су претходиле конференцији у Будимпешти где је прихваћена, није било тих недоумица.

У теорији се код појединих аутора појављује и термин cyber криминал[202] мада већи број користи термин високотехнолошки криминал[203]. Једна група аутора је остала код термина компјутерски криминал у својим старијим радовима[204], мада су неки и даље са овим термином у новијим[205] радовима. Модификација је присутна у термину рачунарски криминал[206]. Најинтересантнија је варијанта код коришћења термина кибер-криминал[207] јер се везује за кибер-простор[208] и термине: кибер-секс, кибер-лопов, кибер-култура, кибер-школа, кибер-банка, пошто је усвојени

---

201 Урошевић В. Уљанов С. Вуковић Р. (2010), Полиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије; http://www.singipedia.com/content/1071-Policija-i-visokotehnoloki-kriminal-Primeri-iz-prakse-i-problemi-u-radu-MUP-a-Republike-Srbije; Živanović S., (2011), Praktični aspekti visokotehnološkog kriminala, Zbornik IAK, str. 138 – 152, http://www.iak-bl.com/images/zbornik/2008/10.pdf, приступљено 5.1.2014;

202 Drakulić M. Drakulić R. (2010), Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnom evropskom pravu, Telekomunikacije, br. 6/2010, http://www.telekomunikacije.rs/arhiva_brojeva/sesti_broj/prof_dr_mirjana_drakulic,_mr_ratimir_drakulic:_evropska_perspektiva_regulisanja_internet_usluga:_izazov_tradicionalnom_evropskom_pravu.344.html; Вулетић Д.,(2011), Одбрана и претње у сајбер простору, http://www.isi.mod.gov.rs/pdf/publikacije/1328179353_Odbrana%20od%20pretnji%20u%20sajber%20prostoru%20-%20za%20sajt.pdf; приступљено 21.01.2014.; Путник Н., (2009), Сајбер простор и безбедносни изазови, Београд, Универзитет у Београду, Факултет за безбедност; Младеновић Д. (2013), Међународни аспект сајбер ратовања, Београд, Одбрана;

203 Prlja D. Reljanović M. (2009), Visokotehnološki kriminal – uporedna iskustva, Strani pravni život, br. 3/2009. str. 161-184; Reljanović M. (2007), Visokotehnološki kriminal - pojam, regulativa, iskustva, Strani pravni život, br. 3, str. 75-98; Jerković R. Borba protiv visokotehnološkog kriminaliteta u Srbiji, Telekomunikacije, http://www.telekomunikacije.rs/arhiva_brojeva/treci_broj/ranko_jerkovic:_borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html; Ивановић З., Бановић Б., (2010), Мобилне социјалне мреже – нови ризик високотехнолошког криминала, у: Злоупотреба информационих технологија и заштита – зборник радова ЗИТЕХ 10., *www.singipedia.com/attachment.php? attachmentid*, приступљено 21.1.2014;

204 Шкулић М. (1997), Компјутерски криминалитет: Да ли смо беспомоћни пред овом опасношћу, Југословенски часопис за правну информатику, Компјутери и право, Вол. 5, број 2, Београд, стр. 43-61; Бановић Б., (2003), Компјутерски криминалитет и заштита личности, Безбедност 1/2003, стр. 16 – 43; Đurić-Lulić A., (2003), Mogućnosti krivično-pravne zaštite od kompjuterskog kriminaliteta po pozitivnom zakonodavstvu SRJ, www.netizen.co.yu/toni/2ojt/index:php?strana=kompjuteri, приступљено 26.09.2004. Drakulić M. (1996), op. cit., str. 386-460;

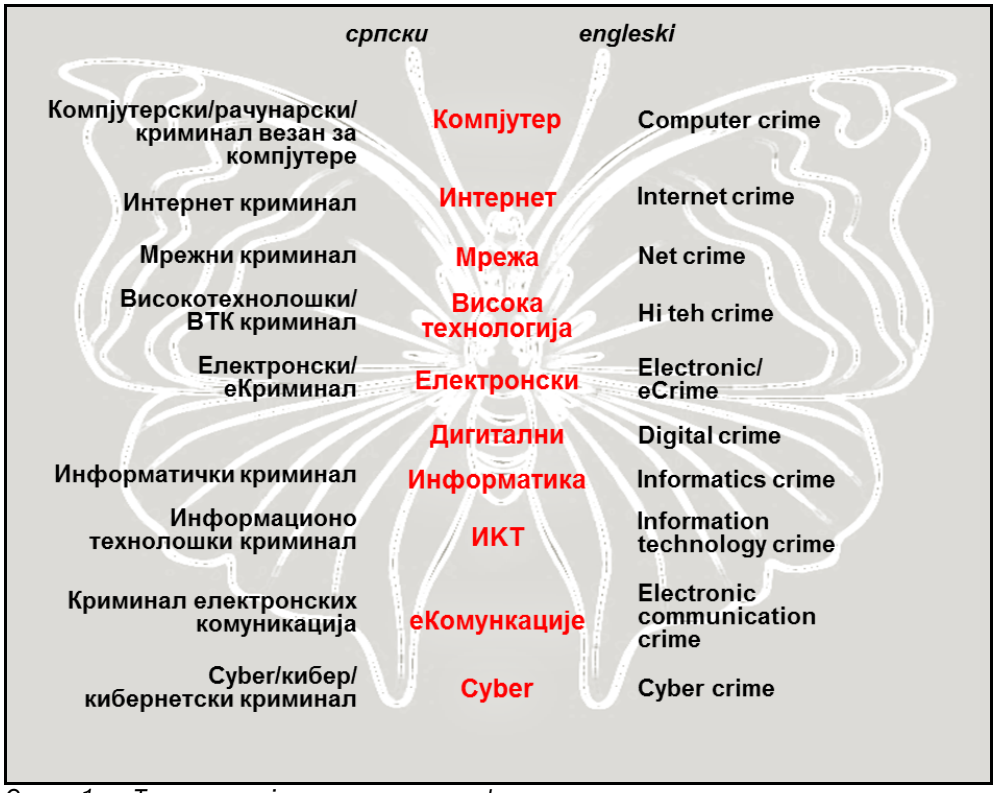
205 Milošević M. (2007), Aktuelni problemi suzbijanja kompjuterskog kriminala, Nauka, bezbednost, policija, 2007, vol. 12, br. 1, str. 57-74;

206 Водинелић В. (1990), Методика откривања, разјашњавања и доказивања рачунарског криминалитета, Приручник 4/90, МУП Хрватске;

207 Petrović S. (2012), Dilema: kiber ili sajber, Strani pravni život 2/2012., str 368–377, http://www.itvestak.org.rs/library/DILEMA%20KIBER%20ILI%20SAJBER.pdf, приступљено 21.11.2013;

208 Petrović S.R. (2006), O neophodnosti nacionalne strategije zaštite kiber-prostora, Nauka, bezbednost, policija, vol. 11, br. 2, str. 3-28;

префикс кибер „требало да искаже поштовање и захвалност коју информатика дугује кибернетици“. И тако се из поштовања и захвалности у српском језику појавио и овај термин као последица чистог неразумевања, уз додатну аргументацију да се „наш термин кибер[209] користи и у другим земљама из окружења, као и Русији[210].



Слика 1. Термини који се користе за cyber криминал

У Федерацији БиХ[211] и Хрватској[212] користи се термин **киберентички криминал**, док се у Словенији појављује појам **кибернетски криминал**[213].

209 Међутим, „po autorovom dubokom uverenju ne postoji ni jedan *objektivan* razlog koji bi, u ovom slučaju, opravdao *zamenu našeg* postojećeg termina (*Kiber*) sa istim terminom, ali sa engleskim izgovorom (*Sajber*)“;

210 Иако је све очигледније да се нпр. у Хрватској води полемика о недостацима коришћења термина кибернетички криминал;

211 Odluka o ratifikaciji Konvencije o kibernetičkom kriminalu, http://www.fup.gov.ba/wp-content/uploads/ 2012/01/Konvencija-o-cyber-kriminalu-Budimpesta.pdf, приступљено 2.12.2013;

212 Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, (2002), http://narodne-novine.nn.hr/clanci/medunarodni/327873.html; Škrtic D. (2009), Implementacija odredbi Konvencije o kibernetickom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo, http://www.fvv.uni-mb.si/dv2009/Zbornik/clanki/skrtic.pdf; Vuković H. (2012), Kibernetska sigurnsot i sustev borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, www.*hrcak.srce.hr/file/ /148443*, приступљено

У Црној Гори је присутан и термин **рачунарски криминал**[214], мада се у Стратегији донетој 2013. године користи термин **cyber безбједност**[215]. Овај други термин појављује се и у радовима појединих аутора са те територије[216].

У Републици Српској, вероватно под утицајима који долазе из Србије, користи се термин **високотехнолошки криминал**, али не у регуалтиви већ у оперативи - Одељење МУП-а за борбу против високотехнолошког криминала.

Република Македонија је ратификовала Конвенцију за компјутерски криминал[217] и тако се прикључила групи земаља која користи термин **компјутерски криминал**[218]. Формирана је специјализована јединица МУП-а и посебно тужилаштво[219] за компјутерски криминал.

21.1.2014.; Vojković G. Štambuk-Sunjić M. (2006), Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split;

213 Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih /MKKKDP/Ur.l. RS-MP, št. 17/2004. http://www.uradni-list.si/1/objava.jsp?urlmpid=200468; Kovačič M. (2008), Kiberkriminal, http://matej.owca.info/predavanja/Kibernetski_kriminal_Kovacic.pdf; Šugman K., (2006), Slovenija i njezino približavanje eu na području policijske i sudske suradnje, www.hrcak.srce.hr/file/130332*; Svete U. Kolak A. Varnostna relevantnost kibernetskega prostora v obdobju web 2.0,* http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/vojaski_izzivi/ svi_13_3.pdf, приступљено 21.1.2014.*; Bernik I. Prislan K.* (2012), *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem,* Fakulteta za varnostne vede, Ljubljana;

214 Crna Gora je 3. марта 2010. ratifikovala Sporazum o ratifikaciji Konvencije o računarskom kriminalu (CETS 185 od 7. Aprila 2005.) koji je stupio na snagu 1. jula 2010. Crna Gora je 3. марта 2010. ratifikovala Protokol o ksenofobiji i rasizmu (CETS189) zajedno sa Konvencijom i stupio je na snagu 1. jula 2010. Crna Gora je takođe potpisala Konvenciju o Zaštiti djece od seksualnog iskorišćavanja i seksualnog zlostavljanja (CETS 201) 18. juna 2009. i ratifikovala je u novembru 2010, i stupila je na snagu 1. марта 2011;

215 Strategija sajber bezbjednosti Crne Gore 2013–2017, http://www.gsv.gov.me/biblioteka/strategije?query =sajber%20bezbjednost&sortDirection=desc, приступљено 25.2.2014;

216 Tanilir M.N. Tahirović M. (2013), Međunarodna bezbjednost i sajber opasnosti, Monet, Institut za strateške studije i projekcije (ISSP), Edicija Bezbjednost, Volume 4,стр. 8 – 26, http://issp.me/wp-content/uploads/2012/10/monet34se.pdf, приступљено 25.2.2014;

217 Ратификувана во Советот на европа на 15 септември 2004. година (Објавена во „Службен весник на РМ" бр. 41/2004)

218 Конвенција за компјутерски криминал, Република Македонија, Група на држави за борба против корупцијата, http://old.soros.org.mk/dokumenti/Makedonija&Greko.pdf;

219 Криминалистичке службе су прошле године истраживале скоро 190 случајева компјутерског криминала, што је три пута већи број у односу на претходну годину. „У првој половини ове године разоткривена су 24 компјутерска кривична дела за која смо поднели кривичне пријаве, www.setimes.com, приступљено 17.3.2014;

Табела 2. Коришћење термина у бившим југословенским републикама

Земља	*Термин*	*Коришћење*
Република Србија	**Високотехнолошки криминал**	Законодавство/ литература
	Cyber (сајбер) криминал	Литература
	Компјутерски (рачунарски) криминал	
	Кибер криминал	
Република Хрватска	**Кибернетички**	Законодавство/ литература
Република Словенија	**Кибернетски**	Законодавство/ литература
Република Црна Гора	**Рачунарски**	Законодавство/ литература
	Cyber безбједност	Стратегија
Федерација Босна и Херцеговина	**Кибернетички**	Законодавство
Република Српска	**Високотехнолошки**	Полицијска оперативa/ литература
Република Македонија	**Компјутерски криминал**	Законодавство/ полицијска оперативa

2.2. Cyber криминал – различити аспекти у дефинисању

Cyber криминал је део наше свакодневице, иако често нисмо ни свесни да се са њим сређемо или га, чак, и сами чинимо. Појава и силно повећање броја кривичних дела учињених помоћу или у вези са рачунарима, постали су стално растућа опасност од које се треба, а све више и мора, бранити. Међутим, то је феномен који су правници дуго одбијали да примете и признају, тако да теоријске расправе и разни покушаји да се дефинише и класификује још увек трају[220]. Данас су се искристалисала три приступа у одређивању овог криминала: теоријски[221], нормативни[222] и оперативни[223].

220 Управо је то констатовано и у Студији УН, у којој се наводи проблем дефинисања и изостанка једне опште и међународно прихватљиве дефиниције. Такође, наводи се да постоји онолико дефиниција колико и аутора и написаних студија, али оно што је сигурно и око чега се сви слажу је да - феномен постоји;

221 Игњатовић Ђ. 1991, Појмовно одређење компјутерског криминалитета, Анали Правног факултета у Београду, бр.1-3/91., стр. 137;

222 United Nations Office on Drugs and Crime, (2013), Comprehensive Study on Cybercrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf; Sieber U., (1998), Legal Aspects of Computer-Related Crime in Information Society – comcrime study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, приступљено 25.2.2014;

223 The Internet Crime Complaint Center (IC3), (2012), 2012 Internet Crime Report, http://www.ic3.gov/media/ annualreport/2012_IC3Report.pdf, приступљено 17.12.2013;

У оквиру теоријског одређења појавило се више концепата, иако многи аутори истичу да „колико аутора толико дефиниција и концепата“. Три су кључне[224].

Један концепт полази од компјутерског криминала, односно од криминала везаног за компјутере и компјутерске мреже и других система које користе учиниоци за своје криминалне активности. Они су алат, циљ или место извршења[225]. Њој се, с једне стране, замера преускост, а с друге, да је преширока (на пример, обухвата и традиционалне злочине као што су убиства, ако је учинилац користио тастатуру да удари и убије жртву)[226]. Овај концепт је, у ствари, већ превазиђен[227].

Други концепт је окренут **cyber простору** као специфичном „станишту“ у коме се користе информационо комуникационе технологије за кривичне, штетне и неморалне радње[228]. У овом простору се дешавају разни напади и активности[229]. Иако му се негирују карактеристике које прате традиционалне облике криминала (нпр. реално време, географски прстор – границе, већа окренутост ка учиниоцу)[230], јасно је да је дошло до демистификације cyber простора и до сагледавања његове „патологије и кримогенозности“, мада је то више на страни појединаца него простора[231]. Колико је то постало значајно види се и из расправа вођених око правног статуса cyber простора и интернета. Јавили су се различити приступи: **монолитни,** који је замењен **плурализмом**. Њега надграђује **мултикултуралистички**[232] који полази од индивидуалног и колективног идентитета појединца и различитих социјалних група. Сви односи могу се управо свести на више генерација индивидуалних права која се преко и у оквиру њега реализују, а разне друштвене групе и мреже су део колективног идентитета. Потом настаје **комунитаристички** приступ чије су окоснице либерализам и индивидуализам без

224 ITU, (2012), Understanding cybercrime: Phenomena, challenges and legal response, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, приступљено 17.12.2013;

225 Goodman M D. (1997), Why the police don't care about computer crime, Harvard Journal of Law & Technology Volume 10, Number 3., 468 - 469. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech 465.pdf, приступљено 18.12.2013;

226 ITU, (2012), op. cit., стр. 12;

227 Yang Z. (2011), A Survey of Cybercrime, http://www1.cse.wustl.edu/~jain/cse571-11/ftp/crime.pdf, приступљено 18.12.2013;

227 Dunlap C.J. (2008), Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors, http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1032&context= nlr, приступљено 21.12.2013;

228 Bernik I. (2013), Cybercrime and Cyber Warfare, Wiley, FOCUS Series, стр. 5;

229 Wall D.S. (2005), The Internet as a Conduit for Criminals‘, in Pattavina A. (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage, pp. 77-98;

230 Gottfredson G. & Hirschi T. (1990), A general theory of crime. Stanford, CA: Stanford University Press, http://www.mltei.org/cqn/Adolescent%20Development/Resources/Gender,%20Race,%20Ethnicity%20&%20SES/Gottfredson&%20Hirshi,%20A%20general%20theory%20of%20crime.pdf, приступљено 1.12.2013;

231 Wall D.S. (2008a), Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime, Information, Communication & Society, Vol. 11, No. 6, pp. 861-884, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155, приступљено 2.12.2013;

232 Perritt H.H. (1998), The Internet as a Threat to Sovereignty? Thoughts on the InternetsRole in Strengthening National and Global Governance, IT Chicago-Kent, College of Law, Illinois Institute of Technology,http://works.bepress.com/cgi/viewcontent.cgi?article=1030&context=henry_perritt, приступљено 21.12.2013;

доминације. Новијег датума је покушај посматрања интернета и cyber простора као **јавног добра**[233] и **заједничког наслеђа човечанства** (*common heritage of mankind - CHM*)[234] које је посебно присутно у међународном праву, повлачећи првобитно аналогију[235] са **правним статусом мора**[236]. Покушало се и изједначење са **свемиром**[237]. Посебан је приступ интернету и cyber простору **као људском праву**, односно универзалном праву на приступ интернету и cyber простору, праву на приступ телекомуникацијама и праву на заштиту од недозвољених и штетних садржаја[238], односно праву на безбедност у cyber простору или на безбедност cyber простора[239].

Трећи концепт полази од дефинисања појма cyber криминала са аспекта различих **наука и научних дисциплина**. Психолошки је фокусиран на жртве и учиниоце[240]. Овај аспект треба да да одговоре на питања "ко, шта, где, када, зашто и како"[241]. На основу утврђивања мотива[242] и карактеристика личности дефинишу се и профили учиниоца, али и жртава. Такође, на основу карактеристика личности и учињених „напада“ дају се и одређења типова кривичних дела и типологије

---

233 Shackelford J.S. (2009.), From nuclear war to net war: analogizing cyber attacks in international law, http://www.grocjusz.edu.pl/Materials/_archiwum/archiwum2009/pd_sem_2611_B.pdf, приступљено 21.12.2013;

234 Serrano A.S. (2006), Internet Regulation: A Hard-Law Proposal, www.JeanMonnetProgram.org, приступљено 21.12.2013;

235 Konvencija UN o pravima mora (*UNCLOS – United Nations Convention on the Law of Sea*, 1982.) po Serrano A.S. Internet Regulation and the Role of International Law, http://www.mpil.de/shared/data/pdf/pdfmpunyb/06_antoniov.pdf, приступљено 21.12.2013;

236 Овакав концепт је крајње неодговарајући почевши од проблема како дефинисати “наутичке миље” над којим би државе ипак имале суверенитет, до тога шта би биле његове “територијалне воде, дубине, ширине и висине”;

237 Базирана на следећим *принципима*: а) истраживање и коришћење свемира врши се за добробит и у интересу свих земаља и биће простор целог човечанства; б) свемир ће бити бесплатан за истраживање и коришћење од стране свих држава; в) свемир није предмет националног присвајања, односно суверенитета, и не осваја се и не брани употребом силе или окупацијом, нити на неки други начин; г) бити одговоран за све владине или невладине активности у националном простору; и д) да су одговорне и за штету у свом простором и зато треба да избегавају штетне контаминације простора. Осталих 4 се не могу „протегнути“ на cyber простор. Mussington D. (2007.), The Profileration Chalanges of Cyberspace, http://www.yorku.ca/yciss/publications/CyberspacePart2.pdf, приступљено 27.12.2013;

238 Drakulić M. Drakulić R. (2010), Regulacija interneta, studija, RATEL, Beograd;

239 Brenner S.W. Clarke L. (2010), Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. 43:, http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/Brenner-_Final_1.pdf, приступљено 21.12.2013;

240 Buss M.D. (2012), The Evolutionary Psychology of Crime, Journal of Theoretical and Philosophical criminology Commentary, Special edition, January, 2012, Vol. 1(1):90-98, http://homepage.psy.utexas.edu/HomePage/Group/BussLAB/pdffiles/Evolutionary-psychology-and-crime.pdf; Gráinne Kirwan; Power A., (2012), The Psychology of Cyber Crime: Concepts and Principles, http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf, приступљено 27.12.2013;

241 Shaw D.E. (2006), The role of behavioral research and profiling in malicious cyber insider investigations, hftp://163.13.200.222/Prof_Liang/%BC%C6%A6%EC%C5%B2%C3%D1/Volume%203%20(2006)/Issue%201/Pages%2020-31.pdf, приступљено 21.12.2013;

242 Ngafeeson M. (2010), Cybercrime Classification: A Motivational Model, http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf, приступљено 21.12.2013;

учиниоца. Тако се нпр. инсајдерски компјутерски криминалци појављују као шпијуни, саботери, лопови и злостављачи[243].

Социолошки[244] се бави друштвеним аспектима овог криминала и објашњењем његовог друштвеног контекста.

Појављују се и економски[245], криминолошки[246], криминалистички[247], антрополошки[248], биолошки[249], медицински, техничко/технолошки[250], еколошки[251], менаџмент[252] и други аспекти[253] овог криминала и учинилаца.

---

243 Nykodym N. Taylor R. Vilela J. (2005), Criminal profiling and insider cyber crime. Computer Law and Security Report, 21:408–14., приступљено 21.12.2013;

244 Saini H. Rao Y.S. Panda T.C. (2012), Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209, www.ijera.com, Vol. 2, Issue 2, pp.202-20; Holt T.J., (2011), Cybercrime and Criminological Theory: Fundamental Readings on Hacking, Piracy, Theft, and Harassment, University Readers, San Diego; Grabosky P., Computer Crime: A Criminological Overview, http://www.aic.gov.au/media_library/conferences/other/grabosky_peter/2000-04-vienna.pdf, приступљено 11.11.2013;

245 Cardenas A.A. Radosavac S. Grossklags J. Chuang J. Hoofnagle C. (2009), An Economic Map of Cybercrime, http://chess.eecs.berkeley.edu/pubs/772/cardenas_2009.pdf; Becker G.S. Crime and Punishment: An Economic Approach, http://www.nber.org/chapters/c3625.pdf, приступљено 24.11.2013;

246 Yar M. (2005), The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory, Journal of Contemporary Criminal Justice November, pp. 407-427., http://wenku.baidu.com/view/7855fafe700abb68a982fb5f.html, приступљено 24.11.2013;

247 Hinduja S. (2007), Computer Crime Investigations in the United States:Leveraging Knowledge from the Past to Address the Future, International Journal of Cyber Criminology, Vol 1 Issue 1., http://www.cybercrimejournal.com/sameer.pdf, приступљено 24.11.2013;

248 Libin A. Libin E. (2005), Cyber-anthropology: a new study on human and technological co-evolution. Stud Health Technol Inform. 118:146-55; Sprondel J.T. Breyer T. Wehrle M. (2011), Cyberanthropology - Being Human on the Internet, 1st Berlin Symposium on Internet and Society: Exploring the Digital Future, Berlin, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1943399; Budka P., (2011), From Cyber to Digital Anthropology to an Anthropology of the Contemporary?, http://www.media-anthropology.net/file/budka_ contemporary.pdf, приступљено 24.11.2013;

249 Fishbein D. (1966), Biological Perspectives In Criminology, http://criminology.fsu.edu/crimtheory/fishbein90.htm; Alper J.S., (1995), Biological influences on criminal behaviour: how good is the evidence, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2548687/pdf/bmj00578-0006.pdf; Raine A., (2002), The Biological Basis of Crime, http://cooley.libarts.wsu.edu/soc3611/soc%20361%20summer% 202008/biologicalbasiscrime.pdf, приступљено 5.1.2014;

250 Lipson H. (2002), Trackin and Tracing Cyber/Attacks: Technical Challenges and Global policy Issues, http://www.dtic.mil/dtic/tr/fulltext/u2/a408853.pdf, приступљено 5.1.2014;

251 Yar M. op. cit;

252 Beating cybercrime, Security Program Management from the board's perspective, (2013), http://www.ey.com/Publication/vwLUAssets/Beating_cybercrime:_Security_Program_Management_from_the_Board%E2%80%99s_perspective/$FILE/EY-Beating-Cybercrime.pdf; Walker R., (2013), Four tips for mitigating risk of cyber crime, Data loss doesn't just happen, http://www.sas.com/knowledge-exchange/risk/fraud-financial-crimes/four-tips-for-mitigating-risk-of-cyber-crime, приступљено 25.1.2014;

253 Give and Take Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime, (2012), www.enisa.europa.eu; Poonia A.S., Dangayach G.S., Dr. Bhardwaj A., (2011), Technical management issues for resolving the cyber crime, 3rd International Conference on Information and Financial Engineering, IPEDR vol.12, http://www.ipedr.com/vol12/24-C026.pdf, приступљено 25.1.2014;

Посебан је приступ везан за етику[254]. С једне стране везује за етичност у примени информационо-комуникационих технологија[255], интернета и одређеног начина понашања оних који их примењују, а с друге стране од принципа везаних за поједине групе учнилаца. Cyber етика[256] и етика cyber простора[257] развија се већ неколико година, готово од саме појаве cyber простора и криминала. Њих допуњује и етика одређених криминалних група. Најразвијенија је хакерска[258]. Посебан аспект је етички хакинг[259]. Почињу се правити разлике између: *black hat hackers*, *grey hat hackers* и *white hat hackers*[260].

Нормативни приступ је везан за различита одређења[261] у међународним, националним и саморегулаторним актима.

У оквиру **међународне регулативе** примећују се 2 фазе и више праваца.

Фазе су: до 2001. године и од 2001. године до данас. Кључна тачка је доношење Конвенције о cyber криминалу Савета Европе.

У периоду до 2001. године највише међународних регулаторних активности одвијало се у оквиру ОУН, ОЕЦД, ОЕБС, Међународне телекомуникационе уније, Светске организација за интелектуалну својину, Г8, Европске уније, Савета Европе, Интерпола, Еуропола. Сви акти који су се доносили у оквиру ових међународних организација мање су се односили на компјутерски криминал, односно криминал везан за компјутере директно, већ су се регулисала питања за поједине облике/типове овог криминала, за организовани криминал и процедуре. Највише их је било везано за[262]: угрожавање података о личности, односно приватности; компјутерски економски криминал (почетком 80-их регулишу се дела компјутерске крађе, компјутерске преваре, компјутерске шпијунаже, компјутерске саботаже, незаконитог приступа рачунарима и рачунарским мрежама – хакинг); интелектуалну својину, поготово софтвера/рачунарских програма, топографије интегрисаних кола, база података (ауторска, патентна и остала права); незаконите и

254 Warren E. (2011), Legal, Ethical and Professional Issues in Information Security, http://www.cengage.com/resource_uploads/downloads/1111138214_259148.pdf;. Putnam M.S. (2005), Cyber Ethics in a Real World, http://www.character-ethics.org/articles/cyberethics.htm, приступљено 5.1.2014;

255 Sembok T.M.T. (2003), Ethics Of Information Communication Technology (ICT), http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF, приступљено 5.1.2014;

256 Sukhai B.N. (2005), Hacking And Cybercrime, http://jjconline.net/PAD_750/Readings/Class8/Hacking_ And_Cybercrime.pdf, приступљено 5.1.2014;

257 Gunarto H. (2003), Ethical Issues in Cyberspace and IT Society, http://www.apu.ac.jp/~gunarto/it1.pdf

258 Himanen P. (2001), The hacker Ethic and the Spirit of Information Age, http://code.google.com/p/hfg-resources/downloads/detail?name=The.Hacker.Ethic.pdf; Mizrach S. Is there a Hacker Ethic for 90s Hackers?, http://www2.fiu.edu/~mizrachs/hackethic.html, приступљено 5.1.2014;

259 Fadia A. (2005), The Ethical Hacking Guide to Corporate Security, http://www.centroatl.pt/titulos/tecnologias/imagens/e-book-ca-corporate-security-excerpt.pdf, приступљено 5.1.2014;

260 Black Hat White Hat and Gray Hat Hackers Definition, http://ethical-hacking-course.blogspot.com/2012/01/ethical-hacking-is-considered-as-craft.html, приступљено 5.1.2014;

261 Gercke M. (2009), An introduction to cybercrime, http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf, приступљено 5.12.2013;

262 Sieber U. (1998), op. cit.

штетне садржаје и одговорност провајдера (ширења дечије порнографије, расизма, информација које славе и подстичу насиље); кривичне поступке (доказивање; чување доказа; скупљања, чувања и повезивања података о личности; организовани криминал; кривичне процедуре; екстериторијалност) и безбедност[263].

Друга фаза започела је 2001. године доношењем Конвенције о cyber криминалу. Конвенција је „последица" убрзаног умножавања опасности од компјутерског криминала (по изјава ФБИ дуплирао се сваке године[264]), од појаве тероризма подпомогнутог компјутерима и реализованог у интернет окружењу, огромних губитака насталих као „резултат" економског, али и другог криминала везаног за компјутере, с једне стране и све веће доминације националне инфраструктуре која је повезана и којом се рукује помоћу рачунара. Претходна активност је доношење одлуке Европског комитета за проблеме криминала (*CDPC/103/211196*) у новембру 1996. године, којом је предложено Комитету министара да оснује нови Комитет експерата који ће се бавити cyber криминалом *(The Committee of Experts on Crime in Cyber-Space PC-CY*)[265]. Процес доношења Конвенције је почео у априлу 1997. године када је Комитет експерата о криминалу у cyber простору започео рад на тексту. У априлу 2000. године Комитет је објавио свој први нацрт Конвенције. Од тада до доношења Конвенције Комитет је стално објављивао нове нацрте (последња је била верзија број 27, која је пуштена у расправу у мају 2001. године и о којој се расправљало током 50. пленарне седнице, уз нацрт Протокола о расистичкој и ксенофобичној пропаганди преко рачунарске мреже, као допуне Конвенције). Овако допуњена верзија је објављена 29. јуна 2001. године и поднета као коначни нацрт Комитету министара који је расправљао и усвојио га у септембру 2001. године у Будимпешти. Усвојена Конвенција је била спремна за потписивање у новембру 2001. године од 43 земље чланице Савета и посматрача, укључујући Сједињене Америчке Државе и друге земље нечланице. Ступила је на снагу када ју је пет држава, укључујући најмање три државе чланице Савета Европе, ратификовало. До сада су је прихватиле 52 земље (11 је потписало и 41 ратификовало)[266]. Нечланице Савета Европе, као што су Аустралија, Канада, Доминиканска Република, Јапан, Маурицијус, Јужна Африка, такође су јој приступиле. Решења дефинисана у овој Конвенцији претендују да постану глобални стандарди, иако постоје и другачији приступи. Тако, критицизам по *Brian Harley* који се појавио у оквиру Међународне телекомуникационе уније[267] указује на опасност оваквог приступа.

263 Drakulić M. (1996), op. cit. str. 428-447.

264 Само у октобру 1999. години ФБИ је известио о 800 нерешених случајева, а у 2012. тај број је био 289874;

265 CoE, (2001), Convention on Cybercrime, Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, приступљено 5.2.2014;

266 По подацима од 5. фебруара 2014., Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG, приступљено 5.2.2014;

267 Harley B. (2010), A Global Convention on Cybercrime?, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/, приступљено 5.2.2014;

Интересантно је да је овој Конвенцији претходио нацрт **Међународне конвенције о cyber криминалу и тероризму** (*Proposal for an International Convention on Cyber Crime and Terrorism*) познатом као **Стенфордска конвенција**[268].

Идеја о овој Конвенцији је настала на конференцији која је одржана на универзитету Стенфорд у децембру 1999. години и на којој су учествовали представници владе САД, индустрије, невладиних организација, академских кругова из многих земаља[269]. У свега 22 члана овај нацрт је имао за циљ да укаже да је „cyber криминал транснационалан и захтева транснационални одговор; да cyber криминалци искоришћавају слабости у законима и пракси; да једна држава излаже све друге државе опасности; да брзина и техничка сложеност cyber активности захтева унапред договорене процедуре сарадње у истрази и реакције на претње и нападе; и да би мултилатерална конвенција обезбедила да све државе потписнице донесу законе о опасним активностима cyber криминалаца, да се у спровођењу тих закона могу изручити уколико их гоне стране државе и да је неопходно да се обезбеди сарадња у истрази и пружању доказа за кривично гоњење. Посебна пажња се посвећује заједничком предлагању, усвајању и имплементацији стандарда и праксе које повећавају сигурност и безбедност“[270].

Након доношења Конвенције Савета Европе убрзано се радило на доношењу других аката. Те акривности, а и акти, имају четири правца:

а) акти који су везани за **компјутерски криминал и криминал везан за компјутере** (као и ВТК криминал);
б) акти који су везани за **cyber криминал и тероризам**;
в) акти који посебно регулишу **одређена дела cyber криминала** и
г) акти којима се регулишу питања **cyber безбедности**.

Значи, разлика између овог и претходног периода је у доношењу аката којима се регулише или компјутерски, односно криминал везан за компјутере или *cyber* криминал и што се питањима везаним за *cyber* безбедност посвећује посебна пажња. Субјекти су исти, уз прикључење Комонвелта (*The Commonwealth*), асоцијације Афричких држава (*African Union, Common Market for Eastern and Southern Africa – COMESA*, *Economic Community of West African States - ECOWAS*), Арапске лиге (*League of Arab States*) и Шангајске организација за сарадњу (*Shanghai Cooperation Organization*).

---

268 The Hoover Institution,The Consortium for Research on Information Security and Policy (CRISP), The Center for International Security and Cooperation (CISAC), (2000), Stanford University: A Proposal for an International Convention on Cyber Crime and Terrorism http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm, приступљено 13.12.2013;

269 Sofaer D.A. Goodman E.S. (2000), Proposal for an International Convention on Cyber Crime and Terrorism, A CISAC Report, http://fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a/, приступљено 13.12.2013;

270 Sofaer D.A. Goodman E.S. Cuéllar F.M. Drozdova A.E. Elliott D.D. Grove D.G. Lukasik J.S. Putnam L.T. Wilson D.G. (2000), A Proposal for an International Convention on Cyber Crime and Terrorism, http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf, приступљено 13.12.2013;

Табела 3. Међународни акти везани за компјутерски, односно криминал везан за компјутере и cyber криминал

Компјутерски криминал, одн. криминал везан за компјутере (ВТК)		*Cyber криминал*	
Назив	***Година***	***Назив***	***Година***
The Commonwealth		**Council of Europe**	
Computer and Computer Related Crimes Bill	2002.	Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems	2001.
EU		**African Union, Common Market for Eastern and Southern Africa – COMESA, Economic Community of West African States - ECOWAS**	
Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime	2001.	Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa	2012.
Communication: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000)	2000.	Cybersecurity Draft Model Bill	2011.
		Draft Directive on Fighting Cybercrime within ECOWAS	2009.
League of Arab States		**International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU)**	
Arab Convention on Combating Information Technology Offences	2010.	Model Legislative Texts on Cybercrime/e-Crimes and Electronic Evidence	2010.
		EU	
		Directive on attacks against information systems	2013.
		Joint communication to Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	2013.

Табела 3. Наставак

Компјутерски криминал, одн. криминал везан за компјутере (ВТК)		*Cyber криминал*	
Назив	***Година***	***Назив***	***Година***
League of Arab States		**International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU)**	
		Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'	2013.
		The Stockholm Programme – An open and secure Europe serving and protecting citizens	2011.
		Communication on Delivering an area of freedom, security and justice for Europe's citizens – Action Plan Implementing the Stockholm Programmel	2010.
		Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework	2010.
The Commonwealth		**Council of Europe**	
		Communication on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"	2010.
		Commission Report to the Council Framework Decision on attacks against information systems	2009.
		Communication on Towards a general policy on the fight against cyber crime	2008.
		Council Framework Decision on attacks against information systems	2007.
		Council Framework on attacks against information systems	2005.
		Proposal for a Council Framework Decision on attacks against information systems [COM(2002)	2005.
		Framework Decision combating fraud and counterfeiting of non-cash means of payment	2002.

Када су посебни облици/типови cyber криминала у питању и даље се највише пажње посвећује незаконитом приступу, пресретању, ометању, незаконитим и штетним садржајима, угрожавању приватности и података о личности, cyber преварама и фалсификатима, повредама интелектуалне својине, тероризму, али и новим облицима каква је крађа идентитета, cyber малтретирање, говор мржње, нежељене поруке, завођење[271].

Национална права имају различит приступ дефинисању cyber криминала. Државе су се углавно определиле за неку од следећих варијанти:

а) уношење у **кривични закон** појединачних дела, а њих обично прате допуне кривичних процесних закона[272];
б) **ратификација** Конвенције о cyber криминалу и **аутоматско уношење** у законодавство или усклађивање постојећег кривичног законодавства[273];
в) уношење **казнених одредби** у поједине законе којима се регулишу одређена питања (нпр. Закон о заштити података о личности, Закон о заштити приватности, Закон о ауторском праву)[274];
г) доношење **посебних закона** везаних за законске мере које су значајне за превенцију и борбу против криминала и процесна овлашћења, надлежност, (нпр. о организацији и надлежности државних органа за борбу против високотехнолошког криминала)[275].

У већини земаља прибегава се комбиновању ових решења. У малом броју земаља донет је посебан акт о cyber криминалу, што потврђује констатацију из Студије УН да се **овај термин више користи у међународним него у националним актима**. Међутим, постоје и земље у којима то није тако. То је случај са, нпр. САД у којима је 2011. години предложен **Закон о заштити безбедности од cyber криминала** (*Cyber Crime Protection Security Act, S.2111*)[276], мада му је оригинални назив "*A Bill to enhance punishment for identity theft and other violations of data privacy and security*", а наводи се као Закон о заштити безбедности од cyber криминала, али још није усвојен[277]. У овом акту се дефинишу врсте понашања која представљају овај криминал[278]. Филипини су, такође, донели **Закон о превенцији од cyber криминала** (*Cybercrime Prevention Act of 2012*)[279] у коме су, поред осталог, дефинисани и типови овог криминала као 3 група дела. Прва се односи на: поверљивост,

271 United Nations Office on Drugs and Crime, (2013), op. cit;

272 нпр. Немачка, Финска;

273 нпр. Молдавија, Азарбејџан;

274 нпр. Норвешка, Србија;

275 нпр. Србија;

276 Doyle C. (2013), Cybersecurity: Cyber Crime Protection Security Act (S. 2111, 112th Congress) - A Legal Analysis, http://www.fas.org/sgp/crs/misc/R42403.pdf, приступљено 13.2.2014;

277 Senate of the United States, S. 2111 (112th): Cyber Crime Protection Security Act, https://www.govtrack.us/congress/ bills/112/s2111/text, приступљено 13.2.2014;

278 Petee A.T. Corzine J. Corzine H.L. Clifford J. Weaver G., (2006), Defining "Cyber-Crime": Issues In Determining The Nature And Scope Of Computer-Related Offenses, http://futuresworkinggroup.cos.ucf.edu/docs/Volume%205/PeteeV5.pdf, приступљено 3.11.2013;

279 An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes, http://www.gov.ph/2012/09/12/republic-act-no-10175/, приступљено 24.11.2013;

интегритет и доступност компјутерских података и система: илегални приступ, илегално пресретање, ометање података, системска ометања, злоупотреба уређаја, *cybersquatting*. Друга група је везана за рачунаре: фалсификовање, преваре и крађу идентитета. А трећа група се односи на садржаје: cyber секс, cyber порнографију/дечију, нежељене комерцијалне комуникације, клевете и друго[280].

У неким земљама донети су посебни закони о компјутерском криминалу, нпр. У Малезији[281]и Белгији[282], или о криминалу везаном за информационе технологије, нпр. у Индији[283]. У сваком случају, у већини закона cyber криминал није дефинисан, као ни компјутерски.

Недостатаке регулације cyber простора, услед различитих правних система, културних и друштвених навика и традиција земаља, етничких и других група које се појављују као њени корисници, надокнађују независна невладина тела. Она се појављују као асоцијације, форуми, одбори потрошача, произвођача и дистрибутера информационо-комуникационих производа и услуга, правника и других професиналаца, али и родитеља који успостављају сопствене принципе понашања и функционисања. Независна тела, у жељи да "успоставе ред" и попуне правне празнине, прибегавају саморегулацији. Стварају се „норме" које покушавају да регулишу "нови" простор и коегзистенцију виртуелног и реалног. Тих норми прво се придржавају чланови групе, а касније са повећањем утицаја и подршке од стране других, па и традиционалних полуга власти, она постају опште прихваћене. Међутим, многи, а међу њима и највећи, не укључују се довољно. На пример, становиште *Google-a* је да не би он требало да буде арбитар шта ће се појављивати, а шта не на интернету, сматрајући да је то улога судова и влада.

Саморегулација cyber простора и криминала[284] је настала из 3 кључна разлога[285]: неспремности права да одговори на изазове, непостојања сагласности/консензуса око решења појединих питања и ефикасности у решавању проблема.

У првом случају право често касни за праксом у регулисању одређених појава. То је случај са појединим облицима cyber криминала, каква је нпр. крађа идентитета која се још увек није нашла у већини кривичних закона.

Други случај је када постоје сукоби између два људска права каква су право на приватност и право на слободу изражавања. Многе садржаје везане за приватност тешко је забранити због права појединаца на слободу говора и изражавања. Уз то се поставља питање цензуре одређених садржаја у cyber

280 Philippines, Analysis of the Cybercrime Prevention Act, (2012), http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final_.pdf, приступљено 24.11.2013;

281 Republic of the Philippines, (2012), The Computer Crime Act, (1997), http://cyberlawforyou.blogspot.com/ 2012/09/cyber-crime-laws-in-malaysia.html, приступљено 24.11.2013;

282 Criminal Code on Computer Crime, (2001), http://www.cybercrimelaw.net/Belgium.html, приступљено 24.11.2013;

283 India Ministry Of Law, Justice And Company Affairs, (2000), The Informtion Technology Act, http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf, приступљено 24.11.2013;

284 Hilvert J. (2010), Cybercrime response a win for self-regulation, http://www.itnews.com.au/News/239813, cybercrime-response-a-win-for-self-regulation.aspx, приступљено 24.11.2013;

285 Chawki M. (2005), A Critical Look at the Regulation of Cybercrime A Comparative Analysis with Suggestions for Legal Policy, http://www.droit-tic.com/pdf/chawki4.pdf, приступљено 24.11.2013;

простору који не припадају кривичним делима, али су опасни за одређене категорије „становника“. То је случај са он-лајн игрицама које носе елементе насиља. У Аустралији је, нпр. у јануару 2010. године покренута иницијатива да се класификациони систем оваквих садржаја због застарелости промени кад су у питању компјутерске игрице. Иницијатива је покренута од стране сајта http://www.r18gamesaustralia.com/, на коме је приказано да је 310 игрица класификовано као непогодних за млађе од 15 година (MA15). То значи да нису забрањене већ да деца не могу да их купе без пратње старијих и да родитељи треба да поведу рачуна да ли ће њихово дете играти ту игрицу или не.

Трећи случај настаје из потребе да се одређени проблем хитно реши или да такво решење буде допуна правном. Тако, видео-материјали који садрже сексуалну злоупотребу деце могу бити постављени на интернет у једној земљи, деца-жртве и сексуални предатори живе у другој, веб-сајтови преко којих се дистрибуирају одржавани из треће, у четвртој је регистрован домен, у петој се налази сервер, а они су доступне увек и било где у свету. Само се сталним заједничким напорима влада и других заинтересованих, на међународном и националним нивоима, могу смањити штете које проузрокују ови садржаји. На пример, у Немачкој црну листу веб-адреса заједно састављају Влада и самостално регулационо тело *Freiuilligen Selbstkontrolle Multimedija* (***FSM***). Ако је домаћин илегалног садржаја у Немачкој, налаже му се да га уклони, али ако се садржај хостује изван Немачке, адреса се прослеђује немачким интернет-провајдерима са налогом да им блокирају линкове. Међународну асоцијацију интернет „врућих“ линија *INHOPE* (*International Association of Internet Hotlines*) основала је Европска комисија у оквиру Акционог плана за сигурнији интернет, 1999. године, као одговор на забрињавајући пораст илегалних садржаја на глобалној рачунарској мрежи. *INHOPE* је координатор светске мреже „врућих“ линија. „Вруће” линије су се доказале као прва линија одбране против илегалних он-лајн активности. Преко њих корисници интернета могу пријавити садржаје за које сматрају да су незаконити. Процедура пријаве и поступци по пријему су стандардизовани и транспарентни, а сачињени су у оквиру ове мреже. Анализа пријаве, која је углавном он-лајн преко одговарајућих сајтова, обухвата и проналажење основног домена и сервера са илегалним садржајем. Када се ради о домаћим доменима који имају такве садржаје, они покрећу инцијативу код националних правосудних органа за њихово уклањање и спровођење истраге. У зависности од националних решења захтев за уклањање илегалних садржаја се може упутити и директно, интернет провајдеру код кога је сајт хостован. Међутим, како се у већини случајева он-лајн незаконити садржаји не налазе под доменима који припадају земљи где су пријављени, на њих се не може применити национално законодавство. Другим речима, илегалне интернет активности овог типа су прекогранични проблем и ни једна национална хот-лајн организација им се не може сама супроставити. Да би могле успешно да делују на локалном нивоу, њима су потребни међународни партнери од поверења, са којима ће размењивати искуства, пријаве и извештаје о предузетим акцијама. Пријава која је учињена преко хот-лајн чланице глобалне *INHOPE* мреже биће прослеђена, без одлагања, правосудним органима земље којој припада инкримисани домен. Даља процедура зависи од законодавства те земље[286].

286 Drakulić M. Drakulić R. (2010), Regulacija interneta, op. cit., str. 171-172;

У Француској је Удружење интернет професионалаца *(AFPI)*[287] одлучило да забрани 18 непристојних, педофилских и неонацистичких дискусионих група на серверима. *AFPI*, који има четири члана, али тврди да представља "више од 50%" француског тржишта упозоравао је да су провајдери одговорни за садржаје које преносе.

Оперативна одређења полазе од потребе откривања, гоњења, хапшења, доказивања и кажњавања cyber учиоца. Многи национални али и међународни полицијски и други органи[288] и организације[289] донели су посебна упутства/manuel-е у којим се дефинишу[290]:

а) појмови[291], облици[292] компјутерског, односно криминала везаног за компјутере, интернет криминала, високотехнолошког, cyber[293];
б) процедуре истрага, претреса, заплене, доказивања;
в) облици и начин сарадње, националне и међународне, у гоњењу и изручивању.

При томе су упутства у којима су се дефинисали ови облици криминала у почетку садржала одређење компјутерског криминала, односно криминала везаног за компјутере, да би у следећој фази пажња била усмерена на интернет, а сада на cyber криминал[294]. Посебна пажња се посвећује појединим облицима, највише тероризму и злостављању деце, а тек у скорије време и другим. Тежиште је на форензици и cyber форензици.

---

287 http://www.afpi.org/, приступљено 24.11.2013;

288 Свака повреда кривичног права која укључује познавање компјутерске технологије за припрему, истрагу и пресуђивање, као и а) коришћење комуникационо-информационих мрежа ослобођених географских ограничења и б) циркулацију нематеријалних и нестабилних података, Data Security Concil of India, (2011), Cyber crime Investigation Manuel, http://uppolice.up.nic.in/All%20Rules/Cyber%20crime/4-Cyber_Crime_Investigation_Manual.pdf, приступљено 24.11.2013;

289 ACPO Managers Guide Good Practice and Advice Guide for Managers of e-Crime Investigation, (2008), http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf, приступљено 24.11.2013;

290 Jarrett H.M. Bailie W.M. (2009), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf;

291 Тако се „... cyber претње дефинишу као егзистенцијална претња којом се угрожава само постојање наше земље или знатно мења потенцијал наше нације", Chabinsky R.S., (2010), The Cyber Threat: Who's Doing What to Whom?, Cyber Division Federal Bureau of Investigation http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom, приступљено 24.11.2013;

292 Cyber криминал је један од најбрже растућих облика криминала. Криминалци све више експлоатишу брзину, практичност и анонимност који им модерне технологије нуде за извршење широког спектра криминалних активности. Он укључује нападе на компјутерске податке и системе, крађе идентитета, дистрибуцију слика сексуално злостављане деце, интернет аукцијске преваре, продор у он-лајн финансијске услуге, као и ширење вируса, разне преваре електронске поште, као што је *phishing*. Cybercrime, (2013), http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, приступљено 24.11.2013;

293 Vestbi R.Dž. (2004), Međunarodni vodič za borbu protiv kompjuterskog kriminala, Američka advokatska komora, Komitet za zaštitu privatnosti i borbu protiv kompjuterskog kriminala, Odeljenje za naučno i tehnološko pravo, Beograd;

294 Cyber криминал се развија свакодневно – јављају се нови облици рањивости, нове методе, ново окружење за извршење кривичних дела и нове жртве, Europol, (2013), Strategy & Prevention, https://www.europol.europa.eu/ec3/strategy, приступљено 24.11.2013;

Оперативна одређења изузетно су важна за рад посебних јединица, центара и других институционалних облика у борби против овог криминала[295]. **Европски центар за cyber криминал** (*European Cybercrime Center – EC³*) је нови центар у оквиру Европола[296]. Савет Европске уније донео је 2011. године Приручник за заједничке истражне тимове (*Joint Investigation Teams Manual*)[297], базиран на ***Конвенцији о узајамној помоћи у кривичним стварима*** (*Convention on Mutual Assistance in Criminal Matters - 2000 MLA Convention*).

2.3. Cyber криминал – појам

Требало је да прође низ година од појаве првих облика компјутерског криминала до његовог дефинисања и таман су настале неке сходне дефиниције када се појављује нови феномен – cyber криминал. На размере овог криминала и опасности које носи, између осталог, указало се у документу **Криминал везан за компјутерске мреже** (*Crime related to computer networks*) са Десетог конгреса Уједињених нација посвећеног Превенцији од криминала и третману учинилаца, од априла 2000. године[298]. Радна група експерата под овим криминалом подразумева "**криминал који се односи на било који облик криминала који се може извршавати са компјутерским системима и мрежама, у компјутерским системима и мрежама или против компјутерских система и мрежа**. Криминал се односи на облике понашања која су генерално дефинисана као незаконита, али ће вероватно бити крминализована у кратком временском периоду." У истом документу појављује се и термин cyber криминал, али у контексту категорија и истрага.

Потом почињу да „ничу" разне дефиниције овог криминала. Тако се cyber криминал најшире дефинише **као свака активност у којој су рачунари или мреже средство, циљ или место кривичних активности**[299]. Иако се овој дефиницији

---

295 ASCL Certified Cyber Crime Investigator;

296 European Commission, (2012), Communication on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF, приступљено 24.11.2013;

297 Council of the European Union, (2011), Joint Investigation Teams Manual, https://www.europol.europa.eu/sites/default/files/st15790-re01.en11.pdf, приступљено 24.12.2013;

298 United Nations, (1981), Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, Report of Committee II, Workshop on crimes related to the computer network & Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network,
http://www.uncjin.org/Documents/10thcongress/10cDocumentation/10cdocumentation.html, приступљено 24.12.2013;

299 ITU, (2012), op. cit.; Safety & Security Guide, http://cybercrime.org.za/definition; Prasanna A., Cyber Crimes: Law And Practice, http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf; Taipale K.A., (2009), Unit 01: Overview, What is Cybercrime? http://www.information-retrieval.info/cybercrime/index01.html; Legal and Ethical Aspects, http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-23.pdf; Pfitzmann A., KöhntoppM., (2001), Striking a Balance between Cyber-Crime Prevention and Privacy, http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=40&ved=0CFkQFjAJOB4&url=http%3A%2F%2Fdud.inf.tu-dresden.de%2Fliteratur%2FStriking%2520a%2520Balance%2520betwee.doc

замера што је изузетно широка, она је довољно јасна и обухватна да може да укључи и нове облике, односно нова понашања учнилаца. „То великим делом почива на чињеници да cyber криминал обухвата широк спектар кривичних дела или дела која ће убрзо бити кривична“. За разјашњење сврхе, већина стручњака се слаже да cyber криминал обухвата бар једну од три категорије. **Прво**, компјутер је мета криминалних активности. То укључује случајеве кад учнилац противправно „провали“ у компјутер или компјутерски систем, како би га оштетитио или починио друго кривично дело (нпр. хакерисање, саботажа рачунара). **Друго**, рачунар је средство које се користи или је саставни део извршеног криминала. Ово укључује он-лајн преваре, крађе или проневере. Cyber малтретирање, фалсификовање и ширење дечије порнографије су, такође, cyber криминал. **Треће**, компјутер је само споредан аспект, додатна опрема криминала[300]. Другим речима, сам компјутер није неопходан за чињење криминала/кривичног дела, али је на неки начин повезан“[301].

Са аспекта циљева и намера тај криминал се **везује за незаконите или активности појединаца или група које се сматрају незаконитим и које могу бити спроведене кроз глобалне електронске мреже**"[302].

Овај криминал се објашњава и као „коришћење рачунарске мреже или других система на интернету, напади или злоупотребе система и мрежа у вршењу кривична дела, као и злостављање почињено употребом нових технологија или нових кривичних дела која се стално развијају у cyber простору“[303]. Исти аутор дефинише cyber криминал као **употребу информационо-комуникационе технологије за обављање кривичних, штетних и неморалних радњи у cyber простору**[304].

Такође се cyber криминал дефинише и као „појава штетног понашања која се некако односи на рачунар"[305]. Битно је да су рачунари и информационо-комуникационе технологије утицале на понашање учниоца, односно на њихово девијантно понашање, захваљујући чему се трансформисала и организација криминалних активности.[306]

Поједини аутори[307] дефинишу cyber криминал као **коришћење компјутера за помоћ „традиционалним“ кривичним делима, било у оквиру појединих система или преко глобалних мрежа**. Он, такође, може да укључи криминал који је у потпуности

&ei=fFb_UqSlNoWqyAPv5oCwBw&usg=AFQjCNEGx5ZI7nmzJUlVPZtPwbr8qg0Mng, приступљено 24.11.2013;

300 Finklea K.M. Theohary C.A. (2013), Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, Congressional Research Service, http://www.fas.org/sgp/crs/misc/R42547.pdf, приступљено 24.11.2013;

301 Hale C. (2002), Cybercrime: Facts & Figures Concerning this Global Dilemma, Crime&Justice, September, Vol. 18 – Issue. 65, приступљено 2.11.2013;

302 Yar M. (2005), op. cit.; Thomas D., Loader B., (2000), Cybercrime: law enforcement, security and surveillance at the information age, London, Routledge; Hale C., (2002), op. cit.

303 Bernik I. (2013), op. cit., pp. 11;

304 Bernik I. (2013), op. cit., pp. 11;

305 Wall D.S. (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, pp. 10.

306 Wall D.S. (2005), op. cit;

307 Fafinski S. Dutton W.H. Margetts H. (2010), Mapping and Measuring Cybercrime, OII Forum Discussion Paper No 18, http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf; Simion R., (2010), Cybercrime and its challenges between reality and fiction. Where do we actually stand?, http://www.vittimologia.it/rivista/articolo_simion_2009-03_2010-01.pdf, приступљено 6.12.2013;

подржан технологијом – „трећом генерацијом“ овог криминала. Такав cyber криминал, као што је нпр. спам, искључиво је везан за интернет и не може да постоји без њега. Међутим, многа од дела cyber криминала, која су изазвала забринутост у протеклој деценији, нису нужно криминал у смислу кривичног закона. У суштини, суфикс за "кривично дело" је везан за понашање које не улази лако у границе кривичног закона.“

Постоје и дефиниције које се фокусирају на типологију[308]. Типологија обухвата сваки криминал који се "учинио коришћењем компјутера, мрежа или хардверских уређаја" и обухвата два основна типа: први који је по својој природи више технички и други који је више везан за појединце/учиниоце.

Cyber криминал се може генерално дефинисати и као подкатегорија компјутерског криминала[309]. Наравно да постоје и друге дефиниције[310]. Оно што је битно истаћи је да се приликом дефинисања полази од различитих „објеката“, који једни друге не искључују. Значи, полазишта су:

1) то је такав криминал у коме се **cyber простор** појављује као место извршења, место складиштења доказа и циљ напада, а информационо-комуникационе технологије су оружје и циљ напада. Инфомациона инфраструктутра може бити циљ напада, као и одређени субјекти (државе, организације – јавне, приватне, појединци;
2) то је криминал у коме су **рачунари и/или мреже** средство, циљ или место кривичних активиности;
3) то је криминал код кога се **незаконите активности** спроводе кроз глобане електронске мреже;
4) то је **криминално и штетно понашање**.

Било која дефиниција да се усвоји неспорна је чињеница да је cyber криминал комплексан, чак се сматра кишобран-термином[311] који покрива разноврсне криминалне активности укључујући нападе на компјутерске податке и системе, нападе везане за компјутере, садржаје или својину, нарочито интелектуалну. Он је често транснационалан и по некад организован. У сваком случају то је феномен који има изузетан раст (по броју дела и категорија).

308 Gordon S. Ford R. (2006), On the definition and classification of cybercrime, Journal in Computer Virology, August 2006, Volume 2, Issue 1, pp 13-20, http://link.springer.com/article/10.1007%2Fs11416-006-0015-z#page-1, приступљено 12.11.2013;

309 Shinder L.D. Tittel E. (2002), Cybercrime Scene of the Computer Forensics Handbook, Rockland, Syngress Publishing, Inc. pp. 5;

310 Wall D.S. (2008b), Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime, 22(1) International Review of Law, Computers and Technolog, pp. 45;

311 Finklea K.M. Theohary C.A., (2013), op. cit;

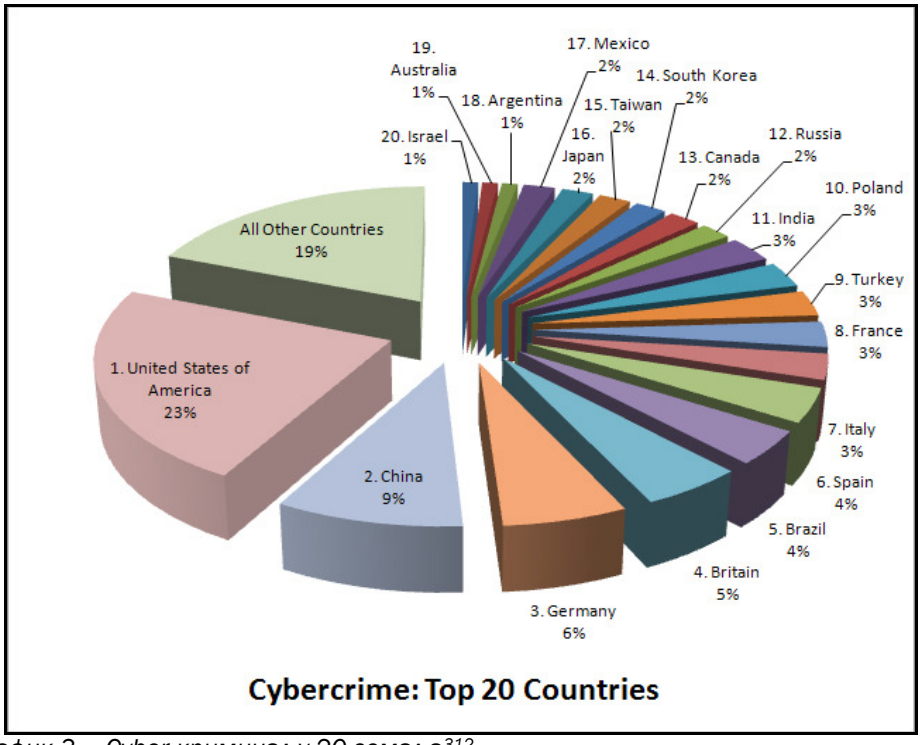


График 3. Cyber криминал у 20 земаља[312]

Иако подаци из разних извора који указују на пораст овог криминала и његову распоређеност по земљама и регионима/континентима нису идентични, јасно је да је то појава у порасту и да захвата развијене као и неразвијене земље, мале и велике, са различитих континената, а зависно од броја корисника информационо- комуникационих мрежа, мобилне телефоније, друштвених мрежа и новоима коришћења *cloud* рачунарства, као и врсте која се прати (нпр. ако се прати хактивизам, cyber криминал, cyber шпијунажа и *cyberspat* заједно).

312 Sumo3000, (2012), Top 20 Countries Found to Have the Most Cybercrime, http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, приступљено 29.1.2014;

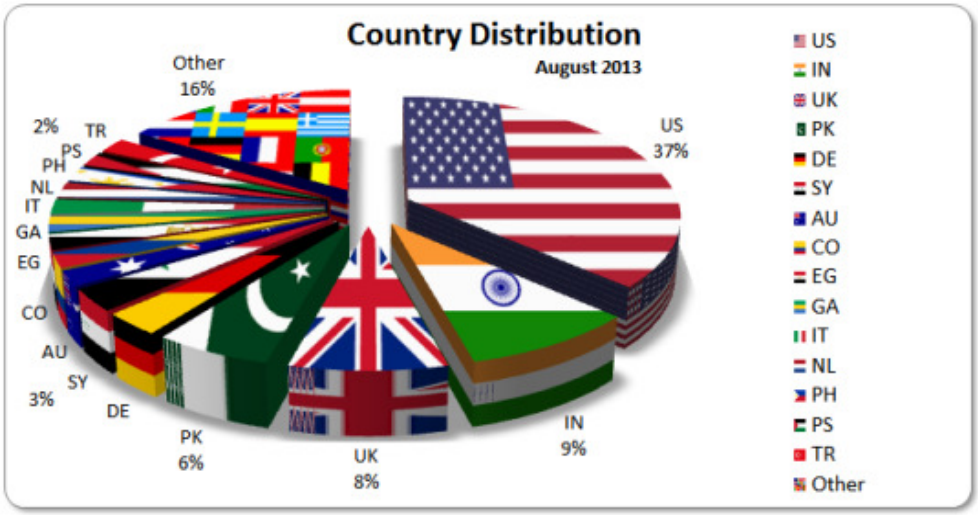


График 4. Дистрибуција cyber криминала по земљама у августу 2013.[313]

Уколико су други облици овог криминала у фокусу интересовања као што је, нпр. ширење компјутерских вируса, уочава се да се оно рапидно повећава и као пандемија захвата огромне просторе. Са аспекта заступљености појединих малициозних веб- сајтова и ширење вируса у ЕУ и Америци јасно је да је то само „мрвица“ у односу на остале земље и остале типове cyber криминала.

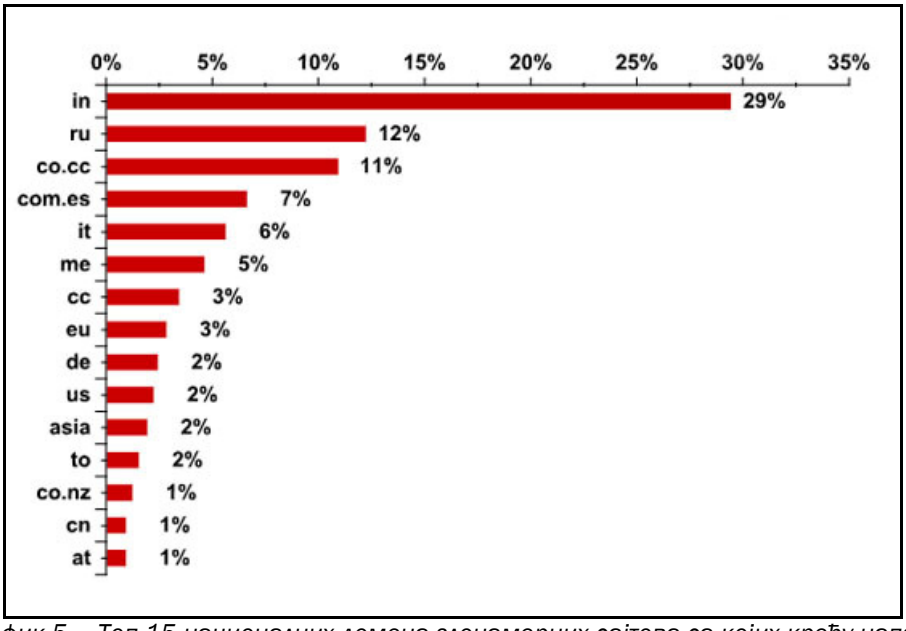


График 5. Топ 15 националних домена злонамерних сајтова са којих крећу напади на северноамеричке и западноевропске кориснике[314]

313 March 2013 Cyber Attacks Statistics, http://hackmageddon.com/2013-cyber-attacks-statistics/#July;

Анализа жртава, нпр. у САД по полу и годинама старости, указује да су мушкарци и жене скоро изједначени, а да је најзаступљенија групација између 40 и 59 година са 43%, иза ње су они између 20 и 30 година са 39%. Млади до 20 и старији од 60 су много мање заступљени, са свега 24%, односно 14%[315]. Дела се мењају зависно од земље.

Значи, cyber простор, односно информационо-комуникационе технологије (које обухватају и компјутерске системе и мреже) појављују се у вишеструкој „улози"[316], односно као:

а) **циљ/мета напада**[317] – нападају се сервиси, функције и садржаји који се на мрежи налазе. Краду се услуге, подаци, идентитет. Оштећују се или уништавају делови или цела мрежа и компјутерски системи или се ометају функције њиховог рада. У сваком случају циљ учнилаца су подаци, својина и/или сам cyber простор, односно мрежа у коју се убацују вируси или црви, обарају сајтови, упадају хакери, вршљају "шуњала", врши се "одбијање услуга"[318]. Преко мреже се долази до података влада, организација, финансијских, здравствених, образовних институција, војске, појединаца и других.

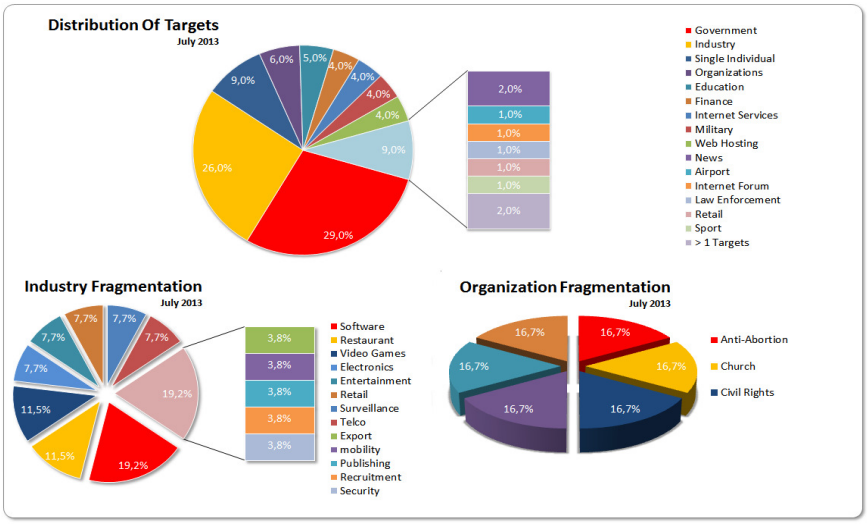


График 6. Дистрибуција по циљевима у 2013. години[319]

---

314 Namestnikov Y. (2012), The geography of cybercrime: Western Europe and North America, http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America?print_mode=1, приступљено 23.1.2014;

315 Internet Crime Complaint Center, (2012), 2012 Internet Crime Report, http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf, приступљено 23.1.2014;

316 Robinson J. (2000), Internet as the Scene of Crime, International Computer Crime Conference, Oslo, www.ccips.org, приступљено 23.1.2014. Drakulić M., Drakulić R. (2005), op. cit;

317 UK Government, (2012), Governments are Prime Targets for Cybercrime, White Paper, http://secunia.com/?action=fetch&filename=governments-are-prime-targets-for-cybercrime.pdf, приступљено 23.11.2013;

318 Drakulić M. Drakulić R. (2005), op.cit;

319 2013 CYBER ATTACKS STATISTICS, HTTP://HACKMAGEDDON.COM/2013-CYBER-ATTACKS-STATISTICS/, ПРИСТУПЉЕНО 23.2.2014;

б) **средство/оружје**[320] – учиниоци од памтивека користе камен, нож, отров, пиштољ и слична оружја, а данас модерни криминалци не "прљају руке" јер користе рачунарску мрежу у чињењу дела и реализовању намера. Некада ова употреба мреже представља потпуно нови алат, док се у другим приликама, већ постојећи, толико усавршава да га је тешко и препознати (чак се спомињу две варијанте: нова дела са новим алатима и стара дела са новим алатима[321]). Коришћење овог оружја нарочито је популарно код дечије порнографије, злоупотреба интелектуалне својине или он-лајн продаје недозвољене робе (дроге, људских органа, деце, невеста, оружја и слично).

в) **место извршења/окружење**[322] у коме се одређено чињење или нечињење реализује[323]. Тако, нпр. пошто су компјутери место извршења кривичног дела, а рачунарске мреже место где настају последице, поставља се питање - како ће се одредити место извршења?[324]. Иако постоје бројне теорије око тога, многа права усвојила су јединство између места извршења и места настанка последица[325], односно места у којем је предузета радња саучесништва[326]. Посебна компликација настаје када се то дешава у оквиру *cloud*[327] и кад су у питању виртуелне личности[328]. Неретко ово окружење[329] служи за прикривање криминалних радњи, као што то веома вешто успевају даураде педофили, а ни други учиниоци нису ништа мање успешни[330]. Зато се и развија cyber форензика[331] која на тако комплексном месту, какав је cyber простор, треба да обезбеди доказе.

---

320 Filshtinskiy S. (2013), Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air?, Communications of the ACM, Vol. 56 No. 6, pp. 28-30;

321 Brenner W.S. (2004), Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law & Technology Association, Vol. 9, No. 13 http://www.vjolt.net, приступљено 23.1.2014;

322 Finklea K.M. Theohary C.A., (2013), op. cit.

323 Иако у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала Републике Србије, члан 2, став 1 стоји: „Високотехнолошки криминал представља вршење кривичних дела код којих се као **објекат** или **средство** извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику";

324 Johnson R.D. Post G.D. (1996), Law and Borders - The Rise of Law in Cyberspace, Stanford Law Review, Vol. 48, pp. 1367, http://ssrn.com/abstract=535, приступљено 4.1.2014;

325 Теорија јединства или теорија *ubikviteta* (на сваком месту, свуда);

326 Јовашевић Д., (2002), Институт саучесништва у кривичном праву, Право – теорија и пракса, вол. 19, бр. 11, стр. 14-26;

327 Fu X. Ling Z. Yu W., Luo J. (2010), Cyber Crime Scene Investigations (C2SI) through Cloud Computing, http://www.cs.uml.edu/~xinwenfu/paper/SPCC10_Fu.pdf, приступљено 4.1.2014;

328 Митровић М.Д. Трајковић С.М. (2011), Може ли виртуелни лик да буде субјект права?, http://anali.ius.bg.ac.rs/A2011-2/Anali%202011-2%20str.%20028-042.pdf, приступљено 4.1.2014;

329 Shinder L.D. Tittel E. (2002), op. cit. приступљено 4.1.2014;

330 Crerar D. (2011), No Hiding Place in Cyberspace: Electronic Discovery from Non-Parties 2011 Updated Version, http://www.blg.com/en/newsandpublications/documents/DAC_Article_-_No_Hiding_Place_in_ Cyberspace_JAN2011.pdf, приступљено 5.1.2014;

331 Denning E.D. Baugh E. W. (1999), Hiding Crimes in Cyberspace, *Information, Communication and Society*, Vol. 2, No 3, http://lotstoread.tripod.com/faqs/hiding.html; Denning E.D., Baugh E. W., (1999), op. cit.; McGuire M., Dowling S., (2013), Cyber crime: A review of the evidence, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf, приступљено 5.1.2014;

Често су поједини аутори додавали и четврту улогу cyber простора, односно информационо-комуникационе технологије као „доказа“, образлажући да се „ ... као што се у класичном криминалу појављује нож, отров, пиштољ или неко друго средство извршења дела, тако се и мрежа и ИКТ могу јавити у доказном поступку за cyber криминал“[332]. Овакво схватање је превазиђено и остало је само као део развоја теорије о cyber криминалу.

Истовремено, cyber простор и мрежа служе за повезивање разних субјеката или су му подршка. Последња улога је везана за застрашивање, обмањивање и уплитање.

Cyber криминалу неспорно је признато „својство” криминала.

Имајући све то у виду може се констатовати да је cyber криминал такав облик криминалног понашања у cyber простору у коме се информационо- комуникационе технологије и системи, првенствено рачунари и рачунарске мреже, појављују као циљ, средство и место извршења кривичног дела. При томе се под cyber простором, подразумева или врста “заједнице” сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова или “простор који креирају компјутерске мреже”. Оно је вештачка творевина која захтева високу техничку опремљеност, добру информациону инфраструктуру који је ничија и свачија својина, у коме паралелно коегзистирају виртуелно и реално и код кога је комуникација колективна. У таквом окружењу изузетно је тешко говорити о националним размерама криминала и друштвеној опасности, бар не у конвенционалном смислу речи. Зато се овај криминал сврстава у најизразитији облик транснационалног криминала против кога ни борба не може бити конвенционална. Поготово што друштвени, социјални и економски контекст овог криминала није истоветан са класичним, транснационалним и организованим[333] криминалом јер за cyber простор важе друга правила – што показује **Глобална студија о организованом криминалу** (*Global studies on organized crime*) Центра за превенцију од међународног криминала и Института Уједињених нација за истраживање интерергионалног криминала[334].

Иако постоје бројне тешкоће у дефинисању, као што постоји и изражена тенденција да му се не признају специфичности, ипак је јасно да такви ставови не могу бити прихватљиви јер се не могу занемарити ни начини реализације овог криминала, као што се ни последице више не мере неколицинама жртава, нити десетинама и хиљадама долара, динара, евра, већ шестоцифреним бројевима. Проблеми настају и због нових елемената за диференцирање овог од других облика криминала.

332 Drakulić M. Drakulić R. (2005), op. cit;

333 Brenner W.S. (2002), Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina Journal Of Law & Technology Volume 4, Issue 1;

334 Centre for International Crime Prevention Office for Drug Control and Crime Prevention United Nations Interregional Crime and Justice Research Institute, (1999), Global studies on organized crime, http://www.uncjin.org/CICP/gsoc_e.pdf, приступљено 4.1.2014;

2.4. Cyber криминал – карактеристике

Cyber криминал је феномен који је:

- константно растући [335];
- транснационалан[336] и организован[337];
- свеобухватан/универзалан[338] - учиниоци и жртве су из разних националних, етничких, верских, расних, политичких група, из разних окружења, социјалног и правног статуса, старосних група; „напади“ су усмерени на све земље и континенте; жртве су из свих друштвених слојева; усмерен је на било ког појединца, организацију, државу[339];
- разноврстан у односу на објекат, субјекат, начин и место извршења[340];
- специфичан у односу на процедуре и принципе откривања, кривичног гоњења, пресуђивања, санкционисања, доказивања[341];

---

335 United Nations, (2010), Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime on its fifth session, http://www.unodc.org/documents/treaties/organized_crime/COP5/CTOC_COP_2010_17/CTOC_COP_2010_17_E.pdf, приступљено 3.1.2014;

336 United Nations Convention against Transnational Organized Crime and the Protocols Thereto, (2000), http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf; The Commission on Crime Prevention and Criminal Justice Resolution 22/7 Strengthening international cooperation to combat cybercrime, (2013), http://www.unodc.org/documents/commissions/CCPCJ_session22/Resolutionsweb/Resolution_22.7.pdf; United Nations, (2010), Twelfth United Nations Congress on Crime Prevention and Criminal Justice Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/ Salvador_Declaration/Salvador_Declaration_E.pdf, приступљено 23.1.2014;

337 Cyber криминал се трансформише у **илегалну индустрију** коју воде организоване криминалне групе међународно умрежене и умножене и које стално траже најновија техничка решења за нова тржишта. *Crimeware* се користи за пословне моделе криминала-као-сервиса (*Crime-as-a-Service*) у којима се користе *crimeware* сервери за организоване нападе, Tropina T., (2014), Cyber Crime and Organized Crime, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=305:cyber-crime-and-organized-crime&catid=50:issue-7&Itemid=187; Cevidalli A., (2010), Leveraging The Multi-Disciplinary Approach to Countering Organised Crime, http://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-06.pdf; Europol, Socta 2013 EU Serious and Organised Crime, Threat Assessment, https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf, приступљено 4.1.2014;

338 Vogel J. (2007), Towards a Global Convention against Cybercrime, First World Conference of Penal Law. Penal Law IN THE XXIst century. Guadalajara (Mexico), 18-23 November 2007, http://www.penal.org/IMG/Guadalajara-Vogel.pdf, приступљено 5.1.2014;

339 Mwaita P. Owo M. (2013), Workshop Report on Effective Cybercrime Legislation in Eastern Africa Dar Es Salaam, Tanzania, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/ 2571_EastAfrica_WS_Report.pdf, приступљено 4.2.2014;

340 Cevidalli A. Austenf J. (2010), The Challenge of Combating Online Organised Crime – A Multi-Disciplinary Perspective, http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Cevidalli_2010. pdf; Ghosh S. Turrini E. editors, (2010), Cybercrimes: A Multidisciplinary Analysis, http://f3.tiera.ru/2/Cs_Computer%20science/Ghosh%20S.,%20Turrini%20E.%20(eds.)%20Cybercrimes..%20A%20multidisciplinary%20analysis%20(Springer,%202010)(ISBN%203642135463)(O)(435s)_Cs_.pdf, приступљено 23.1.2014;

341 McGuire M. (2013), Cyber crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf, приступљено 23.1.2014;

- тренутан (1/24/7/365) и безграничан - у односу на време и место извршења[342];
- непоштедљив - ни једна жртва није „света“[343], ни један учнилац није недодирљив[344];
- променљив/транзитиван[345]/флексибилан[346] - стална промена начина извршења[347] и борбе против њега;
- доступан[348] сваком ко има одређена знања[349] и приступ рачунарима и рачунарским мрежама[350];
- вишеструко утицајан (друштвени, економски, политички, психолошки[351], еколошки)[352];

---

342 Parker B.D. (1989), Computer Crime Criminal Justice Resource Manual, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf; Chik B.W., Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore, www2.law.ed.ac.uk/ahrc/complaw/docs/chik.doc, приступљено 21.12.2014;

343 Secretary General of the Council of Europe, (2008), Internet - a critical resource for all, http://www.coe.int/t/informationsociety/documents/SG-Inf(2008)14_en.pdf; Council of Europe, (2011), Internet Governance - Developing the future together, http://www.un.org/en/sc/ctc/specialmeetings/ 2011/docs/coe/coe-hInf_2011_4.pdf; у једној фази хакери су у оквиру свог кодекса имали и посебна правила везана за одређене категорије субјеката које не би требали да угрожавају, односно „упадају у системе болница или неких хуманитарних, нпр. дечијих, институција“; Drakulić M., Drakulić R., (1996), Hakerska etika u kontekstu profesionalne etike informatičara, Zbornik radova: II naučni skup, Tehnologija, razvoj i kultura, Herceg Novi, 1996. str. 136 – 153; Burgard A., Schlembach C., (2013), Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet, International Journal of Cyber Criminology (IJCC), July – December 2013, Vol 7 (2): 112–124, http://www.cybercrimejournal.com/burgardschlembachijcc2013vol7issue2.pdf, приступљено 19.3.2014;

344 Chon S. Broadhurst R. Routine Activity Theory and Cybercrime: What about Offender Resources, http://ssrn.com/abstract=2379201, приступљено 21.1.2014;

345 Wilson C. (2008), Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, http://www.dtic.mil/dtic/tr/fulltext/u2/a477642.pdf; развија се и посебна теорија „Space Transition Theory“ којом се објашњава природа понашања особа у физичком и cyber простору, Jaishankar K., (2008). Space Transition Theory of cyber crimes. In Schmallager F., Pittaro M. (Eds.), Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall, pp.283-301, приступљено 11.1.2014;

346 Team Cymru, (2006), Cybercrime—An Epidemic Can we protect ourselves from the hazards of an online world, http://queue.acm.org/detail.cfm?id=118019;

347 Fafinski S., Dutton H.W., Margetts H., (2010), op.cit.

348 Gu L. (2013), Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf, приступљено 23.2.2014;

349 Ако се погледа однос стучне спреме и осуђиваности учинилаца дела cyber криминала у Републици Србији, највише их је са средњом стручном спремом (60,6%), па са високом (18,7%), али има и оних који немају никакву школу (1,9%), са основном школом (12,9%), или имају докторат (2,6%), Настић Д. (2012), Профил сајбер криминалаца у Србији, мастер рад, Београд, ФОН; Hargeaves C. Prince D., (2013), Understuding Cyber Criminals and Measuring Thair Future Activities, Developing Cyber crime Research, http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf, приступљено 20.2.2014.; Robert W., Mikko S., (2009), Overcoming the insider: reducing employee crime through Situational Crime Prevention. Communications of the ACM, 52 (9). pp. 133-137;

350 Ngo T.F. Paternoster R. (2011), Cybercrime Victimization: An Examination of Individual and Situational Level Factors, International Journal of Cyber Criminology, Vol 5 Issue 1 January - July 2011, http://www.cybercrimejournal.com/ngo2011ijcc.pdf, приступљено 20.2.2014;

- није мит већ реалност[353];
- мултидисциплинаран[354];
- комплексан[355]/софистициран[356]/камуфлиран[357] - по месту и начину извршења, времену, понашању, истрази, последицама, доказима, окружењу, објекту, алатима, субјектима, бићу дела.
- посебног *modus operandi.*

---

351 Morag N. (2013), Keyboard Criminals: How Cybercrime Has Grown Up and Diversified, http://www.coloradotech.edu/resources/blogs/october-2013/keyboard-criminals, приступљено 20.2.2014;

352 Khadam N. (2012), Insight to Cybercrime, http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf, приступљено 20.2.2014;

353 Schneier B. (2014), Cyberwar: Myth or Reality?, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=315:cyberwar-myth-or-reality&catid=50:issue-7&Itemid=187, приступљено 23.4.2014;

354 Ghernaouti-Hélie S. (2004), Increase trust and confidence in information and communication technologies by a multidisciplinary approach, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.198.3785&rep=rep1&type=pdf, приступљено 23.1.2014.; Ghosh S., Turrini E., editors, (2010), op. cit.

355 Bednar M.P. Katos V. Hennell C. (2009), On the Complexity of Collaborative Cyber Crime Investigations, Digital Evidence and Electronic Signature Law Review, Vol 6, *journals.sas.ac.uk/deeslr/article/download/1894/1831*; Porteous H., Valiquet D., *(2011),* Cybersecurity and Cybercrime: Dealing with a Complex Threat, http://www.parl.gc.ca/content/lop/researchpublications/cei-06-e.htm, приступљено 23.1.2014;

356 Bailey J. (2011), The Increasing Sophistication of Cybercriminals: Techonomy's "Insecurity" Panel, http://www.forbes.com/sites/techonomy/2011/11/15/the-increasing-sophistication-of-cybercriminals-techonomys-insecurity-panel/; The Current State of Cybercrime 2013, An Inside Look at the Changing Threat Landscape, (2013), http://www.emc.com/collate, Morcroft G., (2014), Markets/Finance Cyber Criminals Are Getting More Sophisticated, So Watch Out For These New Scams In 2014, http://www.ibtimes.com/cyber-criminals-are-getting-more-sophisticated-so-watch-out-these-new-scams-2014-1472504, приступљено 22.2.2014;

357 Byrne N. (2008), Camouflage attacks now standard for cyber-criminals, http://www.siliconrepublic.com/enterprise/item/9839-camouflage-attacks-now-stan; 2013 Cyber Threat Landscape Review, (2014), http://www.sunsoftonline.com/wp/?p=2606; Duhaime J.C., Europol issues organized crime threat assessment focusing on cybercrime, hacking, money laundering and drugs, http://www.duhaimelaw.com/2013/03/21/europol-issues-organized-crime-threat-assessment-focusing-on-cybercrime-hacking-money-laundering-and-drugs/, приступљено 23.3.2014;

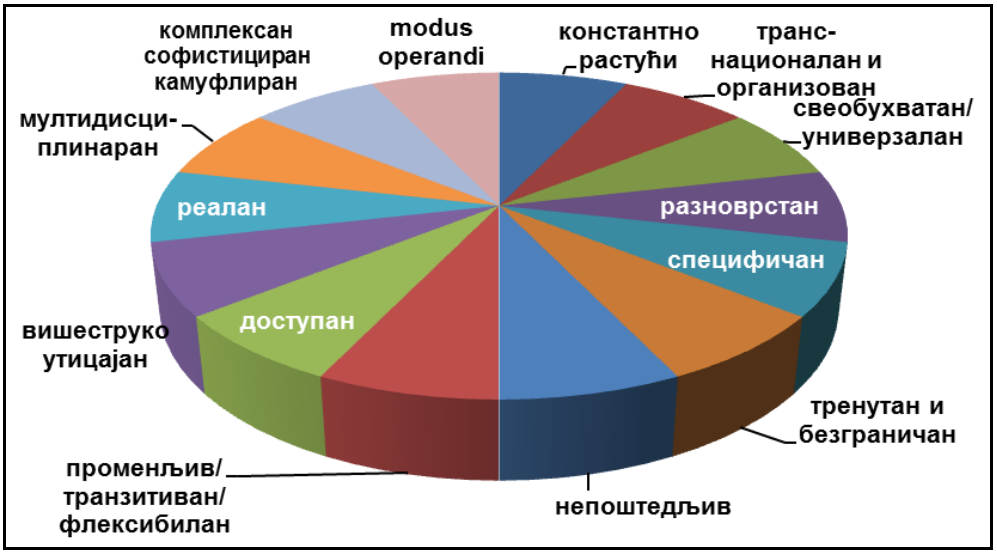


График 7. Карактеристике cyber криминала

Да би се утврдио *modus operandi* учинилаца cyber криминала, анализира се начин понашања[358], односно[359] како је и да ли је: **а)** била предузета припрема; **б)** које су биле методе извршења дела, **в)** колико је било учнилаца, односно осумњичених и **г)** одакле су „оперисали".

а) У анализи cyber криминала**,** као и било ког другог криминала, утврђује се да ли је постојала и каква **припрема** јер то треба до доведе до сазнања да ли су у питању дела са умишљајем. Дуго је постајало мишљење да припрема није карактеристична за овај тип учнилаца, већ да они реагују моментално на указану прилику. Међутим, све је присутније да се учиниоци cyber криминала опсежно и систематски припремају[360], као и истражитељи[361]. Припрема се састоји од: избора жртве[362] (нарочито је то

358 Обично се прати " шта учинилац ради да би остварио дело/криминал и садржи елементе који укључују: 1) како обезбедити успех, 2) како се штити идентитет, и 3) како ефекасно побећи. Од 1890. детективи Scotland Yard почињу да праве *modus operandi* фајлове како би могли препознати навике криминалаца одређених округа. За хакинг прате се три кључне ставке: 1) социјални инжењеринг, 2) бруталност, и 3) технике упада; O'Connor T., (2014), Modus Operandi of Hacking, Mega Links in Criminal Justice, http://www.drtomoconnor.com/3100/3100lect04.htm, приступљено 19.4.2014;

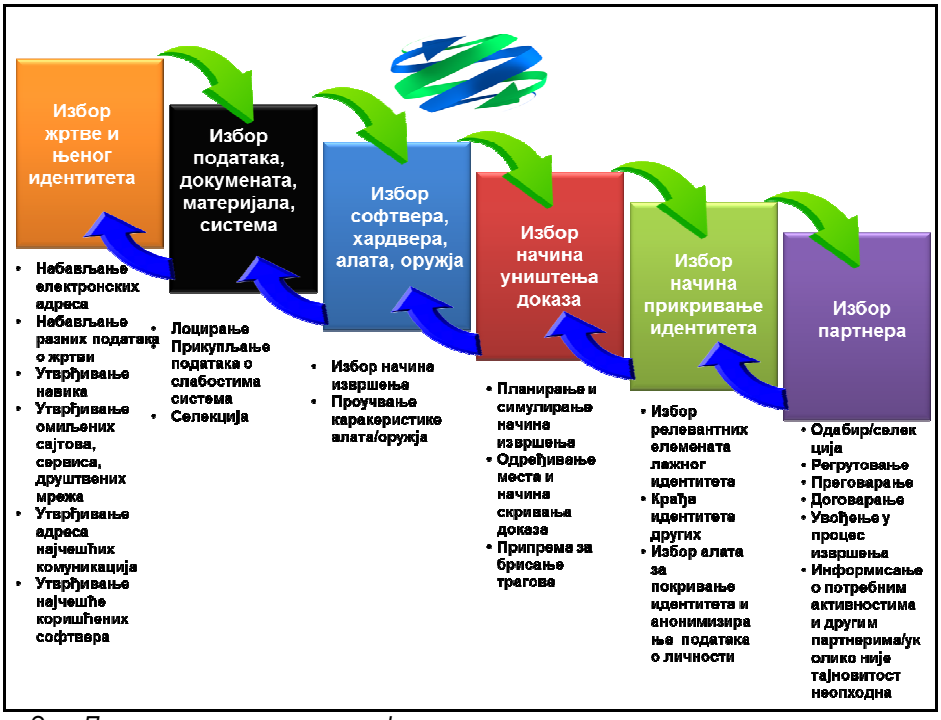
359 Veenstra S. Stol W. Leukfeldt R. (2013), High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands, International Journal of Cyber Criminology, Vol 7 Issue 1 January - June 2013., 2013 International Journal of Cyber Criminology. January – June 2013, Vol 7 (1), pp. 1–1;

360 Turvey E.B. (2011), Modus operandi, Motive and Technology, in edition, Digital Evidence and Computer Crime, Forensics Science, Computers and Internet, Amsterdam, Elsevir, pp. 285 – 304;

361 Aseef N. Davis P. Mittal M. Sedky K. Tolba A. (2005), White Paper: Cyber-Criminal Activity and Analysis, http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf, приступљено 2.4.2014;

362 Hargeaves C. Prince D. (2013), op. cit;

присутно нпр. код педофила[363]); набављања електронских адреса и других података везаних за жртву; прикупљања података о слабостима система; лоцирања материјала, докумената, података до којих се жели допрети[364]; избора начина извршења; избора софтвера, хардвера и других техничко-технолошких алата и оружја; избора начина уништења доказа; избора начина прикривања и покривања идентитета; избора партнера (саучесника).



Слика 2. Припремне активности cyber криминала

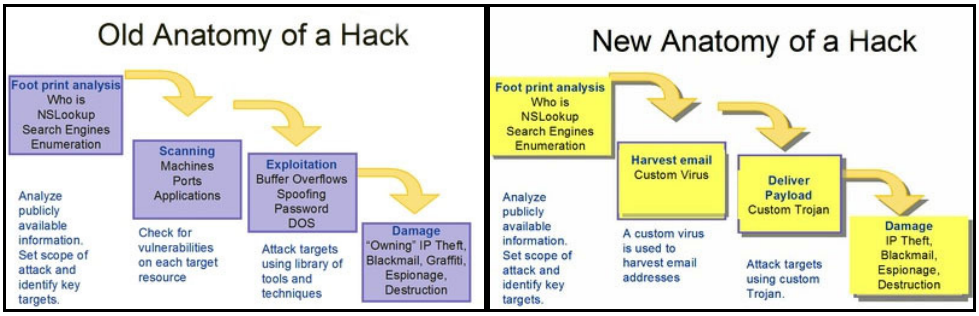
Избор жртве, односно циља, зависи од мотива учниоца и степена рањивости система. Најефикаснији начин је скенирање рањивости јер сви (држава, организација, група, појединац) презентују јавности своје услуге, а оне би могле бити канал за напад. *Graham Ingram*, генерални директор аустралијске организације за рано упозорење на cyber криминал, упозорио је на *AusCERT* конференцији да претње за појединце расту "скоро експоненцијално" и да је власт изгубила борбу[365].

363 Niveau G. (2010), Cyber-pedocriminality: Characteristics of a sample of internet child pornography offenders, http://www.drlynepiche.com/uploads/photos/pedo%20and%20internet.pdf, приступљено 12.1.2014;

364 Lickiewicz J. (2011), Cyber crime psychology – proposal ofan offender psychological profil, Problems of Forensic Sciences 2011, vol. LXXXVII, 239–252, http://www.forensicscience.pl/component/option, com_jbook/task,view/Itemid,2/catid,72/id,664/lang,en/, приступљено 23.1.2014;

365 Gray P. (2005), Beware the crime lords of the internet, http://www.smh.com.au/news/Next/Beware-the-crime-lords-of-the-internet/2005/05/30/1117305534401.html, приступљено 23.1.2014;

б) Учиниоци cyber криминала користе посебне алате, вештине и знања за чињење кривичних дела[366]. **Методологија** извршења дела cyber криминала се стално усавршава[367]. Према *Stiennon*[368] „хакери су пронашли начине да унапреде ефикасност своје класичне методологије или „кувара“. Конкретно, најновији развој је употреба вируса и тројанаца као део *modus operandi*“. Ако би се посматрала „анатомија“ припреме хакинга[369] она би била следећа:



Слика 3. Припрема хакерске активности

Проучавање методологије извршења дела двоструко је значајно: за профилисање учиоца и профилисање жртава. Ипак, методе доживљавају модификације, постају комплексније и софистираније[370]. То се, као бумеранг вратило у неопходности јачања безбедности[371] свих података **и информација.**

в) Број учнилаца (и сарадника) и осумњичених је карактеристика овог криминала. Иако нека истраживања, нпр. у Холандији, Србији, указују да су појединци најмасовнија категорија[372], најопаснија[373] и најатрактивнија

366 Veenstra S. Stol W. Leukfeldt R. (2013), op.cit., „ ... у 61,9% хакерских случајева осумњичени су користили разне криминалне технике, док је у 69,8% предмета постојала информација о коришћењу кривичних техника, али није јасно којих. Пример: корисничко име и лозинка жртве су коришћени да се „пробије“ у систем, али се не зна како се до њих дошло. За мањи број случајава се знало које су технике биле у питању. Најчешћа техника је *defacing* сајтова (61,5%). Већина *defacing je* неовлашћено укључена у модификацију личних страница на сајтовима за друштвене мреже (за убацивање клеветнички слика или текстова на нечији налог)“;

367 Esquibel E.J. Laurenzano A.M. Xiao J.J. Zuvich T. (2005), Cyber Criminal Activity: Methods and Motivations;

368 Парафразирајући O'Connor T. (2014), op. cit. који наводи Stiennon R. (2012), UP and to the RIGHT: Strategy and Tactics of Analyst Influence: A complete guide to analyst influence, IT-Harvest Press, Birmingham;

369 O'Connor T. (2014), op.cit;

370 The Belgian Cybercrime Centre of Excellence for Training, Research and Education, (2012), Cybercrime: modern crime, modern methods, http://www.kuleuven.be/english/news/cybercrime.html, приступљено 22.1.2014;

371 ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE and ISACA Belgium, (2013), Belgian Cyber Security Guide, Protect Your Information, https://www.b-ccentre.be/wp-content/uploads/2013/11/ BCSG.pdf, приступљено 22.1.2014;

372 Veenstra S. Stol W. Leukfeldt R. (2013), op. cit. „У већини случајева су били појединци. У неколико случајева је било двоје, а у малом броју више од двоје. Утврђено да је више од једног осумњиченог не значи да су у питању познаници или сарадници. Већина случајева не укључује организовани

је категорија организованог криминала. Она је нарочито везана за групу кривичних дела против безбедности рачунарских података, али и за одређена дела против полних слобода, као што је злоупотребе деце[374], дечија порнографија и материјали експлоатације деце (каква је Операција Армагедон[375]), педофилија, секс-туризам, продаја невеста. Њих следе *spam* и *phishing*, као и производња и дистрибуција вирусоликих рачунарских програма. По *McGuire,* односно *BAE Systems Detica* извештају[376] половина овог криминала чине групе састављене од 6 или више чланова, а једна четвртина има више од 10 чланова. Такође, једна четвртина cyber криминалних група је деловала мање од 6 месеци. По структури постоје 3 основна типа организовних група, са субгрупама, cyber криминалаца: у првој су оне чији су циљеви и деловање искључиво он-лајн и углавном су виртуелне, а могу бити ројеви (*swarms*) или чворови (*hubs*). Друга група обухвата комбинацију он-лајн и оф-лајн деловања и може бити хибридна груписана (*clustered hybrids*) или хибридна проширена (*extended hybrids*). Трећа група углавном делује оф-лајн, али користи интернет технологију да олакша своје активности. Појављује се као агрегати (*aggregates*) или хијерархија (*hierarchies*). У сваком случају, деловање cyber група је изузетно присутно[377] и често подржано од националних влада (какав је био случај са „државним" хакерима у Србији за време НАТО бомбардовања[378]).

г) **Локација** је четврта битна компонента *modus operandi*. Иако имају изванредне могућности да лако и безбедно прелазе границе учиниоци

криминал или осумњичене који „раде" заједно. Понекад су организоване групе укључене у хаковање и е-преваре. У 4,6% хакерских случајева осумњичени су били део криминалне групе који се међусобно познају и раде заједно. Студија случаја показује да је хакерисање дело које се обично чини изван организованих криминалних група. Још мање, само у 2,2% случајева, дела е-преваре било је извршено од стране организованих група. Пример је група осумњичених која је варала људе помоћу лажне компаније за продају и која никад није испоручила робу. Постоје и примери превара у којима је жртвама речено да су освојили луксузно крстарење и само је требало платити депозит. Е-превара је слична хакерисању и већину дела нису починиле организоване групе";

373 Broadhurst R. Grabosky P. Alazab M. Bouhours B. Chon S. Da C. (2013), Crime in Cyberspace: Offenders and the Role of Organized Crime Groups, http://ssrn.com/abstract=2211842, приступљено 3.1.2014;

374 Drakulić, M. Drakulić, R. (1999), Deca i zloupotreba interneta, Beograd, Jugoslovenski komitet pravnika za ljudska prava, стр. 7-15:

375 Ова операција траје већ више година и на „удару" су лица за кривично дело приказивања, прибављања и поседовања порнографских материјала и искоришћавања малолетног лица за порнографију. До сада је ухапшено више лице из разних крајева Србије;

376 McGuire M. (2012), Organised Crime in the Digital Age, London: John Grieve Centre for Policing and Security, https://www.baesystemsdetica.com/news/organised-crime-in-the-digital-age/; или Detica, (2012), Organised Crime in the Digital Age: The Real Picture, Executive Summary of BAE Systems Detica and the John Grieve Centre for Policing and Community Safety 'Organized Crime in the Digital Age' research report, http://www.baesystemsdetica.com/uploads/resources/ORGANISED_ CRIME _IN _THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf, приступљено 3.1.2014;

377 Типични примери су: Carberp, Unlimited Operation, Koobface, али се појављују и групе подржане од влада: PLA Unit 61398, Operation Olympic Games;

378 Drakulic M. Drakulic R. (1999), Balkan Hackers War in Cyberspace, BILETA, CYBERSPACE 1999: Crime, Criminal Justice and the Internet", http://www.bileta.ac.uk/content/files/conference%20 papers/1999/Balkan%20Hackers%20War%20in%20Cyberspace.pdf, приступљено 3.1.2014;

cyber криминала су често орјентисани на сопствену земљу и локалну заједницу. По подацима из Холандије[379] већина осумњичених су из Холандије, а само по неко је из иностранства: 23,4% хакера и 14,5% код е-превара. Чак и код сексуалне експоатације деце домаћи учиниоци имају велико учешће. Тако по подацима ФБИ, нпр. тродневна Операција *Cross Country* била је фокусирана на малолетне жртве проституције (око 105 сексуално експлоатисане деце) и 150 макроа и других појединаца. Акција се синхронизовано одвијала у 76 градова и спроведена је од стране ФБИ заједно са локалним, државним и федералним агенцијама за спровођење посебног закона и Националног центра за несталу и злостављану децу[380].
У Србији подаци за 2012. годину показују да је највећи број осуђених cyber криминалаца из Београда (44,4%), али их има и из Босне и Херцеговине (1,9%) и са Косова и Метохије (0,6%)[381]. Ипак, свих 10 најтраженијих cyber криминалаца од стране ФБИ, за дела почињена у САД (прање новца, банкарске преваре, пасошке преваре и крађе идентитета у септембру 2010) јесу странци и то: по 2 из Литваније, Руске федерације и Пакистана, а по један из Индије, Ел Салвадора, Шведске и Сирије[382].
Њима треба додати и податке са којих локација крећу различити cyber напади.
Што се других напада тиче они највише долазе из Кине (35%), затим Индонезије, САД-а, Тајвана, Русије, Бразила, Индије, Румуније, Јужне Кореје и Венецуеле[383].

379 Veenstra S. Stol W. Leukfeldt R. (2013), op. cit.

380 FBI, (2013), Operation Cross Country Recovering Victims of Child Sex Trafficking, http://www.fbi.gov/news/stories/2013/july/operation-cross-country-recovering-victims-of-child-sex-trafficking, приступљено 25.2.2014;

381 Настић Д. (2012), op. cit. стр. 72;

382 FBI, (2014), Cyber's Most Wanted, http://www.fbi.gov/wanted/cyber, приступљено 4.4.2014;

383 Percentage of global internet attack traffic during 3rd quarter 2013, by originating country, (2013), http://www.statista.com/statistics/276425/internet-attack-traffic-by-originating-country/, приступљено 22.2.2014;

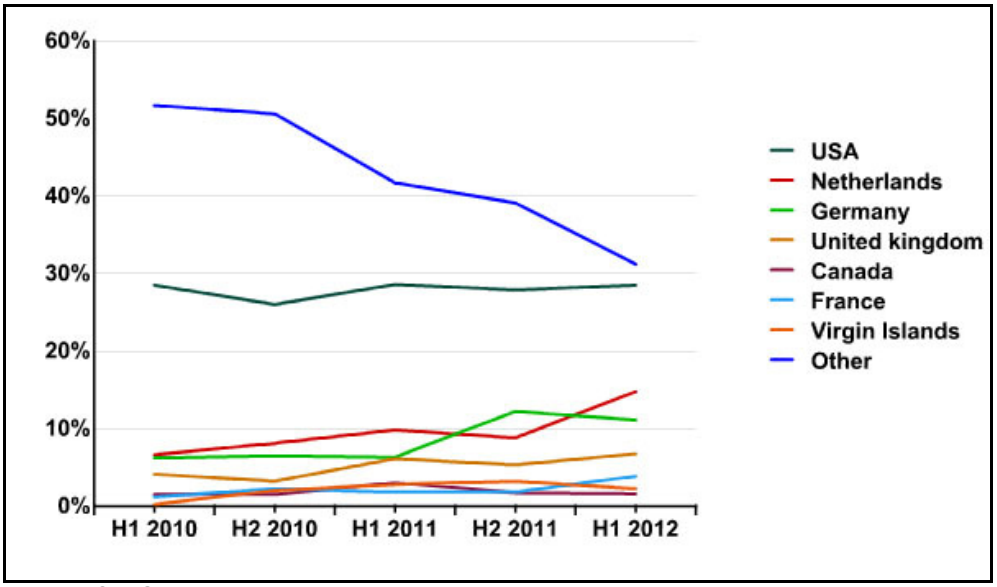


График 8. Земље са чијих сервера се највише „испоручује“ малициозних рачунарских програма[384]

2.5. Облици cyber криминала

Као што још увек не постоји јединственост у томе шта је cyber криминал, тако не постоји ни усаглашеност око тога која дела и понашања треба третирати као дела овог криминала. Међу ауторима и докментима, који се све више баве овом појавом, углавном се могу наћи две групе схватања: једни полазе од **општег појма** cyber криминала и сва дела која имају својства особена овој појави, појму, укључују у њега, док други примењују **метод (позитивне) енумерације** и набрајају дела која се под cyber криминалом подразумевају[385].

У прву групу спада класификација cyber криминала која се нашла у материјалу за “радионицу” о криминалу на мрежи Десетог конгреса УН, у коме се констатује да постоје две субкатегорије[386]:

а) **cyber криминал у ужем смислу** - као свако незаконито понашање усмерено на електронске операције сигурности компјутерских система и података који се у њима обрађују;

б) **cyber криминал у ширем смислу** - као свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминал какво је незаконито поседовање, нуђење и дистрибуирање информација преко компјутерских система и мрежа.

---

384 The geography of cybercrime: Western Europe and North America, (2013), http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America, приступљено 22.4.2014;

385 Дракулић М. (1996), op. cit. стр. 427, на исти начин се класификује и компјутерски криминал;

386 United Nations, (1981), op. cit.

У истом документу наводе се и конкретни облици овог криминала у складу са Препоруком Савета Европе и листом ОЕЦД-а из 1989, односно 1985. године:

1) неауторизовани приступ компјутерском систему или мрежи, кршењем мера сигурности (хакинг);
2) оштећење компјутерских података или програма;
3) компјутерска саботажа;
4) неовлашћено пресретање комуникација од и у компјутерским системима и мрежама и
5) компјутерска шпијунажа.

Сваки од ових облика може се укрштати са сваким јер готово да не постоји "чисти" облик. Тако хакинг, поред неовлашћеног уласка у компјутерске системе и мреже, често обухвата и уништење података или компјутерску шпијунажу (као што је то случај са упадима на веб-сајтове и уништење или "преправљање" података на њима или хакинг и трговина пасвордима). Измена компјутерских података и програма укључује и "лансирање" компјутерских црва и вируса што је најчешће праћено заустављањем рада компјутерског система и уништењем података. У мрежама црви и вируси се у већини случајева "размењују" електронском поштом, а неретко то чине и хакери прликом неовлашћеног приступа.

Од дела cyber криминала у ширем смислу најчешће се појављују:

1) компјутерски фалсификат;
2) компјутерска крађа;
3) техничка манипулација уређајима или електронским компонентама уређаја;
4) злоупотреба система плаћања као што је манипулација и крађа електронских кредитних картица или коришћење лажних шифара у незаконитим финансијским трансакцијама.

Њима се у новије време додају и дела подржана рачунарима. Ова дела обухватају "растурање" материјала или само њихово поседовање при чему се мрежа користи за постизање бољих резултата криминала или покушаја избегавање правде. У ова дела се убрајају разни незаконити и штетни садржаји, кршење ауторских и сродних права, продаја забрањене робе (оружја, крадене робе, лекова) или пружање недозвољених услуга (коцкање, проституција). Највише пажње у овој групи дела привлачи дечија порнографија и дистрибуција разних материјала интернетом[387].

Много је већа група аутора и докумената која полази од енумерације, при чему се дела или само набрајају/ређају или се класификују (групишу) по одређеним критеријумима.

387 United Nations, (1981), op, cit;

Од најједноставнијег набрајања полази Аустралијски институт за криминологију[388] по коме постоји 9 типова cyber криминала[389]:

а) крађа телекомуникационих услуга;
б) комуникација у циљу остварења кривичних завера;
в) телекомуникациона пиратерија;
г) ширење увредљивих материјала;
д) електронско прање новца и утаја пореза;
ђ) електронски вандализам, тероризам и изнуда;
е) преварне продаје и инвестиције;
ж) илегално пресретање телекомуникација;
з) преварни електронски трансфер средстава.

У Енциклопедији cyber криминала наводи се да ФБИ и Национални центар за криминал белих крагни САД (*National White Collar Crime Center*) откривају и прате следеће облике:

а) упаде у компјутерске мреже;
б) индустријску шпијунажу;
в) дечију порнографију;
г) бомбардовање електронском поштом;
д) "њушкање" пасворда;
ђ) софтверску пиратерију;
е) "прерушавање" једног рачунара да електронски "личи" на други како би се могло приступити систему који је под рестрикцијама и
ж) крађу кредитних картица.

Касније, у новој Енциклопедији cyber криминала[390] се наводи да постоји много врста cyber криминала и злоупотреба информационих система, укључујући и:

а) несавесно коришћење информационих система, кршење политике или праксе безбедности и тиме излагање система и података cyber нападима;
б) конвенционалан криминал који користи рачунаре или друге врсте електронских и других уређаја за информационо-технолошке комуникације као подршке незаконитих активности;
в) он-лајн преваре као што су *phishing, spoofing, spimming* или на други начин обмањивање људи на мрежи за финансијску добит, као и преваре са кредитним картицама и крађом идентитета;
г) неовлашћени упад у рачунаре и информационе системе, уз откривање лозинки ради провале у системе и мрежне и/или оф-лајн злочине;
д) злонамерно писање и дистрибуцију рачунарских кодова који подразумевају креирање, копирање, ширење *malware* (деструктивни вируси, тројанци, црви или *adware/spyware* програми);
е) дигиталну пиратерију музике, филмова, и/или софтвера посебно преко *peer-to-peer* мрежа;

388 Australian Institute of Criminology, (1999), 9 Types of Cyber Crime, http://www.aic.gov.au/crime_types/cybercrime/definitions.html, приступљено 12.11.2013;

389 У оквиру којих су објашњења и навођење примера;

390 McQuade C.S. III, (2009), Encyclopedia of Cybercrime, London, Greenwood Press, pp. 44;

ж) cyber малтретирање, претње, намерно срамоћење или принуду, као и cyber шиканирање;
з) он-лајн ухођење и друге увредљиве cyber понуде, нпр. сексуалне, заједно са слањем нежељених слика или текстова сексуалне природе, промовисање секс- туризма, или коришћење интернета за олакшавање трговине људима у сексуалне или друге сврхе;
и) академске преваре и научне злоупотребе од стране ученика, студената, наставника, професора као плагирање (крађа идеја и текстова), варање на испитима или лажирање методе истраживања или резултата;
ј) организовани криминал коришћењем интернета од стране етничких група за олакшавање комбинација илегалних и легалних активности, као што су кријумчарење и продаја људи, оружја, дроге;
к) владино шпијунирање, корпоративну шпијунажу која обухвата незакониту употребу шпијунских и *key logger* софтвера за откривање података који могу бити украдени или коришћени за извршење додатног криминала;
л) cyber тероризам када се покушава испуњење „социјалних, верских или политичких циљева изазивањем страха или оштећењем или ремећењем критичне информационе инфраструктуре“.

Оваквом начину класификовања се замера непостојање основе за увођење нових облика. Сликовито се може навести схватање изнесено у документу *The Future Challenges of Cybercrime*[391] у коме се констатује да „упркос специфичне идентификације кривичних дела, правна дефиниција cyber криминала има тенденцију да буде „велики списак“ и не предвиђа будуће варијације cyber кривичних дела“.

Прекретница у дефинисању облика, односно категорија cyber криминала је била Европска конвенција о cyber криминалу у којој су предвиђене 4 групе дела[392]:

а) **дела против поверљивости, интегритета и доступности компјутерских података и система** – њих чине незаконити приступ, пресретање, уплитање у податке или системе, коришћење уређаја (производња, продаја, увоз, дистрибуција), програма, пасворда;
б) **дела везана за компјутере** код којих су фалсификовање и крађе најтипичнији облици напада;
г) **дела везана за садржаје** као што је дечија порнографија која је најчешћи садржај који се појављује у овој групи обухватајући поседовање, дистрибуцију, трансмисију, чување или чињење доступним и расположивим ових материјала, њихову производњу ради дистрибуције и обраде у компјутерском систему или на носиоцу података;
д) **дела везана за кршење ауторских и сродних права** обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима.

391 Finnie T. Peteet T. Jarvis J. ed. (2010), The Future Challenges of Cybercrime: Volume 5 Proceedings of the Futures Working Group, http://futuresworkinggroup.cos.ucf.edu/docs/Volume%205/index.php;

392 Council of Europe, (2001), Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, приступљено 12.11.2013;

У *UNODC* студији *Comprehensive Study on Cybercrime* из 2013. године[393] се полази од 14 дела груписаних у 3 категорије[394]:

а) **дела против поверљивости, интегритета и доступности компјутерских података или система** код којих су најзаступљенији незаконити приступ компјутерском систему; незаконити приступ, пресретање или стицање компјутерских података; незаконито ометање компјутерског система или компјутерских података; производња, дистрибуција или поседовање алата за злоупотребе рачунара и кршење приватности или мера за заштиту података;

б) **дела везана за компјутере ради личне или финансијске користи или штете** какви су превара или фалсификат; дела везана за идентитет; кршење ауторских права или права на жиг; слање или контролисање слања *spam-порука*; дела који проузрокују личну штету и тражење или „нега“ деце;

в) **дела везана за компјутерске садржаје** односе се на говор мржње; дистрибуцију или поседовање дечије порнографије или за подршку тероризму.

Ова класификација се разликује од оне предвиђене у Конвенцији Савета Европа што може имати негативне глобалне последице јер праћење и регулација, односно инкриминација ће се разликовати између земаља чланица Савета Европе и потписница које нису чланице и у осталим земљама чланицама УН, као и у међународним актима које ове две организације доносе. Друга негативност је у нејасности и неконзистентности критеријума на основу којег се класификација реализовала (за две групе је у питању објект „напада“, а за једну циљ извршења дела). Позитивност ове класификације је у таксативном навођењу основних дела cyber криминала која се могу појавити као минимум за регулацију.

У студији Међународне телекоминикационе уније[395] *Understanding Cybercrime: Phenomena, Challenges and Legal Response Cybercrime* из 2012. године, наводе се следеће категорије и врсте cyber криминала:

а) **дела против поверљивости, интегритета и доступности компјутерских података и система**:
   - незаконити приступ (хакинг, *cracking*),
   - незаконито стицање података (шпијунажа),
   - незаконито пресретање,
   - уплитање/ометање података,
   - ометање система;

б) **дела везана за садржаје:**
   - еротски или порнографски материјал (искључујући дечију порнографију),
   - дечија порнографија,
   - расизам, говор мржње, глорификација насиља,

393 United Nations Office on Drugs and Crime, (2013), op. cit;

394 У објашњењу стоји да се овај списак аката користио у упитнику који је послат државама, ентитетима приватног сектора, као и међувладиним организацијама и академским институцијама за прикупљање информација. Истовремено сврха листе је увођење пробног сета аката у циљу успостављања основа за анализу.

395 ITU, (2012), op. cit., str. 16-40;

- дела везана за религију,
- незаконито коцкање и он-лајн игре,
- клевета и лажне информације,
- *spam* и сличне претње,
- други облици незаконитих садржаја;

в) **дела против ауторских права и права на жиг:**
- дела везана за ауторско право,
- дела везана за жигове.

г) **дела везана за компјутере:**
- преваре и компјутерске преваре,
- компјутерски фалсификати,
- крађа идентитета,
- злоупотреба уређаја;

д) **комбинована:**
- терористичко коришћење интернета,
- cyber ратовање,
- cyber прање новца,
- *phishing.*

Класификација *ITU* је комбинација класификације из Конвенције Савета Европе и *UNODC-a.* Врло је исцрпна и увођењем комбинованих дела омогућује да ништа не изостане. Она објашњења и појединачна понашања која илуструју сваку категорију и сваку групу, довољно су индикативна и за модификована дела.

Међутим, дубљом анализом уочава се изостанак одређених облика (нпр. угрожавање приватности, информационе, медицинске, генетске), односно експлицитно угрожавање појединачних права личности.

Другачији је начин класификовања[396] који полази од идентификације шест категорија:

а) ометање законитог коришћења рачунара (cyber вандализам, cyber тероризам, ширења вируса, црва и других облика злонамерних кодова);
б) ширење увредљивих материјала (дечија порнографија и други облици порнографског материјала, расистичке мржње, он-лајн коцкање);
в) претње комуникацијама (cyber ухођење),
г) фалсификовање и кривотворење (крађа идентитета, *phishing*);
д) преваре (преваре са кредитним картицама, преварни е-трансфер средстава, крађа на интернету или крађа телефонских услуга, интернет преваре са хартијама од вредности);
ђ) друге врсте cyber криминала (пресретање комуникација, комерцијална и корпоративна шпијунажа, коришћене комуникација ради злочиначког удруживања, електронско прање новца).

Постоје и класификације које су пошле од формулисања генеричке типологије[397] по којој се разликују 2 типа: **један** који је усмерен на технологије и

396 Broadhurst R. (2006), Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies and Management, 29, 408-433, http://eprints.qut.edu.au/3769/1/3769_1.pdf, приступљено 22.12.2013;

обухвата нпр. хакинг, *phishing* и разне облике превара и **други** који је усмерен на људе, као што су *cyberstalking*, злоупотреба деце, изнуде, корпоративна шпијунажа и cyber тероризам.

Посебно је становиште по коме постоје следеће врсте cyber криминала и могућности[398]:

а) **криминал против машина** (дела против интегритета компјутера);
б) **криминал уз коришћење машина** (дела која се односе на рачунаре или су њима потпомогнута);
в) **криминал у машинама** (дела везана за садржаје).

Њима се додају и могућности у које се убрајају: коришћење компјутера у традиционалном криминалу, хибридни криминал и прави криминал.

Једна од подела је она која је полазила од циљева, па се cyber криминал класификује као[399]:

а) **политички:**
- cyber шпијунажа,
- хакинг,
- cyber саботажа,
- cyber тероризам,
- cyber ратовање;

б) **економски:**
- cyber преваре,
- хакинг,
- крађа интернет услуга и времена,
- пиратство софтвера, микрочипова и база података,
- cyber индустријска шпијунажа,
- преварне интернет аукције (неиспоручивање производа, лажна презентација производа, лажна процена, надграђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишеструке личности);

в) **производња и дистрибуција недозвољених и штетних садржаја:**
- дечија порнографија,
- педофилија,
- ширење ставова верских секти,
- ширење расистичких, нацистичких и сличних идеја и ставова,
- злоупотреба жена;

г) **манипулација** (трговина, дистрибуција и слично) **забрањеним производима, супстанцама и робама:**
- дрогом,
- људима и децом,
- људским органима,
- оружјем;

---

397 Gordon S. Ford R. (2006), op. cit;

398 Wall D.S. (2005), op. cit;

399 Drakulić M. Drakulić R. (2005), op. cit;

д) **повреда cyber приватности:**
- надгледање е-поште,
- *spam,*
- *phiching,*
- крађа идентитета,
- прислушкивање, снимање *chat rooms*,
- праћење е-конференција,
- прикачињање и анализа *cookies*.

Недостатак ове класификација је појава истог дела у различитим категоријама (хакинг, нпр.) или непостојање одређеног дела ни у једној категорији (нпр. прављење и дистрибуција рачунарских вируса).

Као сводна класификација[400] наводи се она која „сажето укључује разне критеријуме и класификације“:

а) **политички упади и cyber ратовање:**
- индустријска шпијунажа и cyber изнуда,
- cyber тероризам,
- информационо ратовање;

б) **виртуелна пиратерија:**
- угрожавање заштићених ауторских права софтвера,
- угрожавање заштићених ауторских права на музику и видео;

в) **cyber** преваре:
- крађа идентитета,
- он-лајн преваре платних картица,
- он-лајн банкарске преваре,
- превара код личног плаћања картицама,
- лажни антивируси,
- угрожавање фармацеутике/лекова,
- преваре путника,
- преваре са лажним депоновањем,
- превара са провизијама,
- нигеријска превара или "419" превара,
- *PABX* превара,
- фискалне преваре,
- друге комерцијалне преваре;

г) **незаконити, штетани, увредљиви садржаји сајтова:**
- дечија порнографија,
- говор мржње;

д) **виктимизације појединаца на интернету:**
- дистрибуција недоличног материјала,
- интернет сређивање,
- ухођење,
- узнемиравање,
- изнуда,
- педофилија.

400 Bernik I. (2013), op. cit., pp.12-13;

Оваква класификација је можда исцрпна, али не постоји дефинисан и јасан критеријум по коме се обавља већ измешаност циљева, објеката и последица.

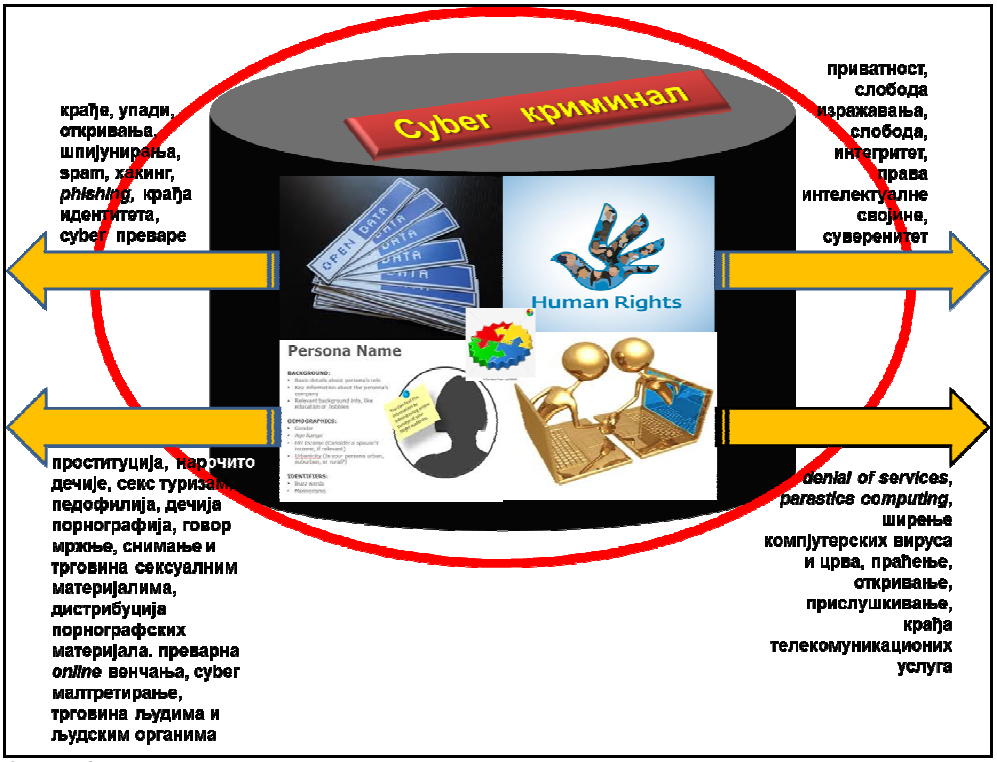
Зато се прешло на класификовање дела cyber криминала полазећи од предмета напада: података, права, информационо-комуникационих технологија и лица.

а) кад су у питању **подаци,** дела су усмерена на податке појединаца, организација, група, државе, међународних организација и асоцијација. Најчешће су то крађе, упади, откривање, шпијунирања (корпоративна, војна, cyber шпијунажа), *spam*, хакинг, *phishing*, крађа идентитета, cyber преваре и слично. Одређени садржаји су посебна категорија података, те се дела усмерена на њих могу укључити у ову категорију;

б) ако су предмет извршења дела **права,** најчешће се угрожавају права појединаца (приватности, слободе изражавања, слободе, интегритета и слично), али и права интелектуалне својине (ауторска, патентна, права на жиг, индустријски дизајн, сродна, топографије интегрисаних кола и слично) која могу бити и права организација. Суверенитет државе је специфична категорија права за које се воде cyber ратови или су предмет cyber тероризма;

в) **информационо-комуникационе технологије и услуге**, попут рачунара, рачунарских мрежа, информационих система, база података, информационе инфраструктуре, телекомуникационе, провајдерске и друге услуге су објекат *denial of services*, *parastics computing*, ширења компјутерских вируса и црва, саботаже и слично. Комуникације су жељени објект за многа дела cyber криминала јер се на свим нивоима оне желе пратити, откривати, прислушкивати. Крађа телекомуникационих услуга била је чешћа у периоду доминације компјутерског криминала, а сада су присутније злоупотребе провајдерских услуга;

г) **лица**(физичка и правна)**,** наравно, нису поштеђена деловања учниоца cyber криминала било да су млади, деца, стари, посебне групе, мањине које се излажу: проституцији, нарочито дечијој, секс-туризму, педофилији, порнографији, говору мржње, снимању и трговини сексуалним материјалима, дистрибуцији порнографских материјала, преварним он-лајн венчањима, cyber малтретирању, али и трговини људима и људским органима.



Слика 4. Типови cyber криминала

Јасно је да велики број различитих класификација сам по себи показује разноврсност ових дела и комплексност њихових појавних облика, али и различитост критеријума који се користе. У сваком случају то би поред упада у компјутерске системе и мреже, шпијунаже, саботаже, пиратерије, бомбардовања електронске поште примањем нежељених порука, "њушкања" пасворда, "прерушавања" једног рачунара другим, били и вируси, односно њихова производња и дистрибуирање, као и цео скуп недозвољених и штетних садржаја од дечије порнографије до растурања верских, расистичких и сличних садржаја. Томе треба додати и cyber саботаже[401] и тероризам, као и крађу интернет времена, услуга, индентитета, разне злоупотребе кредитних картица.

401 Weston P. (2002), Sabotage, WVP, http://www.stpubtraining.com/images/Documents/SABOTAGE.pdf; Icove D. Seger K. VonStorch W. (1995), Computer Crime, http://oreilly.com/catalog/crime/chapter/cri_02.html, приступљено 12.11.2013;

3. CYBER КРИМИНАЛ У РЕПУБЛИЦИ СРБИЈИ

3.1. Мала хронологија – како је почело?

Компјутерски криминал у бившој Југославији није новијег датума[402]. Први случајеви су забележени 80-тих година прошлог века[403]. Наиме од 1980. до 1985. године забележена је појава учесталог коришћења рачунара у пословним банкама и прве злоупотребе од стране њихових радника. Та појава је посебно евидентирана на територији града Београда. Прво такво дело са судским епилогом учинио је директор Електронског центра за аутоматску обраду података, заједно са шефом обраде и припреме података и било је дело у стицају - пљачка са злоупотребом службеног положаја, као и фалсификовање службених исправа. Циљ им је био исплата камате, а не саме суме. Вештим прикривањем, откривање дела је било отежано, а осумњичени је, чак, успео и да побегне из земље. Новац је, наравно, подигао. Из Париза је враћен захваљујући сарадњи надлежних органа.

Други је случај везан за благајника једне експозитуре банке који је, такође, извршио кривично дело пљачке са злоупотребом службеног положаја. Дело је уочено тек накнадном контролом дневника терминала.

За треће дело, које се десило 1984. године, оптужена је виша стручна сарадница у одељењу за односе са другим банкама. Вештим трансакцијама дело се појавило као дело непознатог учиниоца. Ипак је било откривено, а касније истрага показала је да је на тој књижици често било разних трансакција у периоду између 1972. и 1979. године. Међутим, власник књижице није била она. Трагање које је настављено довело је до њеног супруга који је био власника књижице. Она је знала број, па је отворила дуплу штедну књижицу, тако да муж није знао шта се са његовом књижицом дешава.

Четврти случај везан је за трансакције шалтерских службеника, који су чековним бланкетима до којих су долазили у својој експозитури, подизали веће суме новца у другим експозитурама, а затим део новца одмах, на благајни у експозитури у којој им се водио текући рачун, уплаћивали на своје рачуне.

Посебни случајеви откривени тих раних 80-их били су везани за присвајање девизне штедње и односили су се на злоупотребе електронске обраде података: присвајање девизних средстава са туђих девизних штедњи и каматних рачуна банака, недозвољене куповине девиза из депозита по кредитима и злоупотреба код обрачунавања и исплате девизне камате. Пошто је тајност штедног улога загарантована, било је отежано откривање ових дела, као и откривање и доказивање кривице извршилаца. То је био случај и са шефом девизне штедње, који је интерним налозима пребацивао средства са једне партије штедње на другу, тако што је вршио сторнирање ових промена и нових пребацивања на своју девизну штедњу, а штету сводио на терет банке у којој је радио. Извршење ових радњи омогућено је начином обављања меморисања штедњи из које су изостајали подаци о адреси штедише, његовом називу, односно имену и презимену.

---

402 Случајеви су преузети из књиге; Drakulić M. (1996), op. cit. str. 401–404;

403 Крушчић М. (1986), Искуства ГСУП-а Београд у откривању нових појавних облика кривичних дела из области привредног криминалитета у пословним банкама, Безбедност, бр. 2/86. стр. 169-176;

Тако је једна банкарска службеница између 1980. и 1983. године за "откуп" девизних депозита и динарских средстава за рачун банке упућивала своја средства на партију кредитног штедише и тако му отплаћивала кредит, да би затим "интерним налогом" стављала на исти налог своје име и презиме, партију депозита и девизну партију, па тако девизна средства усмеравала себи. Уместо за рачун банке службеница је за свој рачун вршила откуп, а како се касније показало и за рачун својих колегиница.

Слично се десило и у Пули где је због пљачке и злоупотребе службеног положаја оптужени добио 4 године и 10 месеци затвора.

Потом следе:

1984. прва пресуда у Новом Саду због крађе рачунарских програма (није у питању повреда ауторских права) и уништења рачунарских података (две године затвора);

1993. политички - ноћна крађа (из просторија једне опозиционе странке у Нишу нестрали су рачунари са свим подацима о чланству, акционим и осталим плановима и слично);

1995. факултетски - крађа рачунара (у току ноћи нестали су рачунари на којима се радио софтвер за једну државну институцију са свим корисничким захтевима и подацима);

1995. превара;

1996. војни, фалсификати;

1996. “Full Internet” и упади у академску мрежу:
- без званичних реакција
- учиниоци „клинци“
- Горан Катлевић & одговор;

1997. ФОН-овац на делу - у једном успешном предузећу у околини Београда неколико година за редом, непосредно пре и у току годишњих одмора, долазило је до диспропорције између обрачуна плата и налога банци за уплате на текуће рачуне запослених. Укупна обрачуната и укупна уплаћена сума су биле једнаке. Разлика је уочена тек након годишњих одмора (у октобру) и приписана апликацији за обрачун плата. Пошто је грешку „направио рачунар“, нема кривице запосленог, повраћај је вршен у наредних неколико месеци одбијањем одређене суме од плате. Када се ситуација поновила и четврте године банка је сугерисала фирми да провери о чему се ради јер су уплате вршене само на рачун једног запосленог, који је у то доба на годишњем одмору и новац подиже у пошти на мору. Утврђено је да постоји разлика између “оригинала” и онога што се шаље банци. Покренут је судски спор, а учинилац је отпуштен. Након извесносг времена организација је повукла тужбу;

1998/99. октобар - март:
- “Глас Косова” = почетак хакерског рата
- “Вјесник”;

1999. шпијунажа и одавање војне тајне;

1999. злоупотреба кредитних картица – оптужница је подигнута против два лица. Један од оптужених (30 година стар, незапослен из Београда) користио је бројеве туђих кредитних картица како би отворио рачун на спорткој кладионици на интернету (*EUROBET*) на

који је ставио новац преузет са рачуна власника украдених бројева картица (13000 немачких марака). Са тог рачуна је уплатио шестину укупне суме свом „другару“ у Великој Британији. Пошто се није кладио, власник коцкарнице је обавестио власника картице и на тај начин је почело откривање целе конструкције. Другооптужена је била секретарица у фирми чијем власнику и директору је узела све потребне податке за коришћење кредитних картица и дала првооптуженом. Оптужени су били за превару из користољубља,издавање и неовлашћено прибављање пословне тајне;

1999. нишки случај[404] - на једном америчком сајту појавила се листа са шифрама свих корисника нишког провајдера *Cent Net*[405]. Листу је пратило и упутство како да се ти подаци искористе. Истовремено испред седишта провајдера на улици се делила иста листа;

```
user=ivica š
        #email = ivica@xyz.co.yu
        #pf = pojedinac
        #opendate = 1997.10.10
        #lastlogin = 1999.02.13
        #timeleft = 66724
        #mail2h = 0
        #mail0h = 0
        login = cleartext slabojk!
        name = "Popovic Ivica"
        member= korisnici
        #no = 00002
```

Слика 5. Списак шифара корисника Cent Net објављен на америчком сајту

Због масовне крађе времена, која је касније довела до пропасти провајдера, деветоро оптужених оштетили су га за укупну суму од преко 50.000 (тадашњих) динара. Кривична пријава подигнута је почетком 2000. године[406], завршни претрес одржан је 2002, али се

404 Stojičević D. (2003), Nullum crimen nulla poena sine lege, Svet kompjutera, br. 3/2003;

405 Иначе у то време провајдер је био у опозицији Слободана Милошевића, а цео случај су започела лица која су специјално вратила у Ниш са студија на којима су били у Београду. Постојала је „оправдана“ сумња да је цео случај био „намонтиран“;

406 Консултације са провајдером обављене су пре подизања кривичне пријаве. Извршена је и едукација нишких судија на посебном округлом столу;

оптужени нису осећали кривима[407]. Ипак их је суд прогласио кривим и кажњени су са 15.000 динара, уз накнаду судских трошкова и причињене штете;

2001. кривичне пријаве против двојице хакера због *Denial of Service* напада на сервере ПТТ-а и *Tehnicom-a*, који су због тога имали прекид у раду од недељу дана и штету од милион и по динара;

2001. случај крађе бројева кредитних картица домаћих власника, чиме је нанесена материјална штета;

2001. Београдски процес[408] - оптужени је крајем 2001. године бесправно, на штету једне државне институције „узео“ 2 сата и 58 минута времена на интернету. У питању је било дело ситне крађе. Оптужени је признао кривицу и морао је да надокнади 81 динар оштећеној страни, кажњен је минималном казном од 1000 динара и морао је да плати судске трошкове у висини од 3000 динара (укупно 4081 динара).

2003. Cyber преваре – тројица осумњичених бавили су се преварама ступањем у везу са жртвама као купци или продавци музичких уређаја и то колекционарских. Организована група је била сигурна да нико у Србији неће реаговати и да су гитаре и новац, који су им слале жртве из Сједињених Америчких Држава у неким случајевима примали на своје адресе, потписујући се својим именима. Ова организована група се специјализовала за електричне гитаре и америчке држављане. Тако су у Београд стигле четири гитаре од којих је једна, као колекционарски примерак, процењена на 25.000 америчких долара.

Овакве активности довеле су до све веће потребе за регулацијом бројних питања везаних за компјутерски и cyber криминал, сигурност националне инфраструктуре и злоупотребе информационо-комуникационих технологија. Тако је у првој половини 1998. године, после бројних верзија и решења, дошло до доношења савезног Закона о заштити података о личности[409].

Претходио му је савезни Закон о ауторском и сродним правима. Тиме је био учињен заначајан помак у регулисању неких од проблема насталих у cyber простору. Њих је требао да заокружи Закон о телекомуникацијама. Најважнији је, свакако, савезни Кривични законик. У јуну 1998. године радна група је припремила текст новог законика. Посебно поглавље (Глава XXXIII) је било посвећено **кривичним**

---

407 У чланку Stojičević D, ((2003), Sve sudije da sude po zakoniku, Svet kompjutera, br. 5/2003, http://www.sk.rs/2003/05/skin05.html) наводи се „Opravdanja" za svoje postupke našlo je njih osmoro, dok je samo jedan priznao krivicu. Veoma zanimljiva bila su „opravdanja": *„Neko je meni krao sate pa što i ja ne bih krao", „Provajder je mogao bolje da se osigura", „Log-fajl provajdera mogao je da promeni bilo ko", „Zvao sam sa analogne centrale, a to se ne može videti u log-fajlu".* Ipak, najinteresantnije je bilo tumačenje oca optuženog maloletnika, inače čoveka iz kompjuterske „branše" a zaposlenog u državnoj instituciji, koji je izjavio da ako su navodi optužbe tačni, njegov sin je genije i to što je učinio predstavlja podvig.";

408 Stojičević D. (2003), op. cit;

409 Drakulic M. Drakulic R.(2000), Privacy in the Yugoslav Cyberspace -Problems and Protection, 15th BILETA Conference: Electronic Datasets and access to legal information, http://www.bileta.ac.uk/content/files/conference%20papers/2000/Privacy%20in%20the%20Yugoslav%20Cyberspace%20-%20Problems%20and%20Protection.pdf, приступљено 10.11.2013;

делима против система за електронску обраду података[410]. Та глава и кривична дела требало је да укључе Југославију међу земље које су регулисале овај облик криминала својим националним правом. Претходила су јој међународна акта и препоруке какве су биле *Computer Criminality Resolution of the VII Congress of OUN, XV International Congress for the Criminal Law, Recommendations of the European Union for Criminality related to computers and Recommendations related to realizing the problems in the criminal procedural law related to information technology*. Тиме се иницирало стално праћење и анализа ових специфичних криминалних активности.

Верзија посебног поглавља обухватала је пет кривичних дела:

1) оштећење рачунарских података и програма;
2) рачунарску саботажу;
3) рачунарску превару;
4) ометање рада система и мрежа за електронску обраду података и
5) неовлашћени приступ заштићеним система и мрежама за електронску обраду података.

Минимум дефинисан међународним актима је усвојен.

У каснијим верзијама преформулисани су наслови, чланови и њихов садржај[411]. У тадашњем члану 138 „Значење израза у овом законику“ унесени су нови термини: рачунарски подаци, рачунарске мреже, рачунарски вирус. Концепт исправе је проширен са рачунарским подацима. Унет је и електронски (дигитални) облик за спис, писмо, пошиљку. Тиме су створене могућности за проширење неких кривичних дела новим облицима са компјутерским модалитетима (као што су крађе, провалне крађе и разбојништва).

Наслов Глава XXXIII је преименован у **Кривична дела против безбедности рачунарских података**. Пет првобитно предвиђених кривичних дела су преформулисана уз адекватну промену садржаја и уз додавање три нова. У тој верзији нацрта Законика предвиђена су следећа кривична дела:

1) неовлашћено коришћење рачунара и рачунарске мреже;
2) оштећење рачунарских података и програма;
3) рачунарска саботажа;
4) рачунарска превара;
5) ометање рада рачунара за обраду података и рачунарске мреже;
6) неовлашћени приступ заштићеном рачунару и рачунарској мрежи;
7) прављење и уношење рачунарских вируса;
8) спречавање или ограничавање приступа јавној рачунарској мрежи.

Уношење кривичног дела спречавање или ограничавање приступа јавној рачунарској мрежи било је резултат лоше праксе која је постојала у Милошевићево време када се често блокирала академска мрежа због спречавања ширења одређених вести. Тада су нарочито били проблематични неки делови академске мреже, па су поједини корисници били искључивани уз образложење да они “злоупотребљавају електронску пошту коју финансира држава"[412]. Прва сумња да се

410 Другачије речено против рачунара!

411 Аутори ових промена били су Мирјана Дракулић и Ратимир Дракулић који су прикључени Радној групи на предлог Савезног завода за информатику;

412 www.internodium.org.yu;

она контролише појавила се у време Студентског протеста 1996/97. године. Наиме, студенти су седмог дана протеста донели одлуку о презентовању свих својих активности на интернету. Приказани су узроци протеста и неколико пута дневно су мењане вести везане за студентске активности и актуелна дешавања у Србији. Мрежа је обавила своју основну функцију – редовно обавештавање и повезивање корисника. Веб-странице Студентског протеста биле су веома посећене (у току четири месеца било је преко 80.000 посета), а преко електрнске поште размењено је на хиљаде порука. У страху од надгледања мреже користили су се пејџери. Поруке су биле надгледане, мада њихови пошиљаоци нису имали непријатности. Други талас сумњи избио је 1999. године у току интервенције НАТО-а, када се југословенским cyber простором пронела вест да су све електронске поруке, па и електронска пошта, под контролом институција из НАТО земаља.

И након израде нацрта Закона ситуација се није много променила. Тако је вест која се 17. марта 2000. године појавила у југословенском cyber постору[413] и узбуркала духове, била везана за одлуку Савезног уставног суда којом се „проглашава неуставном одредба савезног Закона о основама државне безбедности у којој је функционерима те службе дозвољено да на основу сопственог решења прислушкују телефоне, скидају електронске поруке, факсове и отварају писма због безбедности СРЈ". Југословенској јавности није било познато да је и постојала иницијатива за покретање поступка, а многима ни оваква одредба. Слику ситуације допуњује и истоветна одредба у републичком закону о чијој противуставности је био, такође, покренут поступак[414].

Отуда се, увођењем овог кривичног дела у Кривични законик, желела обезбедити слобода приступа, комуникације и изражавања које су 90-их биле озбиљно угрожене. Овакво кривично дело није било уобичајено у другим националним правима, али у другим земљама није постојала толико систематска активност спречавања и контроле приступа, које су у потпуној супротности са филозофијом саме рачунарске мреже какав је интернет. Истовремено то је било супротстављање увођењу на „мала врата" цензуре интернета.

Тада се у дефинисању санкција пошло од „духа" Закона, карактера активности и последица насталих извршењем кривичних дела. Санкције су се кретале од новчаних казни до три месеца затвора, минималнио, до 12 година, што је било максимално. У случају да је кривично дело у стицају затворске казне су могле бити строже. Рачунари и остала опрема, која се користи за чињење кривичних дела, по нацрту су се могли одузети у случају да су својина учиниоца. Ако нису у својини, могли су бити одузета из безбедносних разлога. Обавезно одузимање опреме резервисано је за посебне случајеве одређених кривичних дела каква су, нпр. оштећења рачунарских података и програма и прибављење и уношење рачунарских вируса.

У случају да је неко од 8 предложених дела извршила група учинилаца требало је да буду осуђени на казну затвора. За организатора је била прописана казна од најмање три године, а за остале чланове предвиђала се казна од 6 месеци до 5 година.

413 www.inet.co.yu;

414 Оба поступка за оцену уставности покренуо је, заједно са другима, и YUCOM (Југословенски комитет правника за људска права).

Током времена cyber простор Србије је постаое поприште за многе друге облике cyber криминала. За свега неколико година "успели" смо да се попнемо високо на ранг-листи опасних и несигурних подручја, са актерима којима расте углед у cyber подземљу. Међутим, једна група ових учнилаца изгубила је предзнак криминалаца и сврстана је у хероје, иако су њихове активности увелико превазилазиле такве квалификација. То је био случај са групом државних хакера која је „оперисала" у време НАТО бомбардовања. Неспремност правосуђа и успаваност права олакшали су прелазак ових појединаца у сферу "чистог" криминала. То је охрабрило и многе друге који су из фазе бојажљивих покушаја прешли у дрске и самосвесне криминалце, убеђене да им нико ништа не може. Такву атмосферу прекинуо је све већи број пријава истражним органима који се хватају у коштац са новим облицима криминала. Све већи број тужби нашло се пред судовима. На жалост, бројне су недаће са којима се сређу судије, тужиоци и адвокати, што умногоме отежава и продужује поступке који, иначе, изискују брзину и спремност да се у делићима секунде спасу докази и идентификују учиниоци. Иако је правна празнина, која је постојала у кривичном законодавству попуњена изменама и допунама Кривичног закона Републике Србије, са делима против безбедности рачунарских података, то није било довољно (преузета су готово сва решења нацрта Кривичног законика СРЈ из 1999. године, без допуњавања са новим кривичним делима и облицима инкримнисаног понашања). Изоставило се једно, а унело друго дело. Суочили смо се са неконзистентношћу са другим делима и санкцијама. Иако је експертски тим Савета за државну управу Владе Републике Србије и UNDP-а још у новембру 2002. године израдио прву верзију посебног, lex specialis, закона о cyber криминалу, ова верзија није даље отишла од нечије фијоке. Посебан пропуст је што се у одредбе о организованом криминалу нису уврстили и облици cyber криминала. Ситуација се знатно поправила након посебних тренинга, студијских посета, укључивања у заједничке балканске пројекте везане за борбу против овог криминала, као и све присутније сарадње са међународним организацијама, телима и асоцијацијама, као и националним институцијама других земаља. Напуштање концепције специјализованог суда није било најсрећније решење.

Табела 4. Кривична дела cyber криминала у законима Југославије и Србије

Ред. бр.	*Кривично дело*	*Нацрт Кривичног законика СР Југославије до 1999.*	*Нацрт Кривичног законика СР Југославије 1999.*	*Кривични законик Републике Србије 2005. (са изменама до 2103)*
		Глава XXXII Кривична дела против система за електронску обраду података	Глава XXXIII Кривична дела против безбедности рачунарских података	Глава XXVII Кривична дела против безбедности рачунарских података
1.	*Ометање рада рачунара и рачунарске мреже*	Да, ометање рада системи и мрежа за електронску обраду података	да	не
2.	*Оштећење рачунарских података и програма*	да	да	Да (чл. 298)
3.	*Рачунарска саботажа*	да	да	Да (чл. 299)
4.	*Прављење и уношење рачунарских вируса*	не	да	Да (чл. 300)
5.	*Рачунарска превара*	да	да	Да (чл. 301)
6.	*Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података*	да	да	Да (чл. 302)
7	*Спречавање и органичавање приступа јавној рачунарској мрежи*	не	да	Да (чл. 303)
8.	*Неовлашћено коришћење рачунара или рачунарске мреже*	не	да	Да (чл. 304)
9.	*Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података*	не	не	Да (чл. 304а)

Упоређењем између Кривичног законика Републике Србије и Конвенције може се уочити да постоје одређена одступања.

Табела 5. Групе кривичних дела која су везана за cyber круминал по Кривичном законику Републике Србије и Конвенцији о cyber криминалу

	Група кривичних дела	Кривично дело	Конвенција о cyber криминалу
Кривични законик	*Кривична дела против живота и тела*	Навођење на самоубиство и помагање самоубиства (чл. 119)	
	Кривична дела против слобода и права човека и грађанина	Повреда равноправности (чл. 128)	
		Повреда слободе изражавања, националне и етничке припадности (чл. 130)	
		Угрожавање сигурности (чл. 138)	
		Повреда тајности писма и друге пошиљке (чл. 142)	
		Неовлашћено прислушкивање и снимање (чл. 143)	
		Неовлашћено фотографисање (чл. 144)	
		Неовлашћено објављивање и приказивање туђих списа, портрета и снимака (чл. 145)	
		Неовлашћено прикупљање података о личности(чл. 146)	
		Повреда слободе говора и јавног иступања (чл. 148)	
	Кривична дела против части и угледа	Увреда (чл. 170)	
		Изношење личних и породичних прилика (чл. 172)	
		Повреда угледа Србије (чл. 173)	
		Повреда угледа због расне, верске, националне или друге припадности (чл. 174)	

Табела 5. Наставак

	Група кривичних дела	Кривично дело	Конвенција о cyber криминалу
Кривични законик	*Кривична дела против брака и породице*	Обљуба с дететом (чл. 180)	
	Кривична дела против полне слободе	Подвођење и омогућавање вршења полног односа (чл. 183)	
		Посредовање у вршењу проституције (чл. 184)	
		Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185)	да
		Навођење малолетног лица на присуствовање полним радњама (чл. 185а)	
		Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б)	да
	Кривична дела против интелектуалне својине	Повреда моралних права аутора и интерпретатора (чл. 198)	да
		Неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199)	да
		Неовлашћено уклањање и мењање електронске информације о ауторским и сродним правима (чл. 200)	да
		Повреда проналазачког права (чл. 201)	
		Неовлашћено коришћење туђег дизајна (чл. 202)	да
	Кривична дела против имовине	Превара (чл. 208)	
		Изнуда (чл. 214)	
		Уцена (чл. 215)	
		Прикривање (чл. 221)	

Табела 5. Наставак

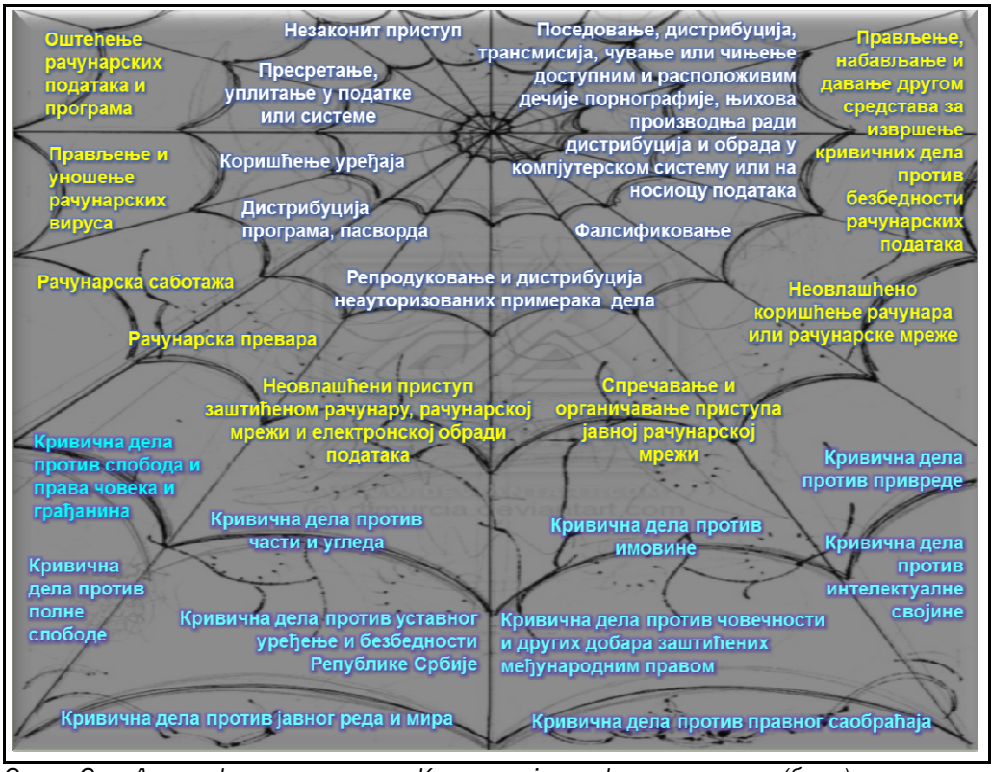
	Група кривичних дела	Кривично дело	Конвенција о cyber криминалу
Кривични законик	*Кривична дела против привреде*	Фалсификовање и злоупотре-ба платних картица (чл. 225)	
		Прање новца (чл. 231)	
		Неовлашћена употреба туђег пословног имена и друге посе-бне озанке или услуга (чл.233)	
		Злоупотреба положаја одговорног лица (чл. 234)	
		Нарушавање пословног угледа и кредитне способности (чл. 239)	
		Одавање пословне тајне (чл. 240)	
		Недозвољена производња (чл. 242)	
	Кривична дела против опште сигурности и имовине	Уништење и оштећење јавних уређаја (чл. 279)	
	Кривична дела против безбедности рачунарских података	Оштећење рачунарских података и програма (чл. 298)	да
		Рачунарска саботажа (чл. 299)	да
		Прављење и уношење рачунарских вируса (чл.300)	
		Рачунарска превара (чл. 301)	да
		Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл.302)	да
		Спречавање и органичавање приступа јавној рачунарској мрежи (чл. 303)	
		Неовлашћено коришћење рачунара или рачунарске мреже (чл. 304)	да
		Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачуна-рских података (чл. 304а)	да
	Кривична дела против уставног уређење и безбедности Републике Србије	Шпијунажа (чл. 315)	
		Одавање државне тајне (чл. 316)	
		Изазивање националне, расне и верске мржње и нетрпељивости (чл. 317)	
		Удруживање ради против уставне делатности (чл. 319)	
		Припремање дела против уставног уређења и безбеднсоти Србије (чл. 320)	

Табела 5. Наставак

	Група кривичних дела	Кривично дело	Конвенција о cyber криминалу
Кривични законик	*Кривична дела против јавног реда и мира*	Изазивање панике и нереда (чл. 343)	
		Договор за извршење кривичних дела (чл.345)	
		Злочиначко удруживање ради вршења кривичних дела (чл. 346)	
		Учествовање у групи која изврши кривично дело (чл. 349)	
		Недозвољен прелаз државне границе и кријумчарење људи (чл. 350)	
		Омогућавање злоупотребе остваривања права азила у страној држави (чл. 350а)	
		Неовлашћено организовање игара на срећу (чл. 352)	
	Кривична дела против правног саобраћаја	Фалсификовање исправе (чл. 355)	
	Кривична дела против човечности и других добара заштићених међународним правом	Расна и друга дискриминација (чл. 387)	
		Трговина људима (чл. 388)	
		Трговина малолетним лицима ради усвојења (чл. 389)	
		Тероризам (чл. 391)	
		Јавно подстицање на извршење терористичких дела (чл. 391а)	
		Вербовање и обучавање за вршење терористичких дела (чл. 391b)	
		Финансирање тероризма (чл. 393)	
		Терористичко удруживање (чл. 393а)	

Ако се узму у обзир друга кривична дела[415] која би могла да буду везана за одређене облике cyber криминала може се констатовати да је кривично законодавство прилично опсежно испунило захтеве из Конвенције о cyber криминалу.

415 По члану 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр. 61/2005 и 104/2009, предвиђено је „откривање, кривично гоњење и суђење за: 1) кривична дела против безбедности рачунарских података одређена Кривичним закоником; 2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара; 3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2 став 1 овог закона.";



Слика 6. Дела cyber криминала у Конвенцији о cyber криминалу (бело), Кривичном законику Србије (жуто) и остала дела криминала у Кривичном законику Србије (плаво)

У Кривичном законику дефинисан је покушај и саучесништво који су предвиђени по Конвенцији. Посебним Законом о одговорности правних лица за кривична дела[416] прописана је и ова специфична кривична одговорност.

Учинио се и корак напред, тероризам[417] који није предвиђен у Конвенцији, регулисан је, поред Кривичног законика[418] и у посебном Закону о спречавању прања новца и финансирању тероризма[419], као и у законима о потврђивању

416 Закон о одговорности правних лица за кривична дела, Сужбени. гласник РС, бр. 97/2008;

417 Иако није дефинисан cyber тероризам, нпр. као код Powers S., (2013), The Threat of Cyberterrorism to Critical Infrastructure, http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/; Prasad K., (2012), Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act; Grabosky P., Stohl M., (2003), Cyberterrorism; http://www.alrc.gov.au/reform-journal; United Nations, (2014), UN Action to Counter Terrorism, International Legal Instruments. http://www.un.org/terrorism/, приступљено 22.2.2014;

418 Kolarić D. (2013), Nova koncepcija krivičnih dela terorizma u Krivičnom zakoniku Republike Srbije, CRIMEN (IV) 1/2013, str. 49–71. http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen_001-2013/Broj%201-2013%20-%2004%20Dragana%20Kolaric.pdf, приступљено 22.2.2014.

419 Закон о спречавању прања новца и финансирању тероризма, Службени гласник РС, бр, 20/2009, 72/2009, 91/2010;

одговарајућих међународних аката (нпр. Закон о потврђивању Европске конвенције о сузбијању тероризма[420]).

Међутим, у Кривичном законику нису експлицитно предвиђена као посебна кривична дела у оквиру Главе 27 (кривична дела против безбедности рачунарских података): незаконито пресретање (члан 3 Конвенције) и компјутерско фалсификовање (члан 7 Конвенције).

Конвенцију је пратио Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система[421], чија дела нису, такође, експлицитно инкриминисана у Кривичном законику.

Нека од процесних права, предвиђена у Конвенцији, унета су у Закон о кривичном поступку[422], али су изостале специфичности као што су: хитна заштита сачуваних рачунарских података (хитна заштита сачуваних рачунарских података; хитна заштита и делимично откривање података о саобраћају) и прикупљање рачунарских података у реалном времену.

3.2. Мала хронологија – како се наставило?

Од 2005. године када је донет Кривични законик Републике Србије, као и Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела[423], Закон о ауторским и сродним правима[424], Закон о заштити података о личности[425], Закон о оглашавању[426], Закон о тајности података[427], Закон о дигиталном потпису[428], Закон о електронској трговини[429], Закон о тужилаштву[430], Закон о уређењу судова[431], Закон о полицији[432] почела је нова ера регулације cyber криминала и нове тенденције у борби против њега.

---

420 Закон о потврђивању Европске конвенције о сузбијању тероризма, Службени лист СРЈ – „Међународни уговори“, бр. 10/200;

421 Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, Службени гласник РС, бр. 19/09;

422 Законик о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013;

423 Службени гласник РС, бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 - др. закон, 45/2005, 61/2005, 72/2009, 72/2011 - др. закон, 101/2011 - др. Закон, 32/20;

424 Службени гласник РС, бр. 104/2009, 99/2011 и 119/2012;

425 Службени гласник РС, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС, 107/2012;

426 Службени гласник РС, бр. 79/2005;

427 Службени гласник РС, бр. 104/2009;

428 Службени гласник РС, бр. 135/2004;

429 Службени гласник РС, бр. 41/2009, 95/2013;

430 Службени гласник РС, бр. 116/2008, 104/2009, 101/2010, 78/2011 – др. закони, 101/2011, 38/2012 – одлука УС, 121/2012, 101/2013;

431 Службени гласник РС, бр. 116/2008, 104/2009, 101/2010, 31/2011 – др. закони, 78/2011 – др. закони, 101/2011, 101/2013;

432 Службени гласник РС, бр. 101/2005, 63/2009;

Подаци о кривичним делима и њиховим учиниоцима добијени су на основу истраживања које је обављено за потребе израде мастер рада студента академских мастер студија Универзитета у Београду – Факултет организационих наука, студијска група Cyber криминал[433]. Анализирани су подаци за учиниоце (тотални узорак до августа 2012. године) разних дела cyber криминала у Србији. За утврђивање њихових карактеристика коришћени су подаци везани за пол, старост, пребивалиште, ниво образовања, занимање, запосленост, брачни статус и број деце, служење војске и осуђиваност. Такође је анализирано и како су дела извршена: самостално или у групи.

3.2.1. Општи подаци о cyber криминалу

Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Министарства унутрашњих послова Републике Србије[434] и Одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва[435]у Београду подносили су пријаве за четири од осам дела која се налазе у Кривичном законику[436]. Та дела су[437]:

1) неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података;
2) прављење и уношење рачунарских вируса;
3) рачунарска превара и
4) рачунарска саботажа.

433 Студент је био на пракси у Вишем тужилаштву за високотехнолошки криминал и снимио стање. Мастер рад је одбранио пред Комисијом проф. др Мирјана Дракулић, ментор, проф. др Драгана Бечејски Вујаклија и проф. др Слободан Миладиновић;

434 Закон о полицији, Службени гласник РС, бр. 101/2005, 63/2009, odluka US, 92/20011;

435 Zakon o izmenama i dopunama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Službeni glasnik RS, br. 61/2005, 104/2009;

436 Одељење за борбу против високотехнолошког криминала је од 2009. до 31. јануара 2014. године добило 73 кривичне пријаве за кривична дела против безбедности рачунарских података и још 1272 за Фалсификовање и злоупотребу платних картица (члан 225); приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185) и искоришћавање рачунарске мреже и комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б). Кад су у питању кривична дела против безбедности рачунарских података неопходно је истаћи: а) да је у 2013. години поднето 12 кривичних пријава, а у јануару 2014. једна; б) кривичне пријаве су поднете за кривична дела оштећења рачунарских података и програма (члан 298), рачунарске саботаже (члан 299), прављења и уношења рачунарских вируса (члан 300), рачунарске преваре (члан 301), неовлшћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302), спречавања и ограничавања приступа јавној рачунарској мрежи (члан 303) и прављења, набављања и давања другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304А). Укупно за сва кривична дела поднето је 1345 кривичних пријава против 1270 лица.

437 Анализа учинилаца је рађена на основу података Одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду.

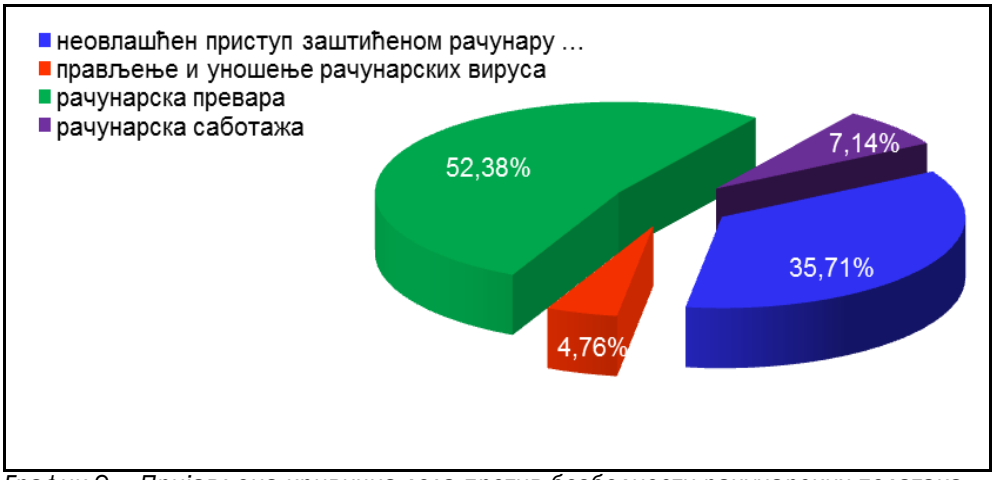


График 9. Пријављена кривична дела против безбедности рачунарских података

Учиниоци су највише извршили дела преваре и неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података (88,1%), што је разумљиво. Због економске кризе, велике незапослености, тешке привредне ситуације, нестабилног политичког амбијента - преваре су логична последица општег стања. Неовлашћени приступ (хакинг) је, између осталог, последица ранијег времена до 2000. године када је било веома много ових дела – најчешће из политичких и државних разлога. „Хероји“, а и они који су то желели да буду, наставили су ове активности, једино што то више није било некажњиво. Ни остала два дела, иако мале заступљености, нису занемарљива. Последица су непажње, знатижеље, славе и „играња“ са програмирањем (рачунарски вируси се праве и убацују и као претходница других дела, као пречица до новца, због психолошке залуђености, академских и/или политичких разлога, некад је то из жеље да се учини зло, а понекад и да се учини добро[438] или из забаве)[439], али и из беса (рачунарске саботаже често настају због незадовољства, потиснуте агресивности и љутње)[440].

Поред ових кривичних дела, која чине више од четвртине (27,1%) кривичних дела cyber криминал, почињена су и друга дела која су у вези са њима и то дела против: слободе и права човека (16,1%), интелектуалне својине (15,5%), полне слободе (32,3%), имовине (2,6%), уставног уређења (1,9%) и привреде (3,9%).

438 Нпр. вирус који траже дечију порнографију је покушавао да заустави илегалне активности;

439 Hackers Write Computer Viruses (2009), http://gizmodo.com/5827405/why-hackers-write-computer-viruses; Carnahan P. Roberts D. Shay Z. Yeary J. (2005), The motivation behind computer viruses, http://vxheaven.org/lib/pdf/The%20motivation%20behind%20computer%20viruses.pdf, приступљено 15.12.2013;

440 Keeney M. Cappelli D. Kowalski E. Moore A. Shimeall T. (2005), Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, http://www.secretservice.gov/ntac/its_report_050516.pdf (приступљено 22.12.2013.) истичу да је најчешћи мотив, поготово саботера инсајдера: а) негативан однос прама раду (92%); б) неуспешне жалбе и исправке грешака пре инцидента (85%); в) освета (84%). Већина се припремала за извршење дела.

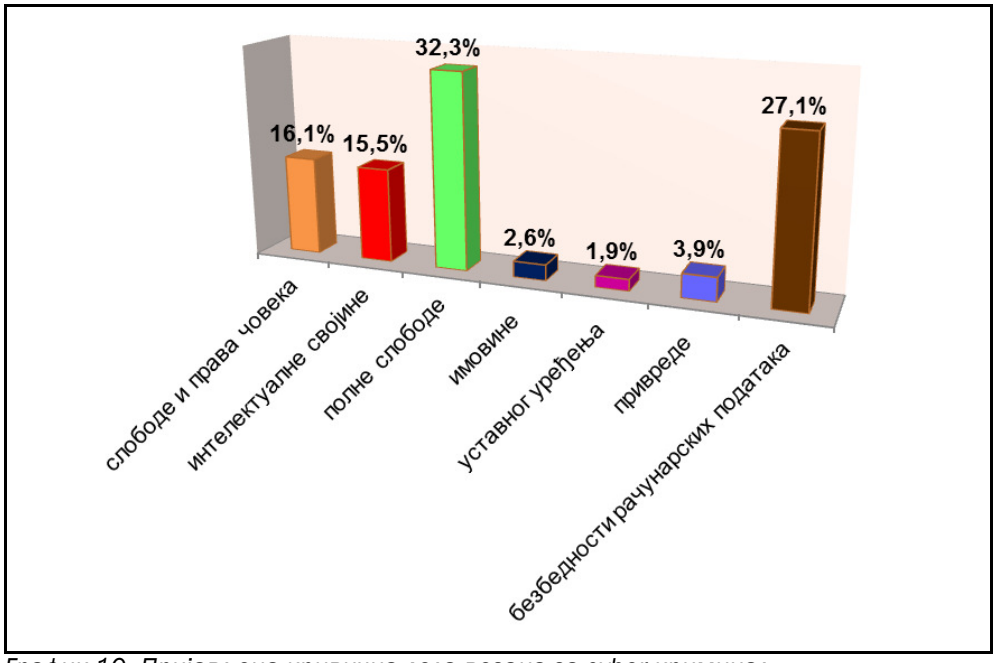


График 10. Пријављена кривична дела везана за cyber криминал

Очигледно је да је највећи део кривичних дела везан за дела против полне слободе. Због бруталности и последица по жртву и њену породицу, али и цело друштво, ова дела изазивају највећу пажњу и појачан напор свих правосудних органа, Она су условила да се донесу и посебни закони: Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (Маријин закон)[441] и Закона о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања[442].

3.2.2. Пол учинилаца

Већина учинилаца cyber криминала у Србији је мушког пола и са 92,9% мушкарци су бројчано доминантни, што значи да се жене ређе појављују као извршиоци (7,1%:92,9%).

441 Службени гласник Републике Србије, бр. 32/2013;

442 Службени гласник РС – међународни уговори, бр. 1/2010;

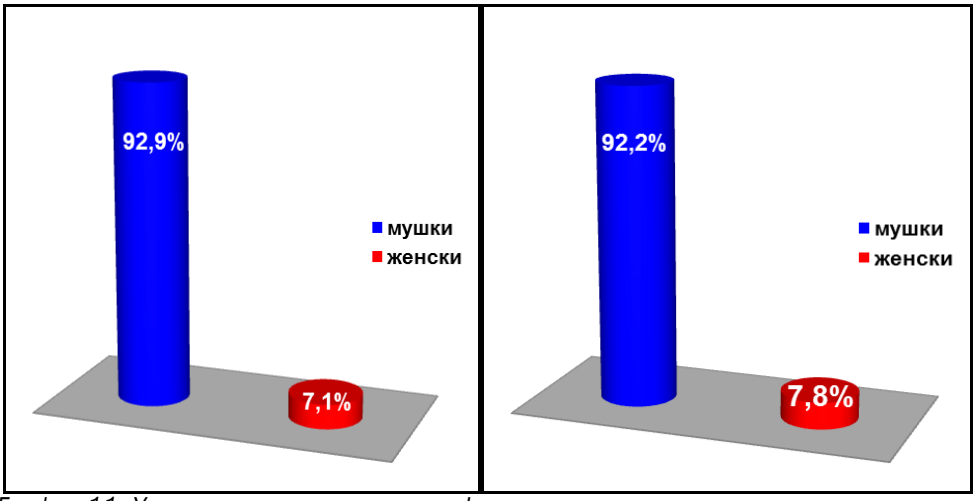


График 11. Учиниоци кривичних дела cyber криминала и свих кривичних дела по полу

Готово идентичан проценат (7,1%:7,8%) је укупно учешће жена у криминалу у Републици Србији, с тим што је највише код дела против имовине, службене дужности, брака и породице и безбедности саобраћаја. Код регионалне заступљености предњаче: Шумадија и Западна Србија, потом следи Београдски регион и Источна Србија, а најмање дела има у Војводини[443].

Без обзира на малобројност жена у криминалу[444] и њихове мотиве[445] треба им посветити посебну пажњу, а посебно у cyber криминалу. Статистике у другим земљама не показују значајно учешће жена у овом криминалу, нпр. 20% у Индији, 30% у Калкути овог криминала извршиле су жене, мада је тренд даљи раст[446]; ФБИ у потерницама за дела овог криминала „потражује“ само једну жену[447]. На

443 Република Србија, Републички завод за статистику, (2013), Пунолетни учиниоци кривичних дела у Републици Србији, 2012. – Пријаве, оптужења и осуде, http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/24/91/SB_576_Punoletni_uciniociKD2012.pdf, приступљено 22.2.2014;

444 Chensney-Lind M., (1986), Women i Crime, The female offenders, http://www.jstor.org/discover/10.2307/3174358?uid=3738928&uid=2129&uid=2&uid=70&uid=4&sid=21103473239181; Ramsland K., Women Who Kill: Part One, http://www.crimelibrary.com/notorious_murders/women/women1/1.html, приступљено 22.2.2014;

445 *Katherine Ramsland* истиче да су мотиви веома разнолики (наводи их 17) од којих су 2 везана за групе и тимове (притисак из банде, хемија тима), остали су новац, ослобађање од терета/проблема, освета, одбојност, заблуде, задовољство, жртва злостављања у детињству и младости, психопатија, изопаченост и сл. Она даље цитира студију *Eric Hickey* о Серијским убицама и њиховим жртвама (*Serial Murderers and Their Victims)* анализирајући 62 жене серијских убица чији „резултат“ је између 400 и 600 жртава, констатује да су неке од њих биле медицинске сестре, неке црне удовице, неке део тима, а неколико предаторки. Серијске убице су: често незапослени, понекад супруге, понекад имају завршен колеџ или неколико година колеџа, често са војним искуством;

446 Mukherjee W. (2007), Women taking to cyber crime in large nos, http://articles.economictimes.indiatimes.com/2007-06-23/news/28434010_1_cyber-crime-women-employees-mukund-pawar, приступљено 22.2.2014;

447 FBI, Wanted by FBI, http://www.fbi.gov/wanted/dt/donna-joan-borup/view, приступљено 22.2.2014;

Тајвану[448] је ситуација слична као у Индији: 81,1% учинилаца су мушкарци, 18,9% жене, а и распон је сличан у односу на учиниоце традиционалног криминала.

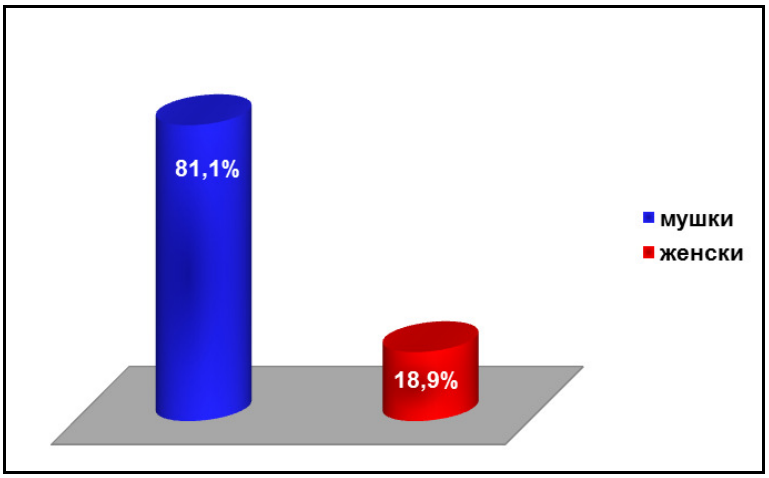


График 12. Учиниоци кривичних дела cyber криминала на Тајвану по полу

Пошто се то на Тајвану прати у периоду 1999–2004. године види се тенденција пораста: од 16% у 1999. до 24,9% у 2004. године. Пад је забележен у 2003. када је било 10,7%. У поређењу са традиционалним кривичним делима код којих је учешће жена у благом паду: 16,0% у 1999, на 15,5% у 2004. години, а једини пораст је био у 2002. години када је тај проценат био 16,2%, види се да су жене као учиниоци cyber криминала постале активније.

Учешћа жена у cyber криминалу у Србији прати још једна карактеристика - нешто мање од половине учинилаца женског пола (45,4%) није радило самостално већ су биле партнерке или познанице неког од чланова групе.

Табела 6. Однос начина извршења кривичних дела cyber криминала и пола учинилаца

		Начин извршења дела		Тотал
		Групно	Самостално	
Пол	Мушки	18,06%	81,94%	100%
	Женски	45,45%	54,55%	100%

За разлику од жена, учиниоци мушког пола углавном су извршавали дела самостално (81,9%)[449].

448 Lu C.C. Jen Y.W. Chang W. Shihchieh C. (2006), Cybercrime& Cybercriminal: An Overview of the Taiwan Experience, Journal of Computers, vol. 1, no. 6, pp. 11-18;

449 Floreencio D. Herley C. (2011), Sex, Lies and Cybercrime Surveys, http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf, приступљено 22.2.2014;

Табела 7. Однос пола учинилаца дела cyber криминала и начина извршења кривичних дела

		Пол		Тотал
		Мушки	Женски	
Начин извршења дела	Групно	83,87%	16,13%	100%
	Самостално	95,16%	4,84%	100%

Жене су често саучеснице што је одраз њихове несамосталности, поводљивости, незаинтересованости за ову врсту криминала или због преовлађујућег схватања да је за овај криминал потребно специфично техничко знање, што све више и јесте[450]. Ако се размотри последњи аргумент мора се поћи од чињенице да мањи број девојака студира техничке факултете[451]. Број студенткиња на техничким смеровима је обично једноцифрен, а инжењерство се и даље сматра доминантно мушким занимањем. Ту се Србија скоро уклапа у европске трендове (у већини земаља Европе жене чине више од половине студената, али тај проценат је много мањи у области инжењерства и технологије, нпр. око 18% у Великој Британији). Како би се ова појава ублажила, односно смањила у Данској је у току пројекат *Danish national project for attracting more girls to technical high-schools*[452]. Кад је информационо-комуникациони сектор у питању, ситуација је следећа: у Великој Британији свега 19,2% је жена менаџера (за остале секторе се њихов број пење до 45,2%[453]); укупан број запослених жена у овом сектору у Данској је 27%, а просек за Европу је око 30%[454]. Учешће жена у бизнису, менаџементу, науци је много мање него учешће мушкараца, као и у иновацијама -

450 Morcroft G. (2014), Cyber Criminals Are Getting More Sophisticated, So Watch Out For These New Scams In 2014, http://www.ibtimes.com/cyber-criminals-are-getting-more-sophisticated-so-watch-out-these-new-scams-2014-1472504, приступљено 22.3.2014;

451 Тако је школске 2009/2010. на Машинском факултету било уписано 1.953 студената и 344 студенткиња (17,61%), на Електротеничком 2.690:737, односно мање од трећине (27,39%) су студенткиње по подацима Завода за статитику Републике Србије. Међутим, слика се мења и све је више девојака које уписују „традиционално" мушке факултете;

452 Danish national project for attracting more girls to technical high-schools, (2012), http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAACAYPX&men=BAAFKZBY&smen=BAAFLAIR&fmn=BAAFLAFT, иста је ситуација и у Ирској у којој је почео пројекат *Attracting more young women into STEM* (Science and Technology) in Ireland, http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAAFKXTX&men=BAAFKZBY&fmn=BAAFLAFT; Republika Srpska vlada gender centar – centar za jednakost i ravnopravnost polova, (2013), Žene i informaciono-komunikacione tehnologije Dostupnost i mogućnosti u Republici Srpskoj, http://www.vladars.net/sr-SP-Cyrl/Vlada/centri/gendercentarrs/media/vijesti/Documents/216ene_i_IKT_FINAL).pdf, приступљено 22.2.2014;

453 Worth D. (2013), Lack of women in ICT sector costs Europe €9bn a year, http://www.v3.co.uk/v3-uk/news/2298528/lack-of-women-in-ict-sector-costs-europe-eur9bn-a-year, приступљено 22.2.2014;

454 Digital Agenda for Europe, (2013), Women in ICThttp://ec.europa.eu/digital-agenda/en/women-ict; Position Statement: Building the Gender Balance in the ICT Profession, (2013), http://www.cepis.org/index.jsp?n=1142&p=827, приступљено 22.2.2014;

свега 8,3% жена је регистровало патенате код Европског патентног завода, а 20,3% *joint venture* послова припада женама[455]. Жене ређе примењују иновације на послу, нпр. иновације у производима - 13,9% : 14,5% (жене : мушкарци); иновације процеса - 4,1% : 7,8%; иновације у организацији - 5,2% : 6,5%; и иновације у маркетинг- у 9,1% : 10,5%[456]. Због тога су Уједињене нације, тачније Међународна телекомуникациона унија (*ITU*) на конференцији у Мексику 2010. године, усвојиле *Резолицију 70: Интегрисање рода у рад Међународне уније за телекомуникације (ITU) и промовисање родне равноправности и оснаживање жена кроз коришћење информационо-комуникационих технологија (ИКТ)* у којој се, између осталог, подстиче и формирање *Глобалне мреже жена доносилаца одлука у информационо-комуникационим технологијама*[457].

Поред тога, разлог може бити и „патријархална свест“[458] са доминантном улогом породице и припадности, привржености и посвећености која се преноси и на „другу породицу - криминалну“.

Погрешно би било тврђење да су жене мање присутне на интернету или да мање њих имају рачунаре. Мада што се информисаности о карактеристика појединих дела cyber криминала тиче ситуација није баш сјајна.

Истраживање спроведено у мају у Србији показује да је од укупног броја испитаника готово незнатна разлика у половима кад су у питању коришћење интернета (49,2%) и знање коришћења рачунара (49,4%). Информисаност о *phishing*–у, на пример, је лоша јер само 5,7% (од укупног броја испитаница) зна за њега, 25% је чуло, али не зна ништа о томе, а 69,3% не зна ништа. Кад је у питању хакинг 44,7% жена (од укупног броја испитаница) зна шта је то, 41,6% је чуло, али не зна ништа и 17,6% ништа не зна. Оваква разлика би могло бити последица веће присутности указивања на хакинг у медијима.

3.2.3. Старост учинилаца

Када се појавио компјутерски криминал највише је био „резервисан“ за младе (до 25 година). Међутим, стално се померала доња старосна граница учинилаца и био је забрињавајући раст учешћа у овом криминалу млађих од 20 година. Један од многих забележених случајева крађе новца од стране десетогодишњих дечака у Аустралији био је довољно индикативан за бригу[459]. По подацима и у САД старосна се граница брзо померала на доле. У Југославији у то

455 Gender Balance and Gender Perspectives in Research and Innovation, (2014), http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAAFBTEG&men=BAAFKZBY&smen=BAAFKZBY&fmn=BAAFLAFT;

456 www.pks.rs, приступљено 22.2.2014;

457 RESOLUTION 70, (Rev. Guadalajara 2010), Gender mainstreaming in ITU and promotion of gender equality and the empowerment of women through information and communication technologies, http://www.itu.int/ITU-D/sis/Gender/Documents/Resolution_70_2010.pdf претходио је документ Gender equality and empowerment of women through ICT, (2005), http://www.un.org/womenwatch/daw/public/w2000-09.05-ict-e.pdf, приступљено 22.2.2014;

458 У друштвеном животу патријархална структурираност је још увек доминантна, као и превага принципа *pater familias;*

459 Coldwell R.A. (1990), Computer Crime: A Social Perspective, Ed.: Essays on Computer Law, Melbourne, Longman Chechire Pty. Lim. str. 219;

време већи број учинилаца су били старији од тих година. Превага је била на запосленима и то на оним који су већ стекли одређене пословне позиције. Касније се ситуација мења тако да у време учесталих хакерских напада највише заступљена групација је била између 20 и 30 година (довољно стари да знају да користе алате и технологије, а довољно млади да експериментишу, занесу се, изврше одређена кривична дела и буду агресивни). Даљим развојем информационо-комуникационих технологија старосна граница се мења. Овај сектор запошљава у свету млађе стручњаке, тако да је по старосној структури релативно млад. Нпр. у 2011. години у ЕУ само је 13,7% запослених било у доби између 50 и 64 године у односу на 26,1%, у целој привреди ЕУ[460]. То се одражава и на криминал. По Националном бироу за евиденцију података о криминалу (*The National Crime Records Bureau Data*) Индије, између 2008. и 2011. године око 60% ухапшених због cyber криминала био је из старосне групе од 18 до 30 година[461]. По истраживању из 2004. године британског *The Home Office Offending, Crime and Justice Survey (OCJS)* један од четири (26%) корисника интернета који су незаконито преузели софтвер, музику или датотеке имали су између 10 и 25 година. Они су учествовали у дистрибицији и прављењу компјутерских вируси, као и за неовлашћене приступе рачунарским датотекама других особа. Старосне разлике су евидентне и између групе са 10-17 година, која чешће шири вирусе и упада у системе, од групе 18-25 (2 : 1). Кад су у питању крађе кредитних картица број младих је веома низак (0,1% група 12-25 година), као и за куповину робе или услуга преко интернета коришћењем туђих картица. Анкета је показала да испитаници старости између 10-25 година посећују сајтове на којима сазнају детаље о томе како да почине криминал, а да они између 18 и 25 година често посећују расистичке сајтове[462].

Слично томе, интернет корисници узраста од 10 до 25 година шаљу е-поруке са намером да малтретирају, плаше и/или прете[463].

Године старости се мењају и у зависности од врсте кривичног дела[464]. Тако по подацима *Mike McGuire*[465] учиниоци сексуалних дела против деце у просеку су

460 EU Skills Panorama Analytical Highlight, (2012), Information and Communications Technologies (ICT) sector, http://euskillspanorama.cedefop.europa.eu/docs/AnalyticalHighlights/ICT_Sector_en.pdf, присту-пљено 22.1.2014;

461 Cyber Crime Offenders of Younger Age Group Rising: National Crime Records Bureau, (2013), http://www.jagranjosh.com/current-affairs/cyber-crime-offenders-of-younger-age-group-rising-national-crime-records-bureau-1375079356-1, приступљено 23.2.2014;

462 Ово питање није постављено млађим од 18 година;

463 McGuire M. (2013), Cyber crime: A review of the evidence Research Report 75, Chapter 1: Cyber-dependent crimes, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/ horr75-chap1.pdf, приступљено 24.2.2014;

464 Škulić M. (2010), Starosna granica sposobnosti za snošenje krivice u krivičnopravnom smislu, http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen%20002-2010%20_%203%20Skulic.pdf, приступљено 23.2.2014;

465 McGuire M. (2013), Cyber crime: A review of the evidence Research Report 75, Chapter 3: Cyber-enabled crimes - sexual offending against children, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf, приступљено 24.2.2014;

стари око 39 година. У Србији, односно Војводини, просечна старост је виша, она је између 40 и 59 у 55% случајева[466].

По подацима изнетим у Студији о компјутерском криминалу[467] Канцеларије УН за дрогу и криминал, већина учинилаца cyber криминала је између 18 и 30 година. Анализа је рађена на основу четири студије (*HPP*[468]*, Li*[469]*, Lu*[470]*, BAE Detic*a[471]) и даје збирни пресек година учинилаца cyber криминала, хакера, специфичности на територији Источне Азије и у односу на криминал уопште. У Студији се анализира и профил *„yahooboys"*[472] из Западне Африке[473] и констатује да је код њих највећа заступљеност учинилаца између 22 и 25 година (50%), нешто мање је оних између 26 и 29 година (40%), а незнатано (5%) у групама млађим од 22 и старијим од 29.

У Србији је, данас, највише учинилаца cyber криминала између 25 и 35 година (40,6%) старости. Ако се њима додају и они од 18 до 25 година (16,1%) добија се да су више од половине (57,6%) млади чиме се уклапамо у светске трендове, као и трендове раста и развоја информационо-комуникационих технологија.

---

466 У Војводини највише учинилаца је просечне старости између 50 и 54 године (16%), затим између 45 и 49 (15%), између 40 и 44 (14%), између 55 и 59 (11%), а најмање преко 65 година (3%) за сексуалног злостављања и злоупотребе деце, Vukotić M. Đolović A. Koprivica I. (2011), Analiza podataka centara za socijalni rad o slučajevima seksualnog zlostavljanja i zloupotrebe dece u AP Vojvodini za period 2006-2010. godina, http://www.pzsz.gov.rs/multimedia/dodaci/Pandorina_kutija_2011.pdf, приступљено 22.2.2014;

467 UNODC, (2013), Comporehensive Study on Computercrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, приступљено 19.1.2014;

468 Пројекат је почео 2004, састоји се од 8 различитих фаза и изведен је уз подршку италијанског Удружења за безбедност информационе технологије (I*talian Association for Information Technology Security - CLUSIT*) и Института за безбедносне (*Institute for Security*) и *ISECOM, Open Methodologies,* http://www.isecom.org/; Chiea R., Hackers Profiling: Who Are the Attackers?, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=302:hackers-profiling-who-are-the-attackers&catid=50:issue-7&Itemid=187, приступљено 19.1.2014;

469 Li X. (2008), The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited Through Typical Cases Prosecuted, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=203452;

470 Lu C.C. Jen Y.W. Chang W. Shihchieh C. (2006), op. cit;

471 Cyber risk assessment, http://www.baesystemsdetica.com/resources/cyber-risk-assessment/

472 Термин *yahooboys* односи се на младе до 30 година, становнике градова, који користе интернет за преваре базиране на рачунарима, *phishing, scamming*;

473 Adeniran I.A. (2008), The Internet and Emergence of Yahooboys sub-Culture in Nigeria, International Journal of Cyber Criminology,Vol 2 (2): 368–381, http://www.cybercrimejournal.com/adebusuyiijccdec2008.htm, приступљено 19.1.2014;

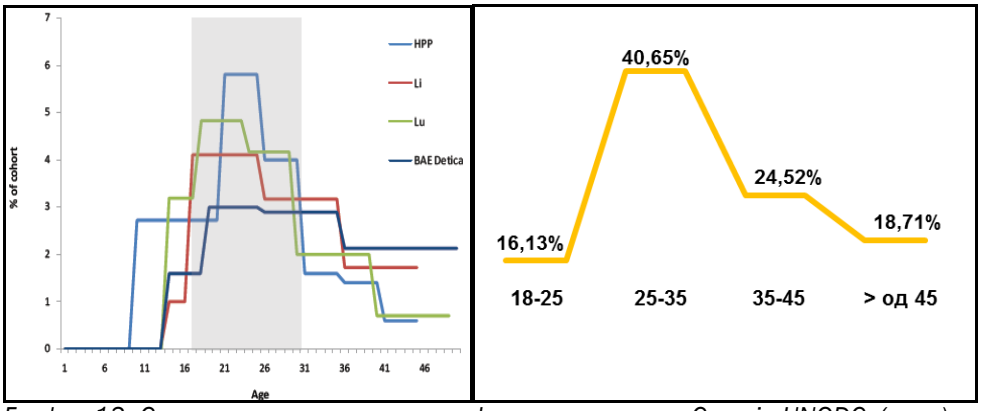


График 13. Старосне групе учинилаца cyber криминала по Студији UNODC (лево) и у Србији (десно)

Код нас нема учинилаца cyber криминала млађих од 18 година што се, иначе, не уклапа у трендове криминала уопште, али се уклапа код млађих од 22 године *yahooboys*-а.

Ипак, разлике које су у почетку коришћења интернета биле између Србије (Југославије) и других земаља у односу на светске трендове полако се губе, те се тако губе и разлике у карактеристикама (по старости).

Зависно од година учиналаца, расподела за класична кривична дела у Србији 2012. године је била мало другачија у односу на cyber криминал: највише их је било старости између 30 и 39 година (21,5%), потом између 40 и 49 година (15,8%), па између 50 и 59 (12%), између 25 и 29 (11,5%), између 21 и 24 (9,4%) и 60 и више (6,7%), а најмање између 18 и 20 година (6%). Значи, више од половине учинилаца су млади. Међутим, велика група, трећа по бројности (17%), непознате је старости[474].

Учинилаца дела cyber криминала који су деловали као група, има око две трећине између 25 и 35 година (61,3%). За дела која су извршена у групи четвртина учинилаца је између 35 и 45 година (25,8%), при томе ситуација је готово идентична и кад су у питању они који то извршавају самостално (24,5%). Занемарљивих 3,2% за дела у групи „припада“ учиниоцима од 18 до 25 година, што није разумљиво јер су то године у којима је својствена[475] припадност било којој групи, па и криминалној.

474 Република Србија, Републички завод за статистику, (2013), op.cit;

475 Припадност групама је више изражена код адолесцената: Б. Димитријевић у чланку Ličnost maloletnih delikvenata, http://www.stetoskop.info/Licnost-maloletnih-delikvenata-305-c4-content.htm наводи: „U kriminalne grupe se povezuju mladi ljudi koji imaju neke psihološke ili društvene probleme. Njihova povezanost zasniva se na prihvatanju istih gledišta i vrednosti koje grupa podržava. To je posebno prisutno kada porodica, škola i druge ustanove za mlade, za njih nisu privlačne, pa grupa postaje zamena za porodicu. Izgubljenu ili nedostajuću porodičnu komunikaciju zamenjuju onom u grupi, a sadržaj njihovog grupisanja postaje kriminalno ponašanje.“

Табела 8. Однос година старости учинилаца и начина извршења кривичних дела cyber криминала

		Старост				Тотал
		18 - 25	25 - 35	35 - 45	Више од 45	
Начин извршења	Групно	3,20%	61,30%	25,80%	9,70%	100%
	Самостално	19,40%	35,50%	24,20%	21,00%	100%

Међутим, кад су у питању самостални учиниоци у односу на грпне разлика је приметна (19,4% : 3,2%) код оних између 18 и 25 година. Код „нешто старијих“, од 25 до 35 година, однос је 61,3% : 35,5%, тј. код њих је много више присутна припадност групи. Између осталог, то је везано за мете и мотиве због којих их извршавају, као и величине дела.

Табела 9. Однос начина извршења кривичних дела cyber криминала и година старости учинилаца

		Начин извршења		Тотал
		Групно	Самостално	
Старост	18 - 25	4,00%	96,00%	100%
	25 - 35	30,16%	69,84%	100%
	35 - 45	21,05%	78,95%	100%
	Више од 45	10,34%	89,66%	100%

Самосталност је најизраженија код учинилаца између 18 и и 25 година (96%), а најмања код оних између 25 и 35 година (69,8%). То може бити одраз одрастања са рачунарима, генерација Z[476], мрежна генерација[477], а такође и специфичности периода у коме се то дешавало (бомбардовања и хаковања разних сајтова, уништавања економије НАТО земаља злоупотребом картица, наручивањем робе, преварама)[478]. Такође може бити и последица карактеристика одређеног типа cyber криминала, нпр. производња и ширење компјутерских вируса више је

476 Salimi E. (2013), Cyber Criminology: investigating the characteristics of internet crimes and criminals, International Journal of Law in the New Century, November 2013, Vol. 1(1), www.lawjournal.ir, приступљено 22.12.2013;

477 Miller M. (2002), Teenagers and Internet Safety, http://www.giac.org/paper/gsec/2081/teenagers-internet-safety/103566, приступљено 27.12.2013;

478 „Crna Ruka je ustala u ‘elektronsku odbranu’ interesa ove zemlje i ne odustaje od napada na sajtove koji plasiraju laži o situaciji u ovoj zemlji”, Dingarac D. Stančević T. (1998), Srpski hakeri „Crna ruka”, Svet kompjutera, 11/1998., http://www.sk.rs/1998/11/skin03.html; Stojičević D., (1998), Želite li američki pasoš?, Svet kompjutera, 12/1998., http://www.sk.rs/1998/12/skin06.html; Dingarac D. (1999), Internetom protiv bombi, Ratovi se danas vode na razne načine. Internet je jedno od oružja koje i mi posedujemo, Svet kompjutera, 4/1999., http://www.sk.rs/1999/04/skak01.html; Dingarac D. (1999), Na Mreži, na položaju, Dok razaranja naše zemlje traju, Internet je ostao jedino oružje koje građani mogu da upotrebe protiv agresora, Svet kompjutera, 5/1999., http://www.sk.rs/1999/05/skak01.html; Anđelić B. (1999), Ostajemo na Internetu, Svet kompjutera, 6/1999., http://www.sk.rs/1999/06/skak01.htm;

индивидуална него организована активност групе[479], мада се ситуација мења (нпр. *mobile malware* све су више последица заједничког програмирања и дистрибуирања).

3.2.4. Пребивалиште учинилаца

Пребивалиште учинилаца било ког, па и cyber криминала, вишеструко је значајно, превасходно због надлежности правосудних органа[480], а потом и због осталих процесних права[481]. Пребивалиште учинилаца може бити значајна карактеристика одређених кривичних дела која се прате и у званичним статистикама[482].

Према Републичком заводу за статистику у Србији је у 2013. години било 59,9% домаћинстава која поседују рачунар. Пенетрација показује узлазну линију у однос на 2012. годину, с тим што је она највећа у Војводини.

479 Symantec, (2013), Internet security Threat Report 2013: Trends, Volume 18, Published, April 2013, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_ 21291018.en-us.pdf, приступљено 22.2.2014;

480 Закон о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 у члану 24 дефинише да је надлежан суд на чијем подручју окривљени има пребивалиште и боравиште уколико није познато место извршења дела или ако је оно ван територије Србије
(чл. 24 ст. 1);

481 Кривични законик Републике Србије има више одредби које се односе на просторно важење. Такође и због Споразума око сарадње у кривичном гоњењу учиналаца кривичних дела, као и сарадње по Конвенцији о cyber криминалу. Иако се многе одредбе и правила везују за држављанство пребивалиште може имати значајан утицај. Тако по Закону о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013), по члану 7 тч 4 Према учиниоцу кривичног дела из члана 3 овог закона, после издржане казне затвора, спроводе се следеће посебне мере „обавезно обавештавање о промени пребивалишта, боравишта ...“, члан 8 о обавезном јављању надлежном органу полиције и Управе за извршење кривичних санкција и др;

482 Републички завод за статистику прати податке који се достављају у четири редовна годишња статистичка прегледа (извештај о учиниоцима кривичних дела који се израђују сагласно Програму и плану статистике учинилаца кривичних дела). Ljubičić S. Stephenson P. Murrill R. Laličić L. (2013), Tehnički dokument Procena sadašnjeg stanja u pogledu statistike o korupciji i privrednom kriminalu i preporuke za poboljšanja u merenju napretka u upravljanju predmetima i njihovom praćenju, http://www.coe.org.rs/REPOSITORY/2930_1_tp2_2013_pacs_assessment_statistics_and_track_record_serb.pdf, приступљено 22.2.2014;

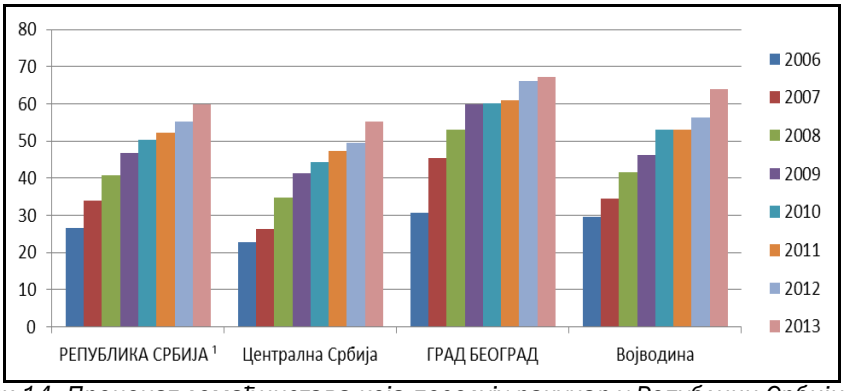


График 14. Проценат домаћинстава која поседују рачунар у Републици Србији и њеним деловима

Пораст је забележен и у броју интернет прикључака у домаћинствима, као и њиховој заступљеност у одређеним деловим Републике Србије[483].

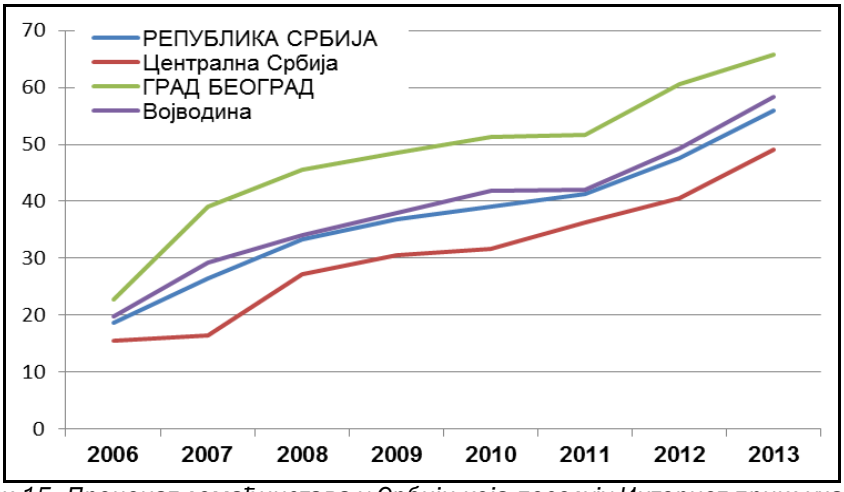


График 15. Проценат домаћинстава у Србији која поседују Интернет прикључак

Учиниоци кривичних дела махом су из великих градова или места која су у близини великих градова. Од укупног броја учинилаца 46% има пребивалиште у градовима са више од 200.000 становника[484], док 9% долази из места до 25.000 становника. У местима између 25.000 и 50.000 је 8% учинилаца, између 50.000 и 100.000 је 14%. Из места између 100.000 и 200.000 је 23%. Оваква расподела је потпуно правилна с обзиром не само на величину него и на степен развоја појединачних места.

483 Република Србија, Републички завод за статистику, (2014), Актуелни показатељи Република Србија, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2#fusnota, приступљено 25.3.2014;

484 У Србији је 3 града од преко 200.000 становника: Београд, Нови Сад и Ниш;

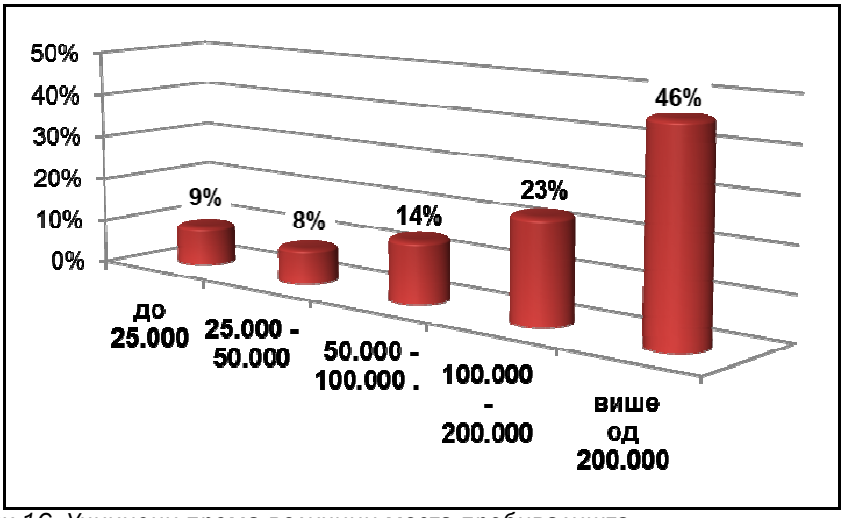


График 16. Учиниоци према величини места пребивалишта

Ако се погледају региони заједно са Београдом уочава са да највише учинилаца има пребивалиште у Београду - 38%, затим следи Војводина са 27,7%. У Шумадији и Западној Србији пребивалиште имају 22% учинилаца, а из Јужне и Источне Србије је 9,7%. На Косову и Метохији била је оптужена само једна особа, али се поступак водио против још неколико грађана те покрајине. Због несарадње косовских власти мала је вероватноћа да ће учиниоци cyber криминала са Косова и Метохије бити кажњени за своја дела. Поред њих појавила су се и 3 учиниоца са пребивалиштем у Босни и Херцеговини.

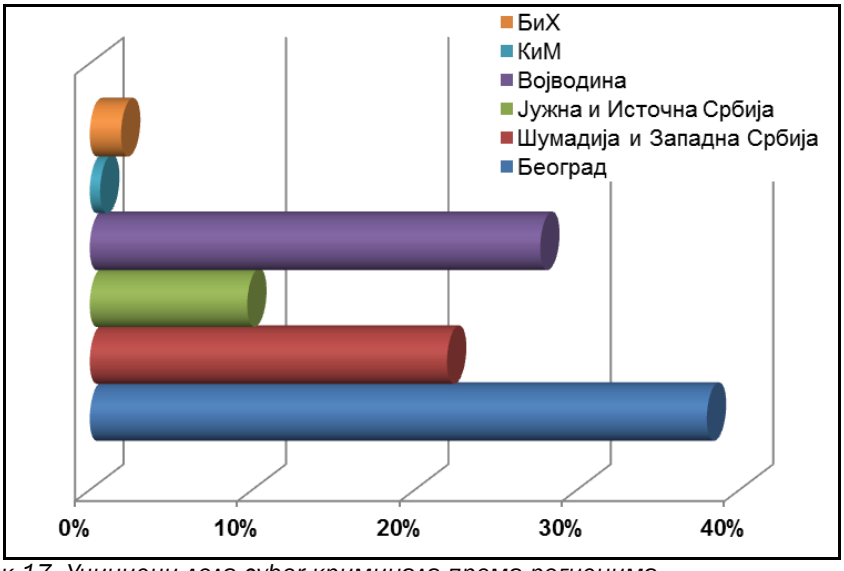
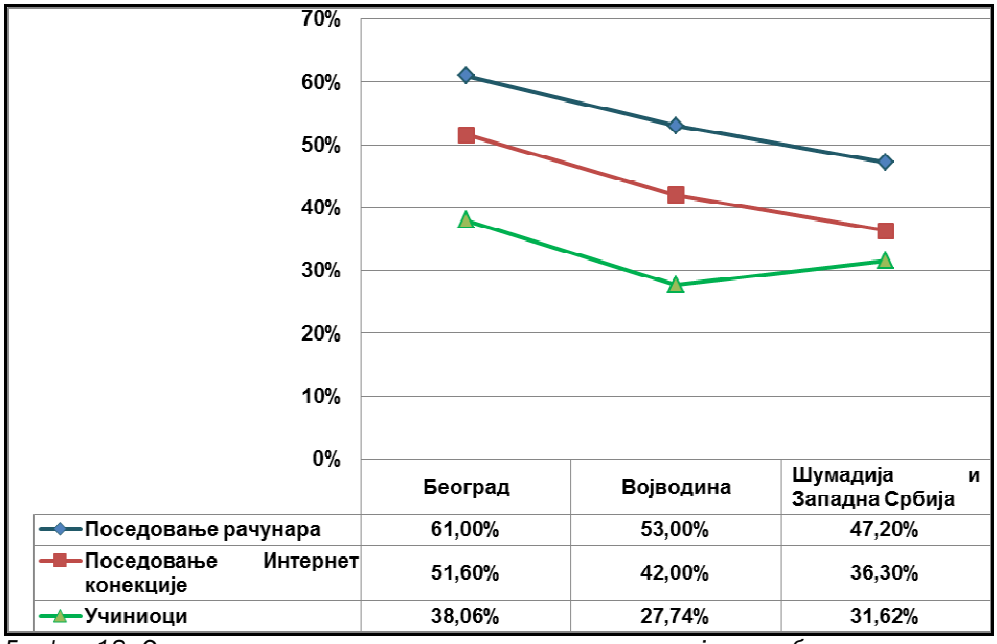


График 17. Учиниоци дела cyber криминала према регионима

Уколико се ставе у корелацију број корисника интернета, број власника рачунара и број учинилаца дела cyber криминала, могу се уочити сличности и разлике. Наиме, за сва три показатеља у Београду је највећа концентрација. Пошто је то и најразвијенији град у Србији са највећом концентрацијом становника са различитим карактеристикма, мада не и са најбржим интернетом (Нови Пазар), највећим бројем ученика и студената, најдоступнијим различитим медијима онда је и висок проценат сасвим нормалан. Једино искакање је у Војводини. За то, донекле, постоји објашњења: смањен наталитет, велики одлив из руралних средина у градове, културно[485], политичко, правно наслеђе, пад учешћа младог становништва у укупном становништву[486], велики број националних и етничких група (26)[487] и различитих концесија[488,] развој информационе инфратруктуре. Међутим, ако се погледа распон између Београда и Шумадије и Западне Србије он није велик[489].



	Београд	Војводина	Шумадија и Западна Србија
Поседовање рачунара	61,00%	53,00%	47,20%
Поседовање Интернет конекције	51,60%	42,00%	36,30%
Учиниоци	38,06%	27,74%	31,62%

График 18. Однос поседовања рачунара, интернет конекција и пребивалишта учинилаца

485 Goethals G.F.,Carugati A., Leclercq A., (2009), Differences in e-commerce behavior between neighboring countries: the case of France and Belgium, ACM, Vol. 40, Iss. 4., pp. 88-116;

486 Пројекције становништва Републике Србије, 2011–2041., http://webrzs.stat.gov.rs/WebSite/public/PublicationView.aspx?pKey=41&pLevel=1&pubType=2&pubKey=2208, приступљено 22.2.2014;

487 Аутономна покрајина Војводина, http://www.vojvodina.gov.rs/sr, приступљено 22.2.2014;

488 Đorđević D. (2006), Religije i veroispovesti nacionalnih manjina u Srbiji, Sociologija, Vol. XLVII (2005), N° 3, str. 193 - 212-. http://www.doiserbia.nb.rs/img/doi/0038-0318/2005/0038-03180503193D.pdf (приступљено 20.11.2013.), У Србији их има 30, а многе су у Војводини;

489 Нису се радила комплетна упоређења јер су КиМ, БиХ и Јужна Србија испод 10% пребивалишта учинилаца овог криминала;

Нешто мање од половине (45,2%) учинилаца дела cyber криминала у Србији, који су учествовали у групном извршењу кривичног дела, долазе из градова са више од 200.000 становника, а више од две петине (41,9%) је имало пребивалиште у градовима између 100.000 и 200.000 становника. Учиниоци cyber криминала, који су учествовали у групном извршењу дела, нису имали пребивалиште у малим местима (до 50.000 становника). Самостални учиниоци углавном живе у великим местима. Другим речима, нешто мање од половине учинилаца (46,8%) има пребивалиште у градовима већим од 200.000 становника.

Табела 10. Однос броја становника у месту пребивалишта и начина извршења дела cyber криминала

		Број становника у месту пребивалишта					Тотал
		До 25.000	25.000 - 50.000	50.000 - 100.000	100.000 - 200.000	Више од 200.000	
Начин извршења дела	Групно			12,90%	41,94%	45,16%	100%
	Самостално	11,29%	10,48%	13,71%	17,74%	46,77%	100%

На учиниоце cyber криминала се још увек не може применити географско профилисање[490]. Ова техника повезује криминалситику, биологију, математику, информатику, право и компјутерску, односно cyber форензику, али за учиниоце cyber криминала нема довољно елемената за њену примену[491]. Наиме, на основу фактора удаљености тешко се утврђује корелација између мете напада, места извршења и пребивалишта учинилаца, јер је избор приступачних тачка или локација објекта напада на мрежи велик и „лако“ доступан без обзира на удаљеност[492].

3.2.5. Ниво образовања учинилаца

Образовање је карактеристика која се увек не прати ни код учинилаца традиционалног облика криминала. Постоји схватање да криминал није „резервисан“ ни за једну категорију ни за један ниво образовања и да је „без боје“ школе која је завршена. Мотивација која је карактеристична за овај, али и за друге облике криминала, ретко је у корелацији са нивоом образовања. Ипак, сви учиниоци cyber криминала имају нешто што је блиско овој области – специфична знања. Та знања мање су везана за формално образовање. Данас, свако, нарочито запослени, мора имати бар минимална знања везана за коришћење информационо-комуникационих технологија. У документу Европске комисије истиче

490 Rossmo K. (2000), Place, space, and police investigations: hunting serial violent criminals, http://www.popcenter.org/library/crimeprevention/volume_04/10-Rossmo.pdf;

491 Tompsett C.B. Marshall M.A. Semmens C.N. (2005), Cyberprofiling: Offender Profiling and Geographic Profiling of Crime on the Internet, http://www2.hull.ac.uk/science/pdf/CyberProfilingIEEE.pdf;

492 O'Leary M. (2009), Improving Mathematical Approaches to Geographic Profiling, http://pages.towson.edu/moleary/docs/Profiling/Report.pdf, приступљено 22.2.2014;

се да основно знање ових технологија, мерено редовном употребом интернета, зависи много више од стручне спреме код радника старијих од 25 година него код млађих. Између 25 и 54 година старости 94% високообразованих су редовни корисници, док је међу најниже образованим мање од 50%. Четвртина високо образованих, који имају више од 55 година, нередовно користе интернет, а проценат за нискообразоване пење се на 80%[493].

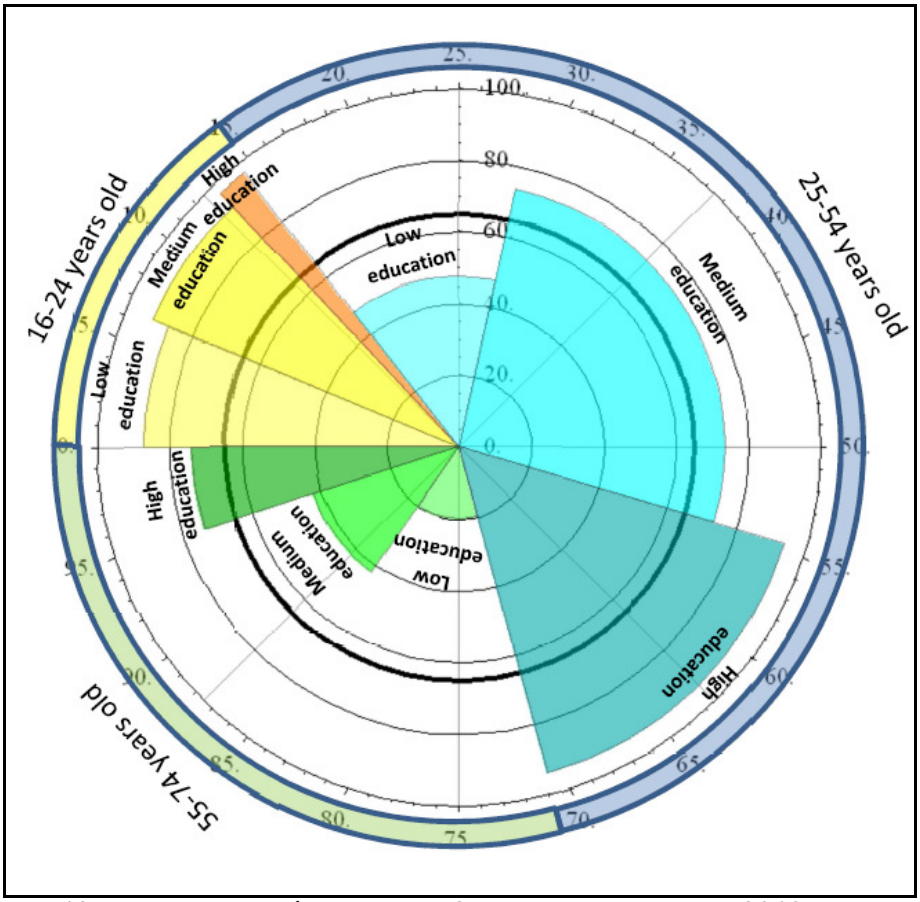


График 19. Редовна употреба интернет у 27 земаља чланица ЕУ у 2010. години од стране запослених по старости и образовању

У таквој „расподели“ нивоа образовања и учесталости, односно интензитета коришћења компјутерске мреже и учиниоци cyber криминала се појављују као специфична група.

493 European Commission, (2012), Commission Staff Working Document, Exploiting the employment potential of ICTs Accompanying the document Communication From The Commission To The European Parliament, The Council, The European Social And Economic Committee And The Committee Of The Regions, Towards a job-rich recovery, ec.europa.eu/social/BlobServlet?docId=7628&langId=en, приступљено 23.1.2014;

Заразност и овисност од изазовних активности их мотивише на стицање бољих и ефикаснијих знања[494] и вештина[495]. У Србији је нешто мање од две трећине учинилаца овог криминала (61%) завршило средњу школу, око 22% има факултет, а највиши ново образовања, докторат, 3%. Само са завршеним основним образовањем је 12,9%, док их је без икакве школе 1,9%.

Истраживање спроведено од 1999. до 2004. године на Тајвану[496] указује да учиниоци cyber криминала, у односу на ниво образовања, имају сличне карактеристике као они из Србије. Из године у годину највећи број је оних који имају средњу школу (63,4%, тј. трогодишњу 17,% и четворогодишњу 45,5%). Друга по величини група има дипломе факултета (27,8%), потом они који су завршили основну школу (5,3%), па непознатог нивоа образовања 2%. Највиши ниво образовања има 1,5%. Међу осумњиченима са дипломама завршених факултета највише је учинилаца дела везаних за ширење порука, нпр. о секс трговини. Кад су основци и средњошколци у питању, они су највише окренути крађама.

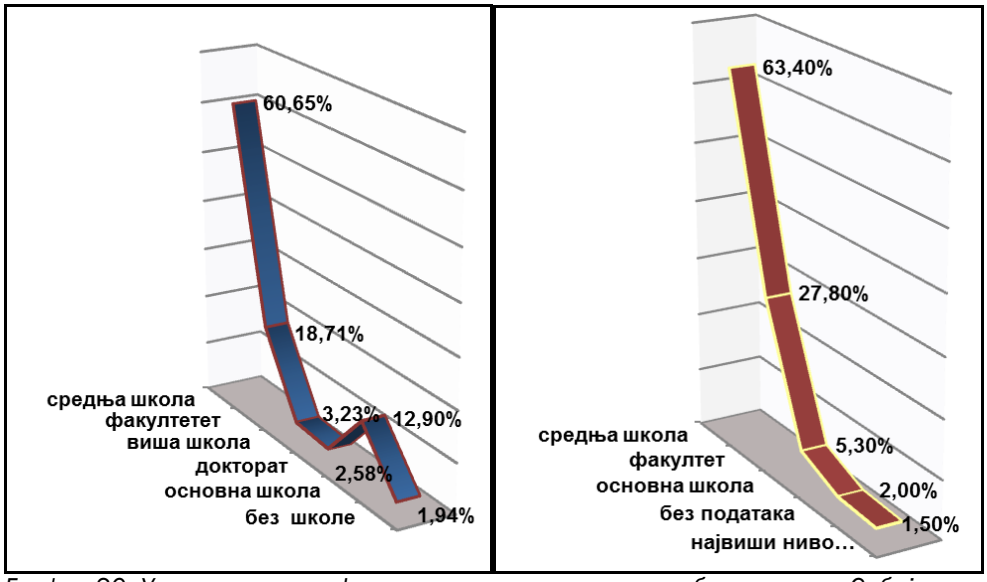


График 20. Учиниоци дела cyber криминала према нивоу образовања у Србији (лево) и на Тајвану (десно)

494 Sukhai B.N. (2004), Hacking And Cybercrime, http://jjconline.net/PAD_750/Readings/Class8/Hacking_And_Cybercrime.pdf; Australian High Tech Crime Centre Hacking Motives, (2005/2006), http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb 006.pdf, приступљено 7.12.2013;

495 Kirwan G. Power A. (2011), The Psychology of Cyber Crime: Concepts and Principles, IGI Global, pp. 59 – 67; Ziegler J.C. Muneaux M. (2007), Orthographic facilitation and phonological inhibition in spoken word recognition: A developmental study, http://gsite.univ-provence.fr/gsite/Local/lpc/dir/ziegler/article/ Ziegler_Muneaux_PBR_07.pdf, приступљено 7.12.2013;

496 Lu C.C. Jen Y.W. Chang W. Shihchieh C. (2006), op. cit;

Образовна структура учинилаца cyber криминала може бити последица учешћа актуелних студената[497], али и студената који су напустили школовање[498] и који су због веће окренутости експериментисању и примени информационо-комуникационих технологија, након успешних подухвата, ушли у воде криминала. Такође, раст ИКТ индустрије постаје примамљив и за ове категорије, а велика конкуренција ствара код њих жељу за доказивањем и истицањем. Један од начина скретања пажње је успешност активности, које по њиховом мишљењу, нису криминал. Посебно и због праксе да се из реда успешних учинилаца регрутују стручњаци за безбедност.

Ако се, пак, ови подаци упореде са подацима о обичном, традиционалним криминалом пропорције су другачије. Највише је оних са завршеним трогодишњом средњом школом (40,9%), затим четворогодишњом (35,4%) и основном школом (13%). Са завршеним факултетом или највишем образовањем је 8%, односно 0,3%.

Табела 11. Учиниоци дела cyber криминала према нивоу образовања на Тајвану[499]

Year	Elementary	J. High	S. High	College	Graduate School	Unlisted
1999	14.4% (13.7%)	12.8% (44.8%)	46.0% (30.7%)	25.1% (5.6%)	1.6% (0.4%)	0.0% (4.8%)
2000	1.7% (13.6%)	15.5% (43.9%)	41.9% (33.3%)	37.6% (7.4%)	1.0% (0.3%)	2.3% (1.5%)
2001	3.0% (13.8%)	17.4% (41.6%)	44.4% (34.2%)	33.0% (7.9%)	1.5% (0.3%)	0.6% (2.3%)
2002	1.4% (13.9%)	20.8% (38.1%)	47.4% (36.2%)	27.7% (8.8%)	1.6% (0.3%)	1.1% (2.8%)
2003	1.4% (11.9%)	23.1% (38.4%)	50.8% (38.2%)	21.6% (9.1%)	1.3% (0.3%)	1.8% (2.0%)
2004	9.6% (10.9%)	17.8% (38.8%)	42.5% (39.6%)	21.7% (8.9%)	1.8% (0.4%)	6.5% (1.4%)
1999-2004 cybercrime	5.3%	17.9%	45.5%	27.8%	1.5%	2.0%
1999-2004 Total crime	(13.0%)	(40.9%)	(35.4%)	(8.0%)	0.3%	2.5%

Разлике између ове две групе указују на то да је cyber криминал привлачнији боље образованим особама.

У Србији у 2012. години највише је учинилаца са средњом школом (53,1%), па са основном (3,7%), а најмање без школе (2,4%). За разлику од cyber криминала, учешће учинилаца са високом школском спремом у традиционалном криминалу је мања, 3,9%[500].

Група истраживача из Немачке и Немачки федерални биро за криминалошка истраживања (*the German Federal Bureau of Criminal Investigation - Bundeskriminalamt, BKA*)[501], при профилисању хакера наводе да су типични

497 Који се евидентирају као учиниоци са средњом школом;

498 Niveau G. (2010), op. cit; Wolak J. Finkelhor D. Mitchell J.K. Ybarra L. M. (2008), op. cit;

499 Lu C.C. Jen Y.W. Chang W. Shihchieh C. (2006), op. cit;

500 Република Србија, Републички завод за статистику, (2013), op. cit;

501 Испитивано је 663 испитаника - учинилаца злоупотребе идентитета, Fötinger S.C. Ziegler W. Understanding a hacker's mind – A psychological insight into the hijacking of identities, a White Paper by the Danube-University Krems, Austria, http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf, приступљено 22.1.2014;

учиниоци: мушкарци, између 16 и 21 година, чија је мотивација финансијска добит или радозналост (експериментисање са пробним верзијама и откривање грешака), који живе са родитељима, *имају средње или високо образовање и знање из рачунара/ства*, да су студенти или на обуци, да користе рачунар у слободно време, да се често састају у оквиру група и слично. Као други, односно трећи мотиватор јављују се радозналост, испробавање и утврђивање грешака (33,1%), односно техничке могућности (12%) као изазов за њихово сазнавање, откривање и савладавање. Економски разлози су први са 51,3%.

3.2.6. Професија учинилаца

Учиниоци cyber криминала поред нивоа образовања имају и одређене професије (занимања). Истраживања која су се бавила прикупљањем података и анализом професија показала су да је већина учинилаца са занимањем које има везе са информационо-комуникационим технологијама, рачунарством, инфорационим системима. ФБИ је извршио класификацију[502] различитих „професија које су се нашле у cyber *crime* бизнису' "[503]. Препознати су[504]:

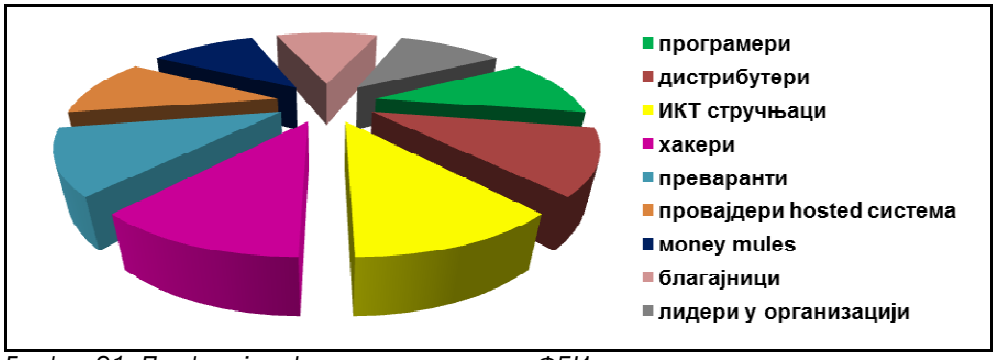


График 21. Професије cyber криминалаца по ФБИ-у

Развој *cloud* рачунарства довео је до промена и веће сложености професионалних и специјализованих знања и вештина које учиниоци cyber криминала „морају" да имају[505]. У студији *Cyber-Criminal Activity and Analysis у вези са тим се каже*: "Наше искуство показује да многи хакери нису више заблудели

502 Према ФБИ-у, организације cyber криминала функционишу као компаније са специјализованим експератима. За разлику од већине компанија, они немају дневни, недељни, годишњи, распоред рада, нити празнике и викенде, The cyber-crime professions, (2011), http://cybercrime.pandasecurity.com/blackmarket/cybercrime_professions.php, приступљено 9.12.2013;

503 Sjouwerman S. (2014), FBI: The 10 Criminal Cyber Crime Professions, http://community.spiceworks.com/topic/440511-fbi-the-10-criminal-cyber-crime-professions, приступљено 22.2.2014;

504 Walker B.M. (2010), FBI's Chabinsky: Cybercrime is a profession, http://www.fiercegovernmentit.com/story/chabinsky-cybercrime-should-be-top-priority-all-agencies-not-just-fbi/2010-03-24, приступљено 22.2.2014;

505 Wattanajantra A. (2011), Cloud security will turn cyber criminals professional, http://www.theinquirer.net/inquirer/news/2079931/cloud-security-cyber-criminals-professional, приступљено 22.2.2014;

тинејџери, који се враголасто играју са рачунарима у својим спаваћим собама. Неки су високи технолошки оператери који користе рачунаре у незаконите сврхе. Профил ранијег типичног хакера: бели мушкарац у тинејџерским годинама, обично интелигентан и из породице горње средње класе, сада је комплетно промењена услед дејства разних фактора, укључујући и економских. Рачунари су постали приступачни, а то је утицало да се профил развија и диверсификује“[506]. То је, наравно, проузроковало и промену код аналитичара cyber претњи. Они морају бити специјалисти за рачунарске мреже (диплома или дуже искуство из рачунарских наука, информационих система и технологија) и познавати методологију, технологију и алате cyber напада и инцидената, оперативу безбедност, *firewall*-ове и слични, истиче *Patricia Pickett*[507]. Она, даље, наводи да су поред тога потребне и одређене вештине: високо развијене истраживачке и аналитичке, изузетне организационе способности, посвећеност детаљима, способност тимског рада, вештине презентовања и комуникације. А те, као и многе друге, поседују и учиниоци.

Највише учинилаца cyber криминала (35%) у Србији има неко од занимања које припада техничко-технолошким струкама. На другом месту су учиниоци, четвртина од укупног броја, који уопште немају занимање. Занимања из друштвено-хуманистичке групације има 18%. Најниже учешће, 4,5%, потиче из области медицинских и природно-математичких занимања. Подаци о занимањима не постоје за 13% учинилаца.

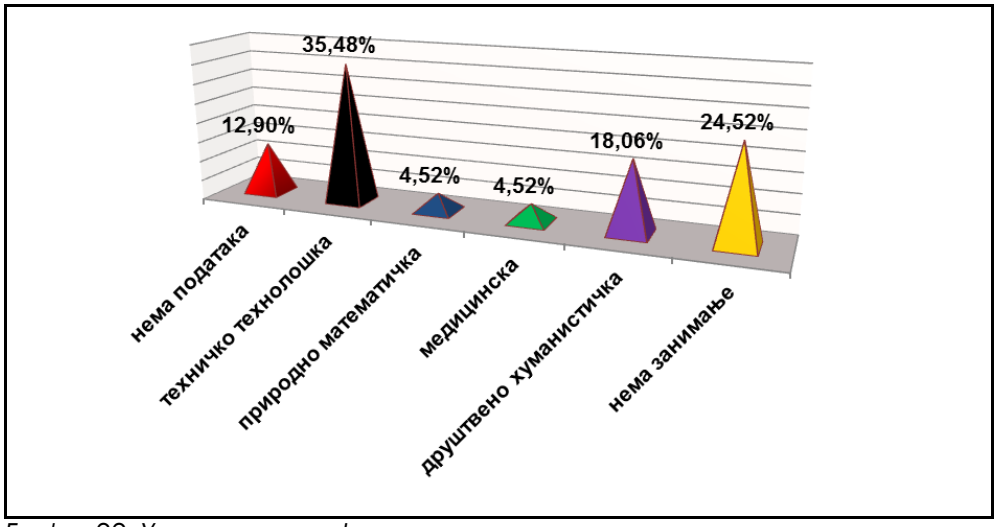


График 22. Учиниоци дела cyber криминала према занимањима

Заступљеност техничко-технолошких занимања сасвим је нормална јер и на средњем и на вишем нивоу образовања постоје веома добри наставни планови и програми који дају солидну основу за одређени фундус знања непходан, и за

506 Aseef N. Davis P. Mittal M., Sedky K. Tolba A., (2005), op.cit;

507 Pickett P. Cyber Threat Analyst - Career Profile, http://jobsearchtech.about.com/od/careertypes/p/Cyber_Threat_Analyst.htm, приступљено 12.1.2014;

криминалне активности[508]. Исти је случај и са факултетима[509]. Мало учешће учинилаца са занимањима из природно-математичке групације је прилично необично јер најјача и најтрофејнија школа у Србији је Математичка гимназија из Београда, а Природно математички факултет школује специјализоване стручњаке и из информатике. Њих је исто као и оних из медицинске групације, а четири пута мање него са занимањима из друштвено-хуманистичке групације. То може бити последица барем неколико ствари: или су толико заокупљени учењем и студирањем да немају времена за друге активности или су толико добри да нису били ухваћени у криминалу или је због изузетног великог „одлива мозгова“ из Србије отишло много њих баш из ове групације[510]. И наравно због могућности њихове веће улоге у припреми (разбијања шифара, израда алгоритама) криминалних активности него у самој фази извршења. Светски трендови су слични по бројевима, али не и по разлозима јер се стручњаци ове професије изузетно много ангажују у креирању сигурности[511], што није случај са Србијом.

3.2.7. Радни статус учинилаца

У Србији учиниоци cyber криминала долазе из свих социјалних група и имају различит радни статус: 58% учинилаца није у радном односу, 34% су стално

508 Средње електротехничке, рачунарске, политехника, техничке, http://srednje-skole.yuportal.com;

509 Барем 10-ак посебних факултета за рачунарство и софтверски инжењеринг и већи број специјализованих смерова на техничким факултетима, http://www.samozamlade.com/studenti/fakulteti.html, приступљено 12.1.2014;

510 Тако, нпр. многи ученици који су освојили светске награде из информатике добили су стране стипендије (највећи број је на Кембрицу). Исто тако „od 1991. godine iz Jugoslavije je otišlo oko 435 hiljada ljudi. Prema podacima Instituta za međunarodnu politiku i privredu zemlju je početkom devesesetih godina napustilo 719 magistara i doktora nauka što predstavlja 67% od ukupnog broja stručnjaka koji su napustili zemlju u prethodnih 15 godina (1979–1993). Inače od početka rata u Jugoslaviji, zemlju je napustilo oko 200 hiljada mladih školovanih lica, koji su izbegli zbog ratne opasnosti ili pak otišli iz jednostavnog razloga što nisu videli svoju perspektivu u kriznoj državi... Danas su traženi uglavnom stručnjaci (informatička struka, inžinjeri, inovatori, programeri, mikrobiolozi, doktori nauka, medicinari, umetnici itd.) određenog profila i po mogućnosti sa početnim kapitalom ili garancijom o izdržavanju.“ по Gabrić Molnar I. (2007). Karakteristike ljudskog resursa u regionu (Demografske promene i migracije u Vojvodini i susednim regionima), http://gabritymolnariren.com/demografske.pdf; Prema podacima ankete Instituta za sociološka istraživanja Filozofskog fakulteta (ISFF) u Begradu o karakteristikama migracija 1994. i 1999. godine, na duže vreme, i verovanto trajno, iselilo se 5% ukupnog stanovništva, što je više nego u ranijim decenijama (1971 - 2,5%, 1981 - 3,6%, 1991 - 3,9%). Prema podacima dobijenih anketom ISFF izrazitu većinu (91%) čine osobe mlađeg i srednjeg uzrasta (manje od 40 godina i to najčešće studenti i ljudi sa visokim obrazovnjem (1994. godine 44%, 1999. godine 48% ispitanika imalo je više od 13 godina školovanja). Prema ovom istraživanju, Srbija je tokom 90-ih gubila znatan deo svoje najbolje potencijalne radne snage.13 Prema podacima Ekonomske komisije UN za Evropu u periodu 1991-1993. iz republika bivše SFRJ emigriralo je između 800.000 i milion ljudi. Procena je da je 2% bilo visokoborazovano, po Grupa 484, (2010), Odliv mozgova iz Srbije - problemi i moguća rešenja, http://wbc-inco.net/object/document/7352/attach/2010majGrupa484OdlivmozgovaFinal.pdf, приступљено 22.12.2013;

511 Woollaston V. (2014), Formula for the perfect HACK: Scientists create mathematical model to understand how cybercriminals know when to strike, http://www.my-rss.co.uk/feeditem.php?feed=0&word=&search=&item=252610; Axelrod R. Rumen I. (2013), Timing of cyber conflict, http://www.pnas.org/content/early/2014/01/08/1322638111, приступљено 29.1.2014;

запослени, 6% повремено ради или их издржава неко други, док пензионисаних лица има 2%.

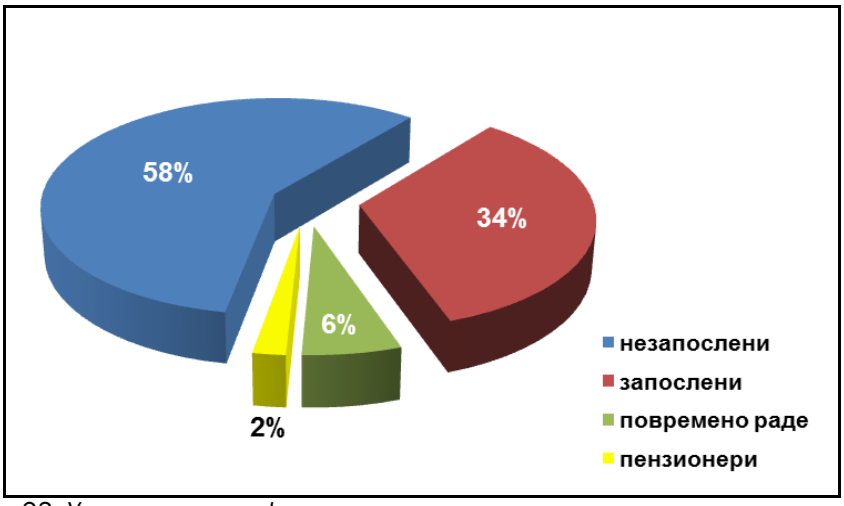


График 23. Учиниоци дела cyber криминала према радном статусу

У Србији је висока незапосленост. У октобру 2013. године укупна стопа незапослености је била 20,1% (мушкараци 19,4%, а жене 21,2%). Стопа незапослености по регионима је износила: Београд 16,7%, Војводина 23,1%, Шумадија и западна Србија 18,6%, а јужна и источна Србија 22%[512]. У децембру 2012. године стопа незапослености је износила 22,4%, и то 21,% за мушко и 23,7% за женско становништво. Стопа незапослености у региону Београда износила је 20,1%, у Војводини 25,7%, у Шумадији и западној Србији 20,3%, док је у јужној и источној Србији била 23%[513].

512 Годишња конференција за новинаре Републичког завода за статистику, http://www.srbija.gov.rs/vesti/vest.php?id=202630#top, приступљено 22.2.2014;

513 Влада Републике Србије, (2012), Стопа незапослености, http://www.srbija.gov.rs/vesti/vest.php?id=182379, приступљено 28.11.2013;

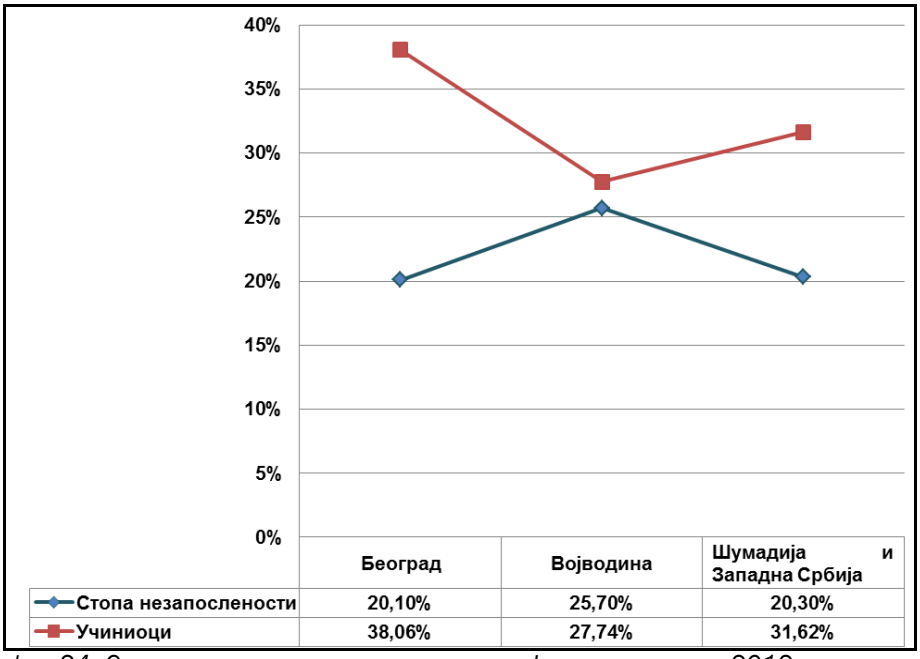


График 24. Стопа незапослености и учиниоци cyber криминала у 2012. години

Очигледно је да се учиниоци cyber криминала регрутују управо из велике групе незапослених, а посматрано по регионима уклапају се у општу слику учинилаца по пребивалишту. То значи да су многи учиниоци овог криминала били мотивисани својим лошим радним статусом и да су финансијски, односно економски разлози проузроковали ова кривична дела (у Београду од свих учинилаца 52,9% су незапослени, у Војводини 92,6%, а у Шумадији и западној Србији 64,2%). Ако се упореди однос запосленост/незапосленост учинилаца било ког кривичног дела у Србији 2012. години, може се уочити:

Табела 12. Однос радног статуса учинилаца кривичних дела и кривичних дела cyber криминала у Србији

	Радни статус				Тотал
	Запослени	Незапослени	Неактивни (студенти, ђаци, домаћице, неспособни, пензионери)	Непознато	
Сва кривична дела	33,78%	44,24%	9,87%	12,11%	100%
Дела cyber криминала	40,00%	58,00%	2,00%		100%

И у укупном броју учинилаца кривичних дела незапослени су у већем броју од запослених и неакативног становништва, мада мање него код учинилаца cyber

криминала. Најмање незапослених учинилаца је за дела против права на основу рада (0,06%), човечности и других добара заштићених међународним правом (0,1%), и Војске Републике Србије (0,2%). Највише незапослених је за кривична дела против имовине (35,5%), здравља људи (10,6%), брака и породице (9,2%). Пропорција и код запослених је више на страни учинилаца cyber криминала него код осталих кривичних дела (највише запослених је учинилаца дела против имовине 18,2% и безбедности јавног саобраћаја 15,6%, а најмање код дела против изборних права 0,028%, Војске Републике Србије и човечности и других добара заштићених међународним правом 0,056%, као и уставног уређења и безбедности Републике Србије 0,2%)[514]. Ови односи указују да су многи учиниоци кривичних дела највише усмерени на имовину, а социоекономски, односно финансијски фактори су значајни мотиватори и веома заступљени и код учинилаца cyber криминала.

Анализа заступљености учинилаца cyber криминал, који су запослени и чија су дела везана за посао који обављају, указује да је и даље присутан тренд великог учешћа интерних учинилаца (*insaiders*) у укупној популацији учинилаца овог криминала. Како наводе *Eric J. Sinrod* и *William P. Reilly* парафразирајући *Michael G. Kessler*[515]: „Запослени чине озбиљне економске губитке везане за компјутерске злоупотребе. Процењује се да је преко 80% напада на рачунарске системе почињено од стране запослених". По Студији Уједињених нација (*UNODC*) опада њихова заступљеност, поготово у приватном сектору[516]. Развијеност није кључни момент – инсајдери су присутни као учиниоци у развијеним, али и у неразвијеним земљама. Такође, заступљени су у свим старосним категоријама, и код yahooboys-a, али мање код Sakawa' boys-a[517] и у свим врстама "активности".

Социоекономски фактори присутни су и код анализе поседовања имовине од стране учинилаца cyber криминала. Имовину нема 88% учинилаца cyber криминала, што значи да је најчешћи мотив за бављење овим криминалом новац и имовинска несигурност.

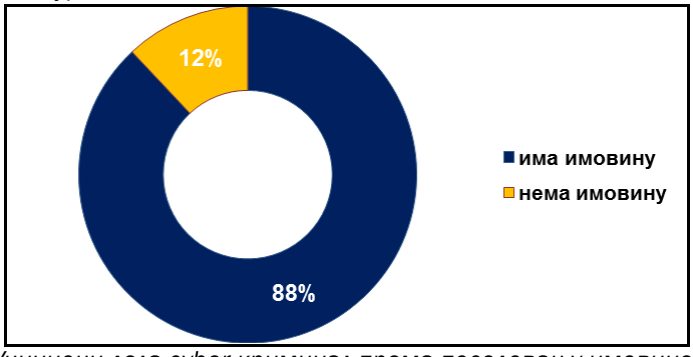


График 25. Учиниоци дела cyber криминал према поседовању имовине

514 Република Србија, Републички завод за статистику, (2013), op. cit;

515 Sinrod J.E. Reilly P.W. (2000), Cyber-crimes: a practical approach to the application of federal computer crime laws, www.sinrodlaw.com/cybercrime.doc, приступљено 28.11.2013;

516 United Nations Office on Drugs and Crime, (2013), op.cit;

517 Термин се користи за младе учиниоце између 13 и 16; иако су добили назив по јапанском граду, највише су присутни у Гани и другим земљама Африке. Antwi-Boasiako J. (2012), Six teenagers engage in mysterious Sakawa deal, http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=260823, приступљено 17.12.2013;

Однос запослености, односно незапослености и имовине учинилаца cyber криминала показује значајну повезаност. Три четвртине запослених учинилаца нема имовину, док је то код незапослених још израженије. Незапослени учиниоци у 93,3% случајева су без имовине. Што се тиче учинилаца из групе пензионера и оних који раде повремено, нико од њих нема имовину.

Табела 13. Однос имовине и радног статуса учинилаца

		Имовина		Тотал
		Има имовину	Нема имовину	
Радни статус	Запослени	25,00%	75,00%	100%
	Незапослени	6,67%	93,33%	100%
	Повремено раде		100%	100%
	Пензионери		100%	100%

Укрштањем варијабли радног статуса са групама дела cyber криминала добијено је да та веза није значајна и да има низак степен повезаности, али указује у којој је групи дела која категорија учинилаца најзаступљенија.

Табела 14. Однос група дела cyber криминала и радног статуса учинилаца

		Група дела cyber криминала								Тотал
		Слобода и права човека	Интелектуалне својине	Полне слободе	Безбедности рачунарских података	Имовине	Уставног уређења	Правног саобраћаја	Привреде	
Радни статус	Запослени	23,08%	11,54%	42,31%	19,23%		1,92%	1,92%		100%
	Незапослени	12,22%	16,67%	24,44%	33,33%	4,44%	2,22%		6,67%	100%
	Повремено раде	20,00%	30,00%	30,00%	20,00%					100%
	Пензионери			100%						100%

Више од две петине запослених учинилаца (42,3%) извршили су дела против полних слобода, оно се код незапослених налази на другом месту (24,4%), а у групи пензионера то једино кривично дело где се они појављују као учиниоци. Запослених нема као учинилаца дела против имовине и привреде, а минимално су склони делима против уставног уређења и правног саобраћаја. Они који раде повремено расподељени су скоро подједнако (2,20% и 2,30%) између четири групе кривичних дела. Највећи број кривичних дела која су извршили незапослени су дела против безбедности рачунарских података (33,3%). То може бити последица могућности и услова за извршење ових кривичних дела – приступ је могућ и од куће, нема контроле послодаваца, довољно је времена за припремање и реализовање дела, извршење може бити у било које време, али и присутна је тежња за финансијским добитима. Изостанак пензионера из ове групе кривичних дела је последица савремености извршења и неопходности одређених знања.

Ако се анализира однос између радног статуса по одређеним групама кривичних дела, уочава се да су четири групе кривичних дела: против имовине, уставног уређења, правног саобраћаја и привреде, у потпуности сконцентрисане између запослених и незапослених. Дела против слободе и права човека готово су правилно распоређена између запослених и незапослених. До угрожавања интелектуалне својине долази највише од незапослених, који су још више усмерени на угрожавање безбедност рачунарских података (71,4%).

Табела 15. Однос радног статуса учинилаца и група дела cyber криминала

		Радни статус				Тотал
		Запослени	Незапослени	Повремено ради	Пензионери	
Кривична дела против:	Слобода и права човека	48,00%	44,00%	8,00%		100%
	Интелектуалне својине	25,00%	62,50%	12,50%		100%
	Полне слободе	44,00%	44,00%	6,00%	6,00%	100%
	Безбедности рачунарских података	23,81%	71,43%	4,76%		100%
	Имовине		100%			100%
	Уставног уређења	33,33%	66,67%			100%
	Правног саобраћаја	100%				100%
	Привреде		100%			100%

Када је у питању однос радног статуса и начина извршења дела cyber криминала, запажа се да је коефицијент контингенције на ниском нивоу и представља ниску повезаност. Степен значајности је у размери према којој се веза дефинише као статистички значајна.

Табела 16. Однос начина извршења кривичног дела и радног статуса

		Начин извршења дела		Тотал
		Групно	Самостално	
Радни статус	Запослен	9,62%	90,38%	100%
	Није запослен	28,89%	71,11%	100%
	Повремено ради		100%	100%
	Пензионер		100%	100%

Незапослени учиниоци у већем броју су извршавали дела у групи (28,9%) него запослени (9,6%). Ипак, извршење у групи није уобичајено ни за једну категорију.

Пензионери и учиниоци који повремено раде, дела су извршавали искључиво самостално. То се не уклапа у општу слику о cyber криминалу, који је у већини случајева окарактерисан као организован. У Студији *UNODC*-а констатовано је да „све већи број незапослених или запослених испод могућности, дипломираних студената са компјутерским вештинама представља нови, велики потенцијални ресурс организованог криминала“[518]. Дечија порнографија (око 50.000 годишње генерисаних нових слика), крађа идентитета (око 1,5 милиона жртава само у 2010. години) и злоупотреба интелектуалне својине (нарочито софтверска пиратерија и други облици повреде ауторских права) постају привлачни за групе[519].

Овим подацима треба додати податке о имовини учинилаца дела cyber криминала.

Табела 17. Однос имовине и радног статуса учинилаца

		Имовина		Тотал
		Има имовину	Нема имовину	
Радни статус	Запослени	25,00%	75,00%	100%
	Незапослени	6,67%	93,33%	100%
	Повремено раде		100%	100%
	Пензионери		100%	100%

Упоређивањем података о имовини учинилаца видљиво је, без обзира којој категорији радног статуса припадали, да углавном немају имовину, с тим што запослени, ипак, поседују више имовине него незапослени.

3.2.8. Брачни и породични статус учинилаца

Анализа брачног и породичног статуса учинилаца кривичних дела вишеструко је значајна. Не само што се на основу података о овом статусу може донети одлука о примени принципа опортунитета[520], весе може сагледати потпунији профил учиниоца[521] и жртве[522], али и ефекти који ће доношење одређене судске одлуке

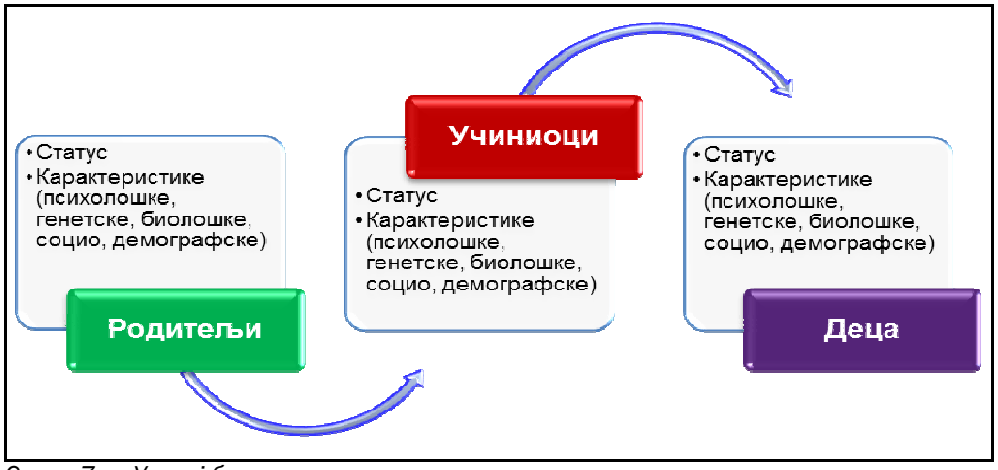
518 United Nations Office on Drugs and Crime, (2013), op.cit.; United Nations Office on Drugs and Crime, (2010), The globalization of crime a transnational organized crime threat assessment, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf, приступљено 22.1.2014;

519 United Nations Office on Drugs and Crime, (2010), op. cit.; Klee M., (2014), The new era of organized cybercrime, http://www.dailydot.com/crime/organized-crime-cybercrime-obsolete/, приступљено 27.3.2014;

520 Bejatović S. Đurđić V. Škulić M. Ilić G. Kiurski J. Matić M. Lazić R. Nenadić S. Trninić V. (2012), Primena načela oportuniteta u praksi, izazovi i preporuke, Udruženja javnih tužilaca i zamenika javnih tužilaca Srbije, http://www.partners-serbia.org/wp-content/uploads/2013/06/primena.nacela.oportuniteta-publikacija1.pdf, приступљено 8.1.2014;

521 Barnett C. (2000), The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data, http://www.fbi.gov/stats-services/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf, приступљено 15.1.2014;

имати на породицу учиниоца. Поготово ако имају малолетну децу која могу понашање родитеља прихватити као сопствени модел (*Robert Tappan Morris, junior & Robert Morris, senior*)[523] или, како истиче Игњатовић[524] наводећи Оксфордски уџбеник психијатрије, изазвати „поремећаје у психолошком развоју (нпр. у усвајању школских навика) и поремећај у понашању и емоцијама (нпр. депресивност)". Очева/мајчина склоност ка алкохолу, криминалу, ментални здравствени проблеми, професионални и образовни статус, класно обележје и слично[525], значајно утичу и на опредељење деце. Поготово утицај има понашање и карактеристике очева на женску децу. Студије спроведене у Данској, Шведској, Канади и на Тасманији стављају у директну корелацију ове факторе учинилаца и понашање њихове деце, као и понашање родитеља. Породица и њене психо-социјалне карактеристике повезане су са криминалним понашањем деце. Оне су индивидуални фактори ризика.



Слика 7. Утицај брачног и породичног статуса учинилаца кривичног дела

Постоје многе предрасуде да су учиниоци cyber криминала: усамљени, без друштва, без партнера, асоцијални, отуђени и од сопствене породице. То се потврђује и код учинилаца овог криминала у Србији јер нешто више од половине (57%) нису удати или ожењени. Осим психолошких карактеристика личности то се може приписати и другим факторима као што је лоша економска ситуација и

522 Ndubueze N.P. Igbo M.U.E, Okoye O.U. (2013), Cyber Crime Victimization among Internet active Nigerians: An Analysis of Socio-Demographic Correlates, International Journal of Criminal Justice Sciences, Vol. 8 (2): 225–234, http://www.sascv.org/ijcjs/pdfs/philipetalijcjs2013vol8issue2.pdf, приступљено 15.1.2014;

523 Robert Tappan Morris, bio je tvorac; Morris Warm, a Robert Morris, otac je se bavio kriptografijom, radio je u Bell Lab, a posle i u NSA. kretor Unix computer operating system i Core War igrice koja je bila preteča trapdoor-a, Drakulić M., (1996), op. cit., str. 432;

524 Ignjatović Đ. (2011), Pojam i etiologija nasilničkog kriminaliteta, CRIMEN (II) 2/2011, str 179–211, http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen_002-2011_02.Ignjatovic.pdf, приступљено 15.1.2014;

525 Klinteberg B. Almquist Y. Beijer U. Rydelius A.P., (2011), Family psychosocial characteristics influencing criminal behaviour and mortality - possible mediating factors: a longitudinal study of male and female subjects in the Stockholm Birth Cohort, http://www.biomedcentral.com/1471-2458/11/756, приступљено 15.1.2014;

демографске карактеристике становништва. Наиме, у Србији свега 20,5% становништва има децу из брачне или ванбрачне заједнице. Ако се томе дода да је индекс функционалног становништва 46,7[526], а просечна старост 42,2 година (мушкарци 40,9, односно жене 43,5)[527], онда је јасно да се корени оваквог брачног стања учинилаца налазе под великим утицајем социодемографских фактора[528].

Проценат учинилаца cyber криминала који су у брачној заједници је 32%, они који су разведени 8%, а у ванбрачној заједници живи свега 3%. Нема удоваца/удовица.

Поређењем са брачним статусом учинилаца других кривичних дела у Србији ситуација је следећа:

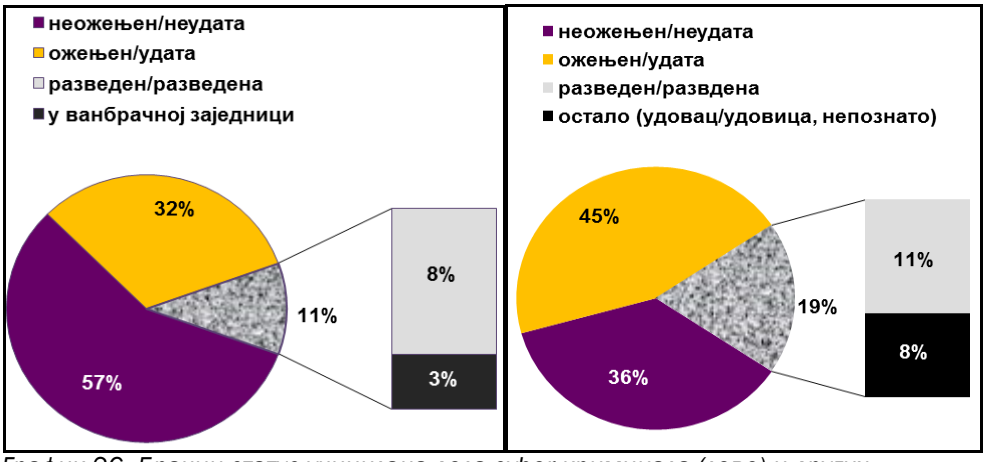


График 26. Брачни статус учинилаца дела cyber криминала (лево) и других кривичних дела (десно)

Много је више учинилаца других кривичних дела који су у браку него разведених, односно оних који су изгубили свог брачног друга.

526 Индекс функционалног становништва представља однос становништва старог 0-14 и 65 и више година према становништву старом 15-64 године, процењеног средином године посматрања;

527 Република Србија, Републички завод за статистику, (2013), Демографска статистика 2012, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=164, приступљено 15.1.2014;

528 Goodwin V. Davis B. (2011), Crime families: Gender and the intergenerational transfer of criminal tendencies Trends & Issues in Crime and Criminal Justice no.414, Australian Institute of Criminology http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi414.html,приступљено 15.1.2014;

Табела 18. Однос радног статуса и имовине са брачним статусом учинилаца cyber криминала у Србији

		Радни статус				Тотал	Имовина		Тотал
		Запослени	Незапо-слени	Повремено раде	Пензионери		Има имовину	Нема имовину	
Брачни статус	Ожењен / удата	46,00%	44,00%	10,00%		100%	28,00%	72,00%	100%
	Разведен / разведена	25,00%	66,70%	8,30%		100%	25,00%	75,00%	100%
	У ванбрачној заједници	50,00%	50,00%			100%	25,00%	75,00%	100%
	Неожењен / неудата	27,00%	65,20%	4,50%	3,40%	100%	1,10%	98,90%	100%

Учиниоци cyber криминала у Србији који су у брачној заједници су скоро у једнаком броју запослени (46%) и незапослени (44%), док 10% повремено ради. Велика већина (72%) нема имовину, а само 28% је поседује. Они који су неожењени/неудати су нешто мање од две трећине (65,2%) незапослени и скоро уопште немају имовину (98,9%).

Већина учинилаца cyber криминала (62,6%) нема децу, 35,5% има до троје деце, док они који имају више од троје деце је 1,9%.

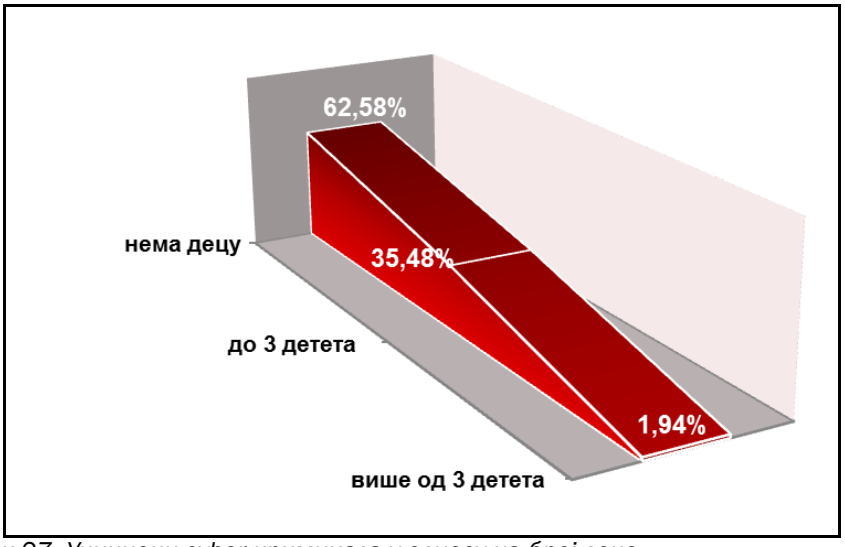


График 27. Учиниоци cyber криминала у односу на број деце

Ако се прати корелација броја деце, радног статуса и имовине, уочава се да је степен контингенције низак, али да указује на њену статистичку значајност. Приближно исти коефицијенти добијени су и при укрштању броја деце са имовином учинилаца cyber криминала.

То значи да је однос броја деце са радним статусом и имовином ових учинилаца статистички значајан, али има ниску повезаност. Скоро две трећине

учинилаца cyber криминала у Србији који немају децу су незапослени (63,9%) и немају имовину (94,8%). Око половине незапослених учинилаца има до троје деце (49,1%). Нешто мање од половине запослених учинилаца (45,5%) има до троје деце. Четвртина (25,5%) оних који имају до троје деце поседују имовину.

3.2.9. Рецидивизам учинилаца cyber криминала

Од 1972. године, када су у Филаделфији *Marvin E. Wolfgang, Robert M. Figlio* и *Thorsten Sellin*[529] објавили обимну студију о рецидивизму, започела је нова ера криминологије и криминолошких истраживања. Почела је примена новог методолошког приступа у анализи временских серија група учинилаца одређених кривичних дела (нпр. *pedo cyber offenders*)[530], који се прате у периоду од 6 месеци до 25 година, након пуштања из затвора. Једно новије истраживање, везано за праћење сексуалних учинилаца, показује да је 52% њих извршило дело у поврату и 25 година након ослобађања, али врло мало их бива ухваћено и оптужено. Број њихових жртава је застрашујући (сваки сексуални преступник у периоду од 25 година након пуштања на слободу има 5,2 жртве)[531].

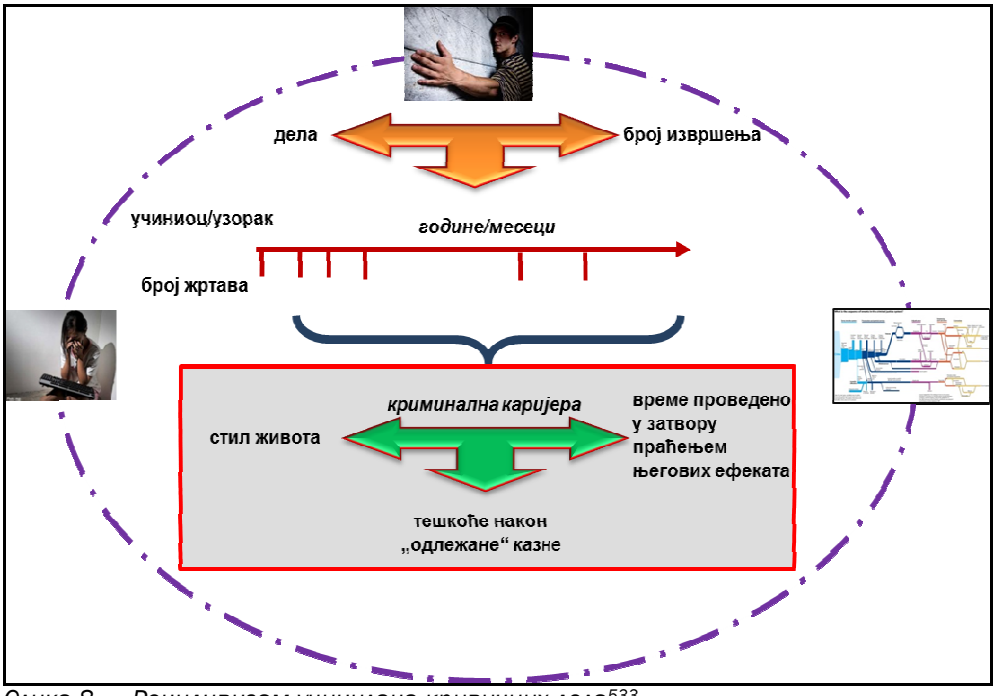
Криминална каријера која се прати базира се на уобичајеним карактеристикама (старост, пол, врста дела и слично) уз додатак стила (начина) живљења и тешкоћа након „одлежане" казне[532]. Праћење се организује у временским серијама које варирају од врсте дела и година, односно старости учинилаца.

529 Wolfgang E.M., Figlio M.R., Sellin T., (1972), Delinquency in a Birth Cohort, University of Chicago Press, Chicago;

530 Erickson L.M. (1973), Delinquency in a Birth Cohort: A New Direction in Criminological Research, Journal of Criminal Law and Criminology, Volume 64 | Issue 3, pp. 362–367, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5866&context=jclc, приступљено 15.1.2014;

531 Steele H. (2010), 25% Recidivism Rate – Really? http://innocentjustice.org/2010/25-recidivism-rate-%E2%80%93-really/, приступљено 15.1.2014;

532 Payne J. (2007), Recidivism in Australia: findings and future research, Australian Institute of Criminology, http://www.aic.gov.au, приступљено 15.1.2014;

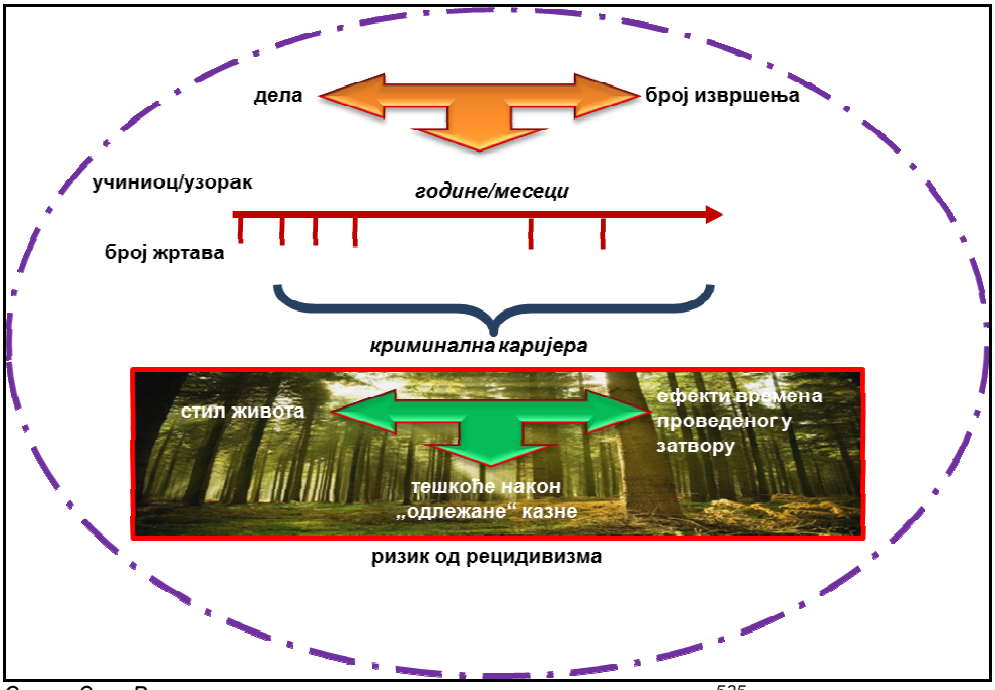


Слика 8. Рецидивизам учинилаца кривичних дела[533]

Све је учесталије проучавање и праћење ризика рецидивизма (низак, средњи или висок). У Филаделфији је развијена посебна техника *Random Forest Modeling*534, која у обзир узима податке организоване у „класификациона и регресиона стабла“ „стотине носилаца појединачних стабала“. У процес изградње стабла је укључен рачунар који путем алгоритма, на основу насумичних показатеља и понављањем процеса из неколико стотина стабала, омогућује добијање једног исхода. За добијање прогнозе у одређеном времену узима се иста таква серија из прошлости (нпр. уколико се жели прогноза за наредних 5 година узимају се подаци из претходних пет или више година). Јединица предвиђања *(unit of prediction*) је везана за крај временског периода (*time horizon*).

533 Payne J. (2007), op.cit;

534 Ritter N. (2013), Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise, NIJ Journal / issue no. 271, February 2013, https://www.ncjrs.gov/pdffiles1/nij/240696.pdf, приступљено 15.1.2014;



Слика 9. Ризик од рецидивизма учинилаца кривичних дела[535]

Уз уобичајене факторе додаје се и време проведено у затвору[536] праћењем његових ефеката, прихватањем једне од три школе[537]:

затвор = казна[538]
затвор = школа криминала/PhD[539]
затвор = минималистичка интеракција

Праћење овог феномена постаје све интензивније, комплексније и мултидисциплинарно[540].

У Србији се још увек „барата“ само са статистичким подацима. Тако у 2012. години више од трећине учинилаца, 38,9%, било је раније осуђивано (највише за кривична дела против имовине 36,5%, а најмање против изборних права 0,008%). Од укупног броја раније осуђиваних лица скоро 10% су жене.

535 Payne J. (2007), op.cit;

536 Murphie A. Wilkins M. Measuring the effectiveness of prison sentences in England and Wales, http://www.justice.gouv.fr/art_pix/MurphieWilkins.pdf, приступљено 15.1.2014;

537 Goggin G.P.C. Cullen T.F. (1999), The Effects of Prison Sentences on Recidivism, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ffcts-prsn-sntncs-rcdvsm/index-eng.aspx, приступљено 15.1.2014;

538 Stuart H. (2003), On the Effectiveness of Prison as Punishment, http://www.is.wayne.edu/StuartHenry/Effectiveness_of_Punishment.htm, приступљено 15.1.2014;

539 Pritikin H.M. (2009) Is prison increasing crime?, Wisconsin Law Review, 1/5/2009, pp. 1050–1108, http://hosted.law.wisc.edu/lawreview/issues/2008_6/1_-_pritikin.pdf, приступљено 15.1.2014;

540 Kropotkin P. (1927), Prisons and Their Moral Influence on Prisoners, http://dwardmac.pitzer.edu/anarchist_archives/kropotkin/revpamphlets/prisonsmoral.html, приступљено 15.1.2014;

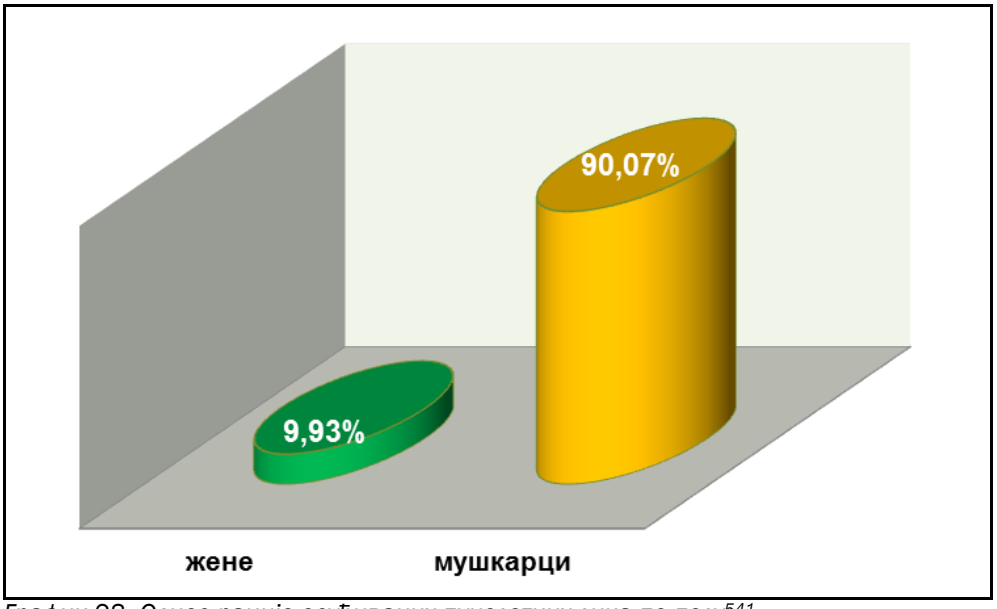


График 28. Однос раније осуђиваних пунолетних лица по полу[541]

Овакав проценат и заступљеност рецидивизма лежи у дејству унутрашњих фактора[542] (кривична и животна историја, детињство, образовање и запошљавање, финансије, породица, смештај, коришћење слободног времена, пријатељи, употреба алкохола и дрога, ментално здравље, ставови)[543]. Породично стање се огледа и по заступљености кривичних дела - поред дела против имовине највише су заступљена дела против здравља људи и брака. Друга група су спољни фактори[544], од којих су кључни: општа економска ситуација у Републици Србији, казнена политика, изостанак објективног система аболиције и помиловања[545]. Посебно је значајан систем аболиције и помиловања, односно њихов изостанак, што утиче на формирање става да ће се без обзира на тежину извршених кривичних дела казне

541 Република Србија, Републички завод за статистику, (2013), op. cit;

542 Probation & Welfare Service, Assessing the Risk of Re-offending, http://www.probation.ie/pws/websitepublishing.nsf/attachmentsbytitle/Assessing+Risk+of+Re-offending/$file/Assessing+Risk+of+Re-offending.pdf, приступљено 15.1.2014;

543 Brunton-Smith I. Hopkins K. (2013), The factors associated with proven re-offending following release from prison: findings from Waves 1 to 3 of SPCR, Results from the Surveying Prisoner Crime Reduction (SPCR) longitudinal cohort study of prisoners), http://socialwelfare.bl.uk/subject-areas/services-client-groups/adult-offenders/ministryofjustice/157543re-offending-release-waves-1-3-spcr-findings.pdf, приступљено 16.1.2014;

544 Håkansson A. Berglund M. (2012), Risk factors for criminal recidivism – a prospective follow-up study in prisoners with substance abuse, http://www.biomedcentral.com/1471-244X/12/111, приступљено 16.1.2014;

545 Цветковић С. (2009), Прилог проучавању амнестија и аболиција политичких осуђеника у Југославији 1944–1980, Архив, часопис Архива Југославије, 1–2, 2009, стр. 120–132, www.arhivyu.gov.rs/index.php?download; Miladinović D, 2007, Institut pomilovanja u svetlu restorativne pravde, Temida, мај 2007, str 37-45, http://www.doiserbia.nb.rs/img/doi/1450-6637/2007/1450-66370701037M.pdf, приступљено 16.1.2014;

скратити, учиниоци пустити из затвора раније или аболирати[546], чиме је изостала превентивна улога санкција.

У Великој Британији са Велсом ситуација је следећа[547]:

- у периоду од јула 2010. до јуна 2011. године сваки четврти учинилац, који је издржавао затворску казну или је пуштен из притвора, извршио је ново кривично дело у року од годину дана. Стопа повратa је расла за 0,5% у односу на претходних 12 месеци (мада се од 2000. године бележи пад од 1%);
- сваки од ових учинилаца је у просеку извршио 2,88 кривична дела у поврату, 82% су извршена од стране одраслих и 18% од малолетника;
- више од половине (56,5%) учинилаца имало је 11 или више претходно извршених дела;
- 0,7% су озбиљна насилна сексуална дела у поврату која су доказана.

Ова појава прати се и у другим државама, поготово у току светске економске кризе због које су почела „пребројавања“ различитих трошкова у националном буџету. САД је то приказао у посебној студији коју је издао *The Pew Center on the States* 2011. године под називом *State of Recidivism April 2011 The Revolving Door of America's Prisons*[548]. За период 1999 – 2004. године „затворски бум“ показује стални пораст у 33 федералне државе (13,5%). Број пуштених затвореника је повећан у 29 држава, а смањен у четири. Стопа рецидива лица пуштених из затвора повећана је за 11,9%. У 33 државе у 1999. Години, 45,4% затвореника пуштених из затвора поново је затворено у року од три године. Јута има највишу стопу рецидива (65,8%). У још пет држава током периода праћења вратило се у затвор више од половине ослобођених затвореника. Најнижу стопу рецидива (24,1%) имала је Оклахома.

Када су у питању учиниоци cyber криминала у Србији, 77% није било раније осуђивано, између осталог и зато што су ова кривична дела уведена у кривично законодавство тек 2005. године.

546 Нпр. председници Републике су у току својих мандата аболирали или помиловали бројне учиниоце, међу њима и познате личности као што су и Драган Џајић, Вучко Манојловић (осуђен за силовање који је након пуштања поново учинио исто кривично дело), Лука Бојовић;

547 Ministry of Justice, (2014), Proven Re-offending Statistics Quarterly Bulletin July 2010 to June 2011, England and Wales, https://www.gov.uk/.../proven-reoffending-statistics-april-2011-march-2012, приступљено 16.3.2014;

548 The Pew Center on the States, (2011), State of Recidivism, The Revolving Door of America's Prisons, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/sentencing_and_corrections/State_Recidivism_Revolving_Door_America_Prisons%20.pdf, приступљено 16.1.2014;

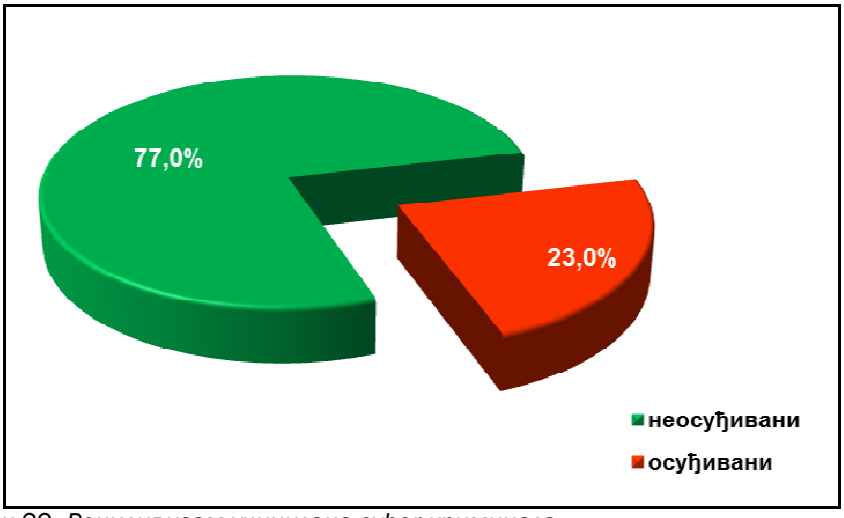


График 29. Рецидивизам учинилаца cyber криминала

Од 23% учинилаца, који су били раније осуђивани, 55,6% је било осуђивано само једном, 19,4% више пута, док за 25% осуђиваних нема података о осуђиваности (не зна се да ли су осуђивани једном или више пута).

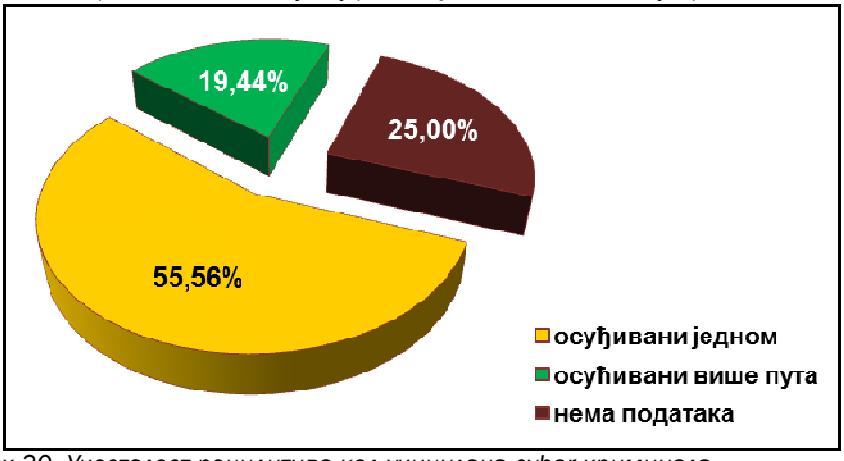


График 30. Учесталост рецидитива код учинилаца cyber криминала

Разлози за ову стопу рецидивизма у почетку су били, између осталог, недовољна припремљеност истражних и правосудних органа да се суоче са овим феноменом. То је утицало на стварање „општег мњења“ код учинилаца да су супериорни и да зато могу проћи некажњено, услед неразумевања надлежних органа начина извршења и мотива. Ништа мање значајно није било и подстрекивање одређених учинилаца (нпр. хакера) од стране државе. Кад се та улога државе изгубила и кад се увећао ниво обучености истражних и правосудних органа ситуација је почела да се мења.

На Тајвану стопа рецидивизма је виша него у Србији (30%) иако се прате само cyber преваре и дела злоупотребе рачунара. Ради смањења стопе

рецидивизма израђују се модели од којих је посебно значајан модел којим се симулирају параметри, међу којима је и рецидивизам праћењем стопе пенетрације доступне компјутерске мреже и понашања учинилаца cyber криминала.

Табела 19. Симулација рецидивизма за параметре cyber криминала на Тајвану[549]

Параметар	*Симулација рецидивизма*
e-Crime report rate from victim	20%
Recidivism rate	30% (24% for Cyber Fraud, 6% for Offense of Computer Usage)
e-Crime transfer rate	6% CF to OCU and 15% OCU to CF

С друге стране, растао је степен образовања учинилаца кривичних дела. Међусобни однос стручне спреме и осуђиваности према коефицијенту контингенције представља ниску повезаност, док се веза нивоа образовања и осуђиваности сматра статистички значајном.

Табела 20. Однос рецидивизма и нивоа образовања учинилаца cyber криминала

		Рецидивизам		*Тотал*
		Осуђивани	Неосуђивани	
Ниво образовања	Без школе	33,33%	66,67%	100%
	Основна школа	40,00%	60,00%	100%
	Средња школа	25,53%	74,47%	100%
	Виша школа	60,00%	40,00%	100%
	Факултет		100%	100%
	Докторат		100%	100%

У већини случајева неосуђиваних је процентуално било више у односу на осуђиване са истим нивоом образовања, изузетак су они са вишом школом којих има више у категорији осуђиваних.

549 Chiu Y.D. Wang S.C. Chung T.T. (2010), Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach, Academy Publisher, Journal of software, vol. 5, no. 12, December 2010, pp. 1349–1354, www.*ojs.academypublisher.com*, приступљено 16.1.2014;

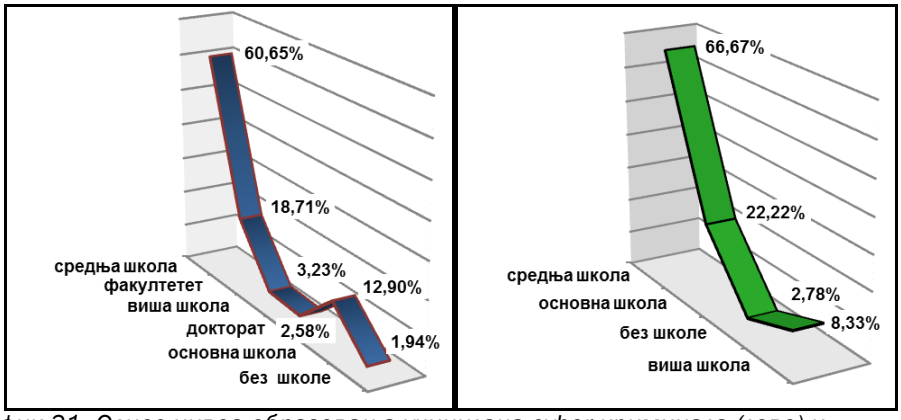


График 31. Однос нивоа образовања учинилаца cyber криминала (лево) и учинилаца cyber криминала са рецидивом (десно) у Србији

Нешто мање од четвртине раније осуђиваних за cyber криминал је завршило само основну школу (22,2%), док нешто више од две трећине има средње образовање (66,7%). Када се упореде ови подаци са подацима о учиниоцима овог криминала уопште, виде се одређена одступања: већи проценат (нпр. учинилаца са средњом школом са рецидивом него код укупног броја) и изостанак учинилаца са факултетом и докторатом, може бити последица њихове развијеније свести о штетности криминалног понашања или веће заокупљености у решавању „легалних“ проблема[550], као и бољег радног и финансијског статуса. Треба додати и већу потребу за самодоказивањем код појединаца са средњом и основном школом, као и оних без школе, али и за већим конформизмом и индолентношћу других, поготово са факултетом и докторатом [551].

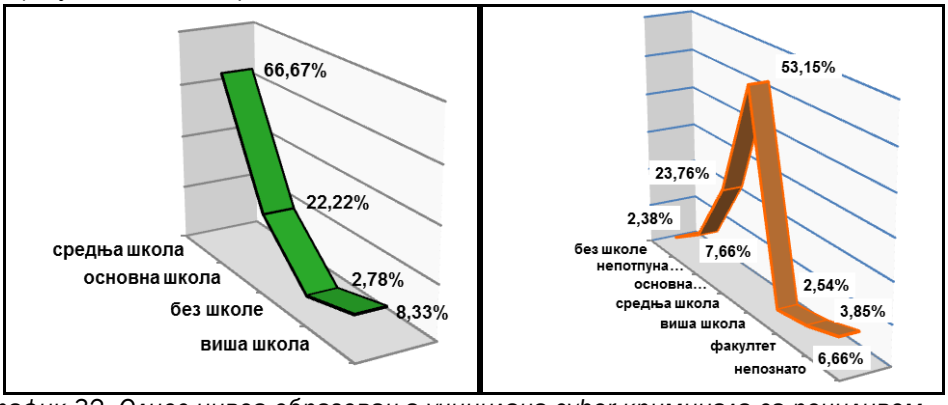


График 32. Однос нивоа образовања учинилаца cyber криминала са рецидивом (лево) и другог криминала са рецидивом (десно)

550 Stewart B.E. (2008), School Structural Characteristics, Student Effort, Peer Associations, and Parental Involvement, The Influence of School- and Individual-Level Factors on Academic Achievement, http://olms.cte.jhu.edu/olms/data/resource/3890/School%20Structural%20Characteristics.pdf, приступљено 16.1.2014;

551 Australian Social Trends, (2013), Characteristics of higher education students, http://www.abs.gov.au, приступљено 16.1.2014;

И у овим групама јасно је изражен тренд повећања учешћа учинилаца са средњом школом (мада је виши код учинилаца cyber криминала са рецидивом него код других облика криминала). Распоред је исти и кад су у питању учиниоци са основном школом, а разлике су нарочито код учинилаца са факултетом и докторатом, којих нема међу учиниоцима cyber криминала са рецидивом, али их има међу неосуђиваним учиниоцима. У овој групацији највише их је са средњом, а најмање са вишом школом, односно без школе. Од оних који нису претходно осуђивани нешто мање од две трећине их је са завршеном средњом школом (58,8%) и нешто мање од четвртине са високим образовањем (24,4%).

Табела 21. Учиниоци cyber криминала без рецидива по нивоима образовања

	Ниво образовања						Тотал
	Без школе	Основна школа	Средња школа	Виша школа	Факултет	Докторат	
Неосуђивани	1,68%	10,08%	58,82%	1,68%	24,37%	3,36%	100%

Као и у претходним укрштањима и у односу на групе дела cyber криминала са осуђиваношћу учинилаца, види се да коефицијент контингенције представља ниску повезаност, а везе су статистички значајне.

У односу између осуђиваних и неосуђиваних највише је разлика између учинилаца дела против слобода и права човека (16%:84%), а најмање против интелектуалне својине (45,8%:54,2%). Равномерност постоји код учинилаца кривичних дела против имовине (50%:50%).

Табела 22. Однос рецидивизма и група дела cyber криминала у Србији

		Рецидивизам		Тотал
		Осуђиван	Није осуђиван	
Група дела cyber криминала против	Слобода и права човека	16,00%	84,00%	100%
	Интелектуалне својине	45,83%	54,17%	100%
	Полне слободе	10,00%	90,00%	100%
	Безбедности рачунарских података	30,95%	69,05%	100%
	Имовине	50,00%	50,00%	100%
	Уставног уређења	33,33%	66,67%	100%
	Правног саобраћаја		100%	100%
	Привреде		100%	100%

Нешто мање од трећине (30,6%) осуђиваних за дела cyber криминала у Србији је извршило дело против интелектуалне својине, док је 36,1% извршило дело против безбедности рачунарских података. Највећи део (37,8%) учинилаца, који нису претходно осуђивани, извршили су дело против полне слободе, а четвртина (24,4%) од укупног броја је извршила дело против безбедности рачунарских података.

Табела 23. Однос група дела cyber криминала и рецидивизма у Србији

		Група дела cyber криминала против								Тотал
		Слобо-да и права човека	Инте-лекту-алне својн-не	Полне слобо-де	Безбе-дности рачуна-рских пода-така	Имо-вине	Устав-ног уре-ђења	Прав-ног саобра ћаја	Прив-реде	
Реци-див-изам	Осуђи-ван	11,11%	30,56%	13,89%	36,11%	5,56%	2,78%			100%
	Није осуђи-ван	17,65%	10,92%	37,82%	24,37%	1,68%	1,68%	0,84%	5,04%	100%

Међусобни однос између служења војног рока и осуђиваности према коефицијенту контингенције показује веома ниску повезаност и према степену значајности сматра се статистички незначајним. Ипак, неопходно је приказати податке како би се могао пратити и овај показатељ. Посебно треба напоменути да је у Републици Србији престало обавезно служење војног рока од јануара 2011. године чиме се прекинула двовековна традиција (од 1807. односно 1836. године). Истим Законом о војсци[552] уведена је могућност да и жене служе војску.

Више од две трећине осуђиваних за дела cyber криминала су служили војни рок (69,4%).

Табела 24. Однос рецидивизма и служења војног рока у Србији

		Рецидивизам		Тотал
		Осуђивани	Неосуђивани	
Служење војног рока	Женске особе		100,00%	100%
	Служио	27,47%	72,53%	100%
	Није служио	22,92%	77,08%	100%
	Ослобођен		100,00%	100%

Нешто више од петине учинилаца ових дела, који су раније били осуђивани, служили су војни рок. Од неосуђиваних више од половине (55,5%) га је служило. Међу њима су и жене. Иако малобројне (9,24%) ипак их је више него оних који су били ослобођени служења (4,2%).

552 Закон о војсци;

Табела 25. Однос служења војног рока и рецидивизма учинилаца дела cyber криминала у Србији

		Служење војска				Тотал
		Женске особе	Служио	Није служио	Ослобођен	
Рецидивизам	Осуђивани		69,44%	30,56%		100%
	Неосуђивани	9,24%	55,46%	31,09%	4,20%	100%

Служење војног рока може имати утицаја на прихватање дисциплине, хијерархије, добрих интерперсоналних односа, формирања одређене интрапсихичке основе, поштовања професионалних улога и заједничких предмета и активности[553]. На крају служења војног рока уочава се: повећање блискости чланова заједнице, појачан степен друштвености и социјалне иницијативе, промена мотивације, бољи однос ка заједничким предметима. Често су пријатељства стечена у току служења војног рока за цео живот, па опстају и у криминалним активностима[554]. Истраживања о односу криминала и служења војске указују на различите тенденције. Служење војске за време Другог светског рата деловало је на смањење укључености ветерана у кривичне или делинквентне активности, док су ветерани Вијетнамског рата, који су често злоупотребљавали алкохол и дроге, то наставили и након војне службе. Могуће је да се слично, као са ветранима из Вијатнама, догодило и са учесницима војних, паравојних и цивилних сукоба на територији бивше Југославије деведесетих година прошлог века[555], Наравно, не треба занемарити ни активности државних хакера који су деловали у том периоду.

Пребивалиште је још једна карактеристика која се прати. Коефицијент контингенције и степен значајности показују да је веза између региона/места пребивалишта и осуђиваности ниског интезитета и да статистички није значајна.

Табела 26. Однос рецидивизма и пребивалишта учинилаца дела cyber криминала

		Рецидивизам		Тотал
		Осуђивани	Неосуђивани	
Пребивалиште	Београд и околина	27,12%	72,88%	100%
	Војводина	9,30%	90,70%	100%
	Шумадија и Западна Србија	29,41%	70,59%	100%
	Јужна и Источна Србија	33,33%	66,67%	100%
	КиМ	100%		100%
	БиХ		100%	100%

553 Dedić G. (2003), Kvalitet života vojnika za vreme služenja vojnog roka, Vojnosanitetski pregled, br. 3, str. 305-314;

554 Teachman J. (2008), Military service and the life course: An assessment of what we know, http://www.ncfr.org/ncfr-report/focus/military-families/military-service-life-course-assessment, приступљено 16.1.2014;

555 Међународни кривични суд за бившу Југославију, Тужилац суда против Slobodana Miljkovića познатог и као "Lugar", Blagoja Simića, Milana Simića, Miroslava Tadića познатог и као "Miro Brko", Stevana Todorovića познатог и као "Stiv", "Stevo", "Monstrum", Sime Zarića познатог и као "Šolaja", http://www.icty.org/x/cases/todorovic/ind/bcs/sim-ii950721b.htm, приступљено 16.1.2014;

Утицај регионима, односно места пребивалишта, више је изражен код неосуђиваних него код учинилаца са рецидивом.

Ако се анализирају учиниоци у поврату највише их је из Београда и околине, а најмање из Војводине (не рачунајући КиМ и БиХ).

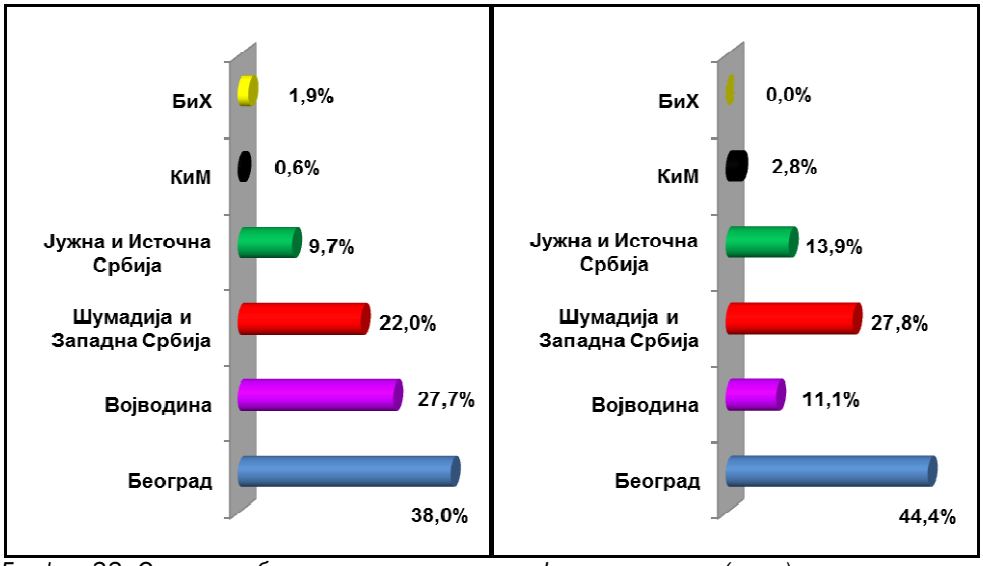


График 33. Однос пребивалишта учинилаца cyber криминала (лево) и учинилаца cyber криминала са рецидивом (десно)

Одступања у процентима између ових категорија указују на то да су учиниоци из Београда најактивнији (38% : 44,4%), слично је и са Шумадијом и Западном Србијом (22% : 27,7%). Раскорак се бележи код Војводине (27,74% : 11,1%).

Табела 27. Однос пребивалишта и рецидивизма учинилаца дела cyber криминала

		Преивалиште						Тотал
		Београд и околина	Војводина	Шумадија и Западна Србија	Јужна и Источна Србија	КиМ	БиХ	
Рецидивизам	Осуђивани	44,44%	11,11%	27,78%	13,89%	2,78%		100%
	Неосуђивани	36,13%	32,77%	20,17%	8,40%		2,52%	100%

Учиниоци ових дела, који нису претходно осуђивани, у највећем броју имају пребивалиште у Београду (36,1%), док их је нешто мање са пребивалиштем у Војводинуи(32,8%).

3.2.10. Начин извршења/број и карактеристике учинилаца cyber криминала

Начин извршења дела са аспекта броја учинилаца cyber криминала и њихове основне социодемографске карактеристике у Србији показују значајну везу[556].

Табела 28. Анализа социодемографских карактеристика и начина извршења кривичног дела

Карактеристике	Сигнификантност	Коефицијент контингенције
Пол	0,029	0,173
Старост	0,021	0,244
Пребивалиште/регион	0,281	0,197
Број становника у месту пребивалишта	0,010	0,280
Ниво образовања	0,116	0,232
Професија	0,055	0,255
Радни статус	0,011	0,260
Имовина	0,270	0,088
Брачни статус	0,443	0,131
Породични статус/број деце	0,514	0,092
Рецидивизам		0,344
Групе дела cyber криминала		0,495

Старост има ниску, али статистички значајну везу са начином извршења ових кривичних дела. Исто је и са пребивалиштем, односно регионом, величином места, као и са радним статусом, имовином и рецидивизмом.

Анализа дела cyber криминала и броја учинилаца указују да су одређена дела овог криминала последица „удруживања ради вршења кривичних дела“[557] и организовања у криминалне групе, односно организованог криминала. При томе се мора имати у виду да организоване групе за овај криминал функционишу на „*stand alone*“ основи са члановима који ретко долазе у директан физички контакт једни са другима[558], тј. чланови су са сопственим мрежама дистрибуираним у разним земљама које су ретко у међусобној „физичкој“ комуникацији[559].

556 Варијабле код којих је сигнификантност мања од 0,05 и коефицијент контингенције између 0,20 и 0,40 представља ниску повезаност. Варијабла група дела cyber криминала има коефицијент контингенције 0,495 што је приближно повезаности средњег интезитета;

557 Кривични законик Републике Србије, члан 346;

558 UNICRI, Cybercrime and Organized Crime, http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/organized_crime/, приступљено 16.1.2014;

559 HM Government, (2013), Serious and Organised Crime Strategy, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf , приступљено 16.1.2014;

Cyber криминал је по *BAE Systems Detica* извештају *John Grieve Centre for Policing and* Security *at London Metropolitan University* увео организовани криминал у *„четврту еру“* и идентификовао шест главних карактеристика организованих група[560]:

- конвергенција он-лајн и оф-лајн светова;
- 80% овог криминала може имати неки облик организованих активности;
- мобилишу се чланови група преко 35 година старости (43%) тако да то више није привилегија младих (свега једна трећина, 29% су испод 25);
- половина група има шест или више чланова, а само једна четвртина се састоји од 11 или вишечланова. Величина група није у корелацији са утицајем и последицама активности – често мали број чланова може да нанесе велику штету;
- 25% активних група су „оперисале“ краће од шест месеци;
- „криминални“ дигитални алати се све више користе и ван група на начин који карактерише „традиционало" криминално понашање (нпр. регрутовање чланова „банде“ или крађа пин кодова).

Табела 29. Однос групе дела cyber криминала и начина извршења

		Група дела cyber криминала против								*Тотал*
		Слобо-да и права човека и грађа-нина	Инте-лекту-алне својн-не	Полне слобо-де	Безбед-ности рачу-нарских пода-така	Имо-вине	Устав-ног уре-ђења	Прав-ног сао-бра-ћаја	Прив-реде	
Начин извр-шења	Групно		22,58%		70,97%				6,45%	100%
	Само-стално	20,16%	13,71%	40,32%	16,13%	3,23%	2,42%	0,81%	3,23%	100%

Укрштање групе дела cyber криминала и начина извршења/броја учинилаца показује да је коефицијент контингенције повезаности средњег интезитета, те је јасно да се ради о статистички значајној вези са средњим интензитетом повезаности.

560 Detica, (2012), op.cit.

У Србији се организоване групе појављују[561]:

- у највећем броју при извршењу дела против безбедности рачунарских података (71%);
- нешто мање од четвртине (22,6%) је извршило дело против интелектуалне својине;
- а 6,4% је извршило дело против привреде.

Код осталих дела cyber криминала није карактеристично удруживање (организовање у групе). Напротив, много више је самосталног извршења:

- највише учинилаца је извршило дела против полне слободе[562] (40,4%);
- петина је (20,2%) извршила дела против слобода и права човека и грађанина;
- нешто више од шестине учинилаца (16,1%) извршило је дело против безбедности рачунарских података;
- најмање је извршено дела против уставног уређења (2,4%), односно имовине и привреде (по 3,2%).

Другим речима, однос између броја извршилаца по групама дела указује на доминантност самосталног извршења, једино је код дела против безбедности рачунарских података превага на групном (организованом) извршењу.

Табела 30. Однос броја учинилаца по групама дела cyber криминала

		Начин извршења		Тотал
		Групно	Самостално	
Група дела cyber криминала против	Слобода и права човека и грађанина		100%	100%
	Интелектуалне својине	29,17%	70,83%	100%
	Полне слободе		100%	100%
	Безбедности рачунарских података	52,38%	47,62%	100%
	Имовине		100%	100%
	Уставног уређења		100%	100%
	Правног саобраћаја		100%	100%
	Привреде	33,33%	66,67%	100%

561 По Извештају МУП-а из 2014. године, op. cit., стр. 24, „Од реализација у овој области издваја се хапшење француског држављанина за којим је била расписана и потерница ИНТЕРПОЛ-а код кога су пронађене четири фалсификоване платне картице, «скимер», 100 бланко пластичних картица; хапшење бугарског држављанина који је поставио «скимере» на девет банкомата у више банака које је оштетио за 30.000 евра; откривање четири лица са подручја АП Војводина која су фалсификованим платним картицама банке "*Citybank USA*" извршила више стотина неовлашћених трансакција на *POS* терминалима својих предузећа и радњи оштетивши банку за преко 15,4 милиона динара; хапшење брокера Брокерско-дилерског друштва из Београда, који је рачунарском преваром и злоупотребом овлашћења прибавио имовинску корист од око 23 милиона динара и око 45.000 евра итд;

Одређене активности су спроведене у области сузбијања пиратерије тако да је у 2013. години, контролисано 345 лица и субјеката. Поднето је 88 кривичних пријава против 86 лица због 102 кривична дела. Одузето је 11.446 пиратских компакт дискова, 801 штампана публикација, 52 техничка уређаја и др."

562 Мада кад је у питању удруживање, односно организовање у групе за ова кривична дела је карактеристичан велики број учинилаца, односно извршилаца.

Уколико се прате карактеристике учинилаца cyber криминала према групама дела, полазећи од заступљености (више од 15%) и укупног броја учинилаца (за кривична дела против безбедности рачунарских података, полне слободе, интелектуалне својине и слобода и права човека и грађанина), може се констатовати следеће:

а) Кривична дела против безбедности рачунарских података

Учиниоци кривичних дела против безбедности рачунарских података су доминантно мушког пола (83%). Скоро две трећине (60%) учинилаца је старости између 25 и 35 година и углавном су из Београда са околином (40,5%) или из градова чији је број становника између 100.000 и 200.000 (36%). Најчешће се њихов степен образовања завршава на средњој школи (57%), док је факултетски образованих 21%. Техничко-технолошким занимањима се бави 29% учинилаца, 26% немају занимање, а за 21% случајева подаци о занимању нису доступни. Као што се могло очекивати запосленост је на ниском нивоу, посао има 24%, док проценат оних који нису у радном односу је вишеструко већи 73%. Брачног друга има 31%, а потомке 9% учинилаца. Војни рок је служило њих 63%. Претходно је осуђивано 31%.

Укрштање ове групе дела cyber криминала и начина извршења/броја извршилаца кривичних дела показује да је коефицијент контингенције приближан средњем интензитету повезаности и да је статистички значајна веза са средњим интензитетом повезаности.

б) Кривична дела против полне слободе

Од 2006. године Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Министарства унутрашњих послове Републике Србије и Одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду поднели су 156 кривичних пријава против 168 лица која су извршила кривично дело *приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију* (члан 185) и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б). У највећем броју случајева подношене су кривичне пријаве због дистрибуције наведеног материјала путем интернета. У кривичном гоњењу учинилаца овог кривичног дела интензивно се сарађивало са другим полицијским службама других земаља. Нарочито успешна и континуирана је била сарадња са Интерполом[563] у размени оперативних података о сајтовима и сервисима

563 UN Economic and Social Council Commission on Crime Prevention and Criminal Justice, (2013), International cooperation in combating transnational organized crime and corruption Report of the Secretary-General, http://www.coe.int/t/dghl/standardsetting/CDPC/PC-GR-COT/ECN.15_2013_4.pdf; Ruyver B., Vermeulen G., Beken T., (2013), Strategies of the EU and the US in Combating Transnational Organized Crime, http://books.google.rs/books?id=O94gPcnKQAwC&pg=PA208&lpg=PA208&dq=cyber+transnational+organized+crime+cooperation&source=bl&ots=ohum9m2gbt&sig=oMmUy6MzJJxW6JTS3yKkx1lcNlo&hl=sr&sa=X&ei=fDVGU6LNNobIsgapi4H4Bw&ved=0CFYQ6AEwCQ#v=onepage&q=cyber%20transnational%20organized%20crime%20cooperation&f=false, приступљено 17.1.2014;

на интернету преко којих су се објављивали, размењивали или продавали забрањени садржаји[564].

Сва кривична дела против полне слободе као групе дела cyber криминала у Србији извршили су мушкарци. До сада није забележено да је било учинилаца женског пола. Они су углавном мушкарци преко 45 година живота (34%) и између 25 и 45 година (30%). Већина је из Војводине (40%), па из Београда и околине (22%). Пребивалиште у местима изнад 200.000 становника има 40% учинилаца. Образовање код ове групе учинилаца је слично као и код осталих, половина их има завршену средњу школу, а факултет има 24% учинилаца. Забележени су и случајеви у којима учиниоци имају докторат. Са техничко-технолошким занимањима је скоро трећина (30%) учинилаца. Запослених има мање (44%) него незапослених. Имовину поседује 22% учинилаца. Многи учиниоци овог дела имају формирану породицу, у брачној су заједници, разведених је 81%, а 9% живе у ванбрачној заједници. Децу има нешто мање од половине (44%) учинилаца. У овој групи 28% учинилаца је ослобођено служења војног рока (болест, инвалидитет), док је 64% одслужило. Осуђивано је 28% учинилаца од којих је 4% осуђивано више пута.

в) Кривична дела против интелектуалне својине

Већина дела против интелектуалне својине везана је за нелегалну продају неовлашћено наснимљених примерака ауторских дела на мултимедијалне носаче и њихову даљу препродају крајњим корисницима (улична продаја, продаја преко организоване мреже препродаваца широм територије Републике Србије и друго). У једном броју случајева Одељење за борбу против високотехнолошког криминала поднело је кривичне пријаве против извршилаца кривичних дела који су неовлашћено оглашавали продају наснимљених примерака филмова, серија, музике и рачунарских програма преко интернет сајтова, путем огласа, а затим те примерке, без знања и овлашћења носилаца ауторских права дистрибуирали широм Републике Србије. Поред овог било је и других начина извршења, као што је дистрибуција заштићених ауторских дела путем *P2P* мрежа (*Peer to Peer*) и путем *FTP* сервера (*File Transfer Protocol*).

Карактеристике учинилаца дела *неовлашћеног искоришћавања ауторског дела и предмета сродног права* (члан 199 Кривичног законика) су следеће: 96% су мушког пола, углавном између 25 и 35 година (37,5%) и са пребивалиштем у великим градовима (67%). Средње су образовани (67%), нису запослени (63%) и ни један нема имовину. У браку је 42%, 37% има до троје деце, а више од троје деце има њих 8%. Војску је служило 65%. Раније је осуђивана скоро половина (46%), од тога: 72% је осуђивано само једном, а 28% више пута. Најчешћи мотив извршења дела је новац.

564 МУП Републике Србије, 2014, Информатор о раду Министарства унутрашњих послова Републике Србије, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/informator;

г) **Кривична дела против слобода и права човека и грађанина**
Одељења која се боре против cyber (високотехнолошког) криминала поднела су 25 кривичних пријава против лица која су извршила дело *угрожавања сигурности* (члан 138 Кривичног законика). Ово кривично дело извршено је преко интернет сајтова, на друштвеним мрежама (*Facebook*), као и путем електронских порука. Извршиоци су упућивали поруке чији садржај представља озбиљну претњу појединцима и групама.
Карактеристике учинилаца дела су: 96% су мушкарци из Београда и околине; 44% има пребивалиште у градовима са више од 200.000 становника. Већина је завршила средњу школу (72%). Скоро половина је запослена (48%), али нема имовину. Углавном немају брачни статус (76%) и немају децу. Пошто је већина млађа од 25 година, нису служили војску. Мало их је претходно осуђивано (16%) и то само једном.

Компаративном анализом добијају се заједничке и специфичне особености учинилаца cyber криминала. Само су три карактеристике заједничке: **сви су неосуђивани мушкарци са средњом школом**.

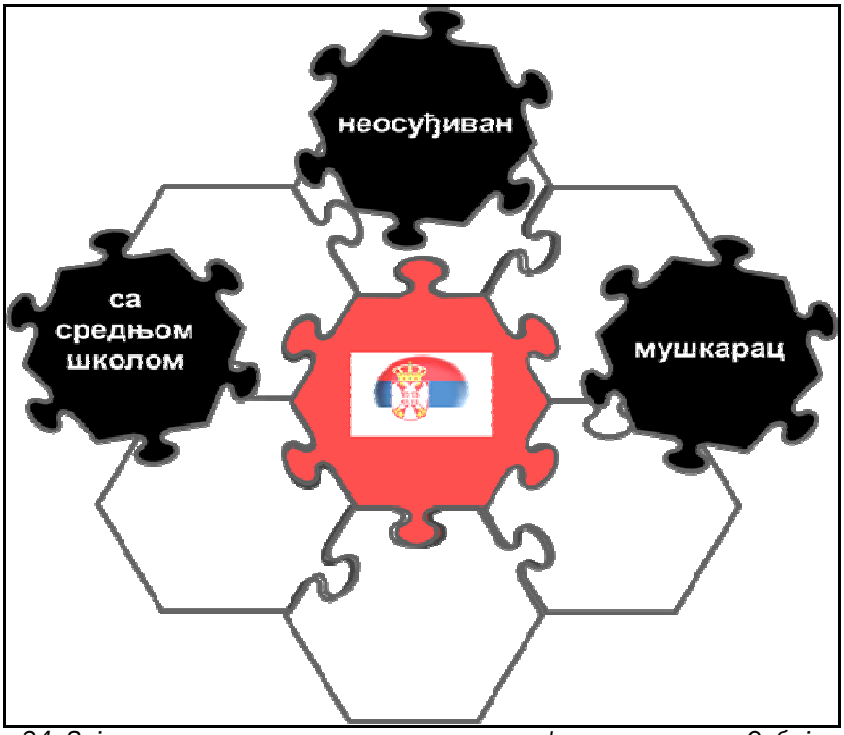


График 34. Заједничке карактеристике учинилаца cyber криминала у Србији

Разлике су у осталим карактеристикама:

- године старости се крећу у оквиру 3 групе: између 18 и 25, између 25 и 35 и преко 45 година;
- учиниоци најчешће потичу из Београда са околином, из великих градова или из Војводине;
- имају децу исто колико и немају;
- већина је ожењена;
- махом су незапослени;
- већина је служила војску.

Што се броја учинилаца тиче углавном се то реализује самостално.

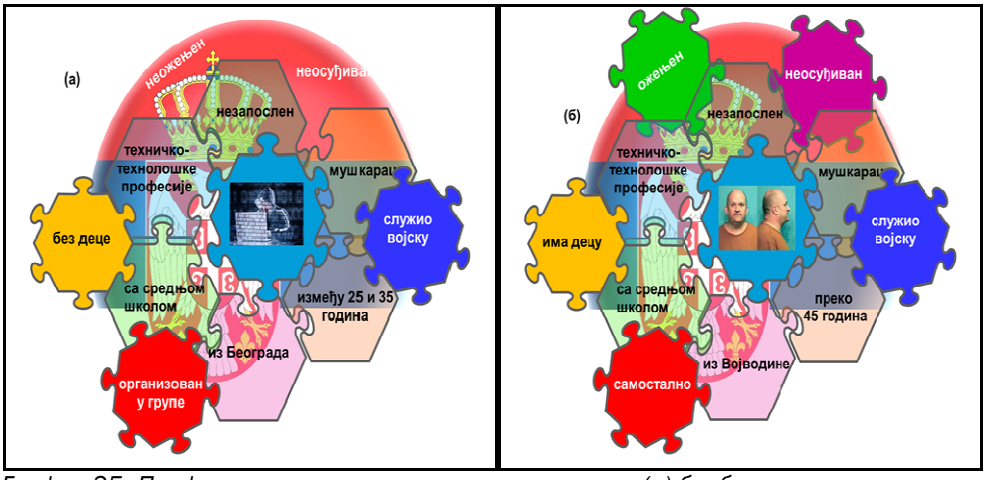


График 35. Профил учинилаца кривичних дела против: (а) безбедности рачунарских података, (б) полне слободе

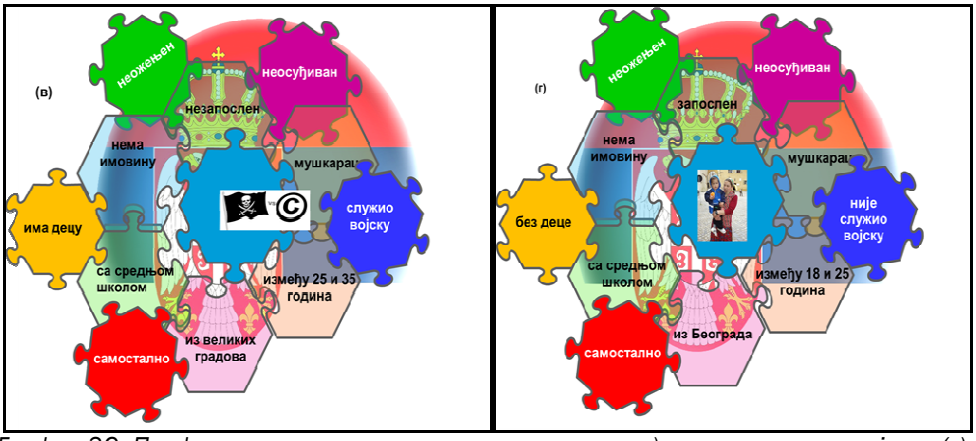


График 36. Профил учинилаца кривичних дела против: в) интелектуалне својине, (г) слободе и права човека и грађанина

3.3. Ставови према појединим делима cyber криминала у Србији

Ставови појединаца, друштвених (интересних) група, креатора политике и друштва према одређеној појави и феномену формирају се на основу различитих показатеља, односно елемената. Три су кључна елемента од којих зависи формирање ставова: емоционални, когнитивни и везани за понашање[565]. Посебно су значајни ставови према криминалу, казнама[566] и истраживањима везаним за њих. Како истичу *Gray, Jackson, Farrall*[567]*, к*риминолошка истраживања ставова највише су окренута негативним емоционалним реакцијама - страху, забринутости и анксиозности. Иако је страх од криминала или страх од злочина код појединаца, нарочито жртава, стар колико и сам криминал, ова истраживања трају само пола века (60-те године XX века у САД-у) студиозног рада и изградње методологије који треба да доведу до његове суштине. Почетне позиције су различите и крећу се од страха од криминала као друштвеног проблема, смањења квалитета живота и здравља, до покушаја прављења мапе страха – нивоа, трендова и друштвених локација[568]. Полазне основе су биле превасходно везане за виктимизацију криминала, да би касније почеле да се окрећу и другим аспектима (економским, демографским и сличним)[569] и то тако што су се са квантитативног[570] усмериле ка квалитативним мерењима и са социолошких ка мултидисциплинарна. Посебна мултидисциплинарна истраживања вазана су за узроке и последице тог страха[571], за перцепцију криминала од стране јавности и за ризике од њега, као за депресију и опште неповерење које криминал изазива. Почеле су да се повезују одређене карактеристике (демографске, националне, етничке, расне, и слично), као и друштвена обележја испитаника[572]. Заначајни су пол (више код жена) и старост

565 Cherry K. (2014), Attitudes How Attitudes Form, Change and Shape Our Behavior, http://psychology.about.com/od/socialpsychology/a/attitudes.htm; Schwarz N., Bohner G., (2001), The Construction of Attitudes, http://sitemaker.umich.edu/norbert.schwarz/files/schwarzz___bohner_attitude-construction-ms.pdf, приступљено 17.1.2014;

566 Hough M. Roberts J. (1998), Attitudes to punishment: findings from the British Crime Survey, http://www.icpr.org.uk/media/10372/Attitudes%20to%20punishment,%20hors179.pdf; Paulin J., Searle W., Knaggs T., (2003), Attitudes to Crime and Punishment: A New Zealand Study, http://www.rethinking.org.nz/assets/Newsletter_PDF/Truth_in_Justice/V2/Auckland_Uni_Attitudes_crime_punishment.pdf, приступљено 17.1.2014;

567 Gray E, Jackson J. Farrall S. (2009), In Search of the Fear of Crime: Using Interdisciplinary Insights to Improve the Conceptualisation and Measurement of Everyday Insecurities;

568 Moore H.M. Trojanowicz C.R. (1988), Policing and the Fear of Crime, U.S. Department of Justice National Institute of Justice, Perspectives of Policing, no.3, pp.1-8;

569 Jackson J. Farrall S. Gadd D. (2004),Filtering Fear?, On the Use of Filter and Frequency Questions in Crime Surveys, http://www.lse.ac.uk/socialPolicy/Researchcentresandgroups/mannheim/JonJackson/FilteringFear.pdf, приступљено 17.1.2014;

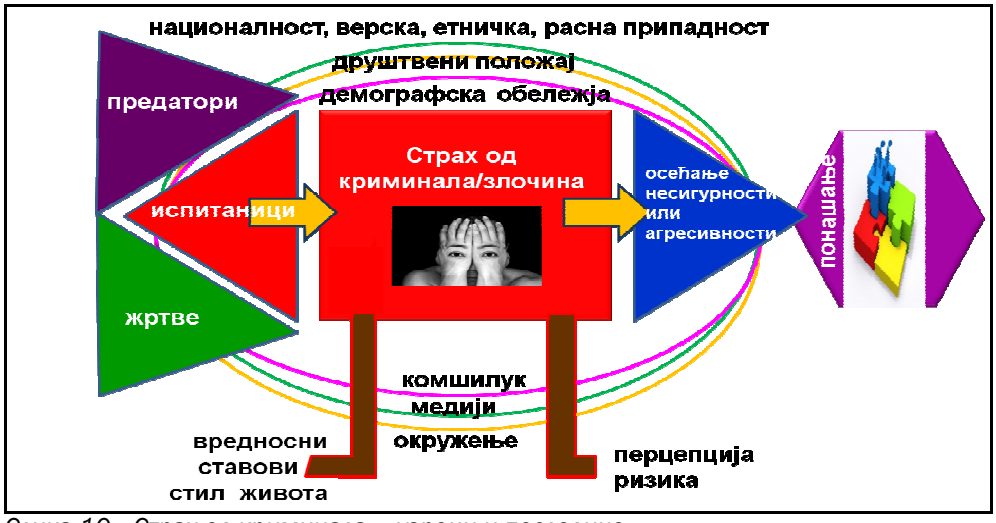
570 Tulloch M. (1998), Quantitative Review, едиција Fear of Crime, volume 1, www.ncavac.gov.au;

571 Garofalo J., (1981), The Fear of Crime: Causes and Consequences, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6243&context=jclc, приступљено 17.1.2014;

572 Fox A.K. Nobles R.M. Piquero R.A., (2009), Gender, crime victimization and fear of crime, Security Journal, vol. 22, 1, pp. 24/39;

(више код старијих од 65 година) као основни (оправдани) индикатори страха[573], а потом се он мање, нагомилава код одређених категорија по обрзовном нивоу, месту становања (пребивалишта), брачном статусу, имовинском или радном статусу или друштвеном положају и националној, верској, етничкој или расној припадности одређеним групама. Поред ових индикатора утицај на формирање, односно подизање страха, имају и утицаји из окружења. Бројни аутори истичу да је комшилук та мини локална заједница у којој појединци живе и стварају „погодности“ за формирање страха од криминала. Сликовито названа **теорија разбијених прозора**[574] каже - ако су у комшилуку као окружењу изражени знаци нереда, незадовољства, маргиналности, слабе социјалне кохезије (насеља у којима доминирају празне зграде сломљених прозора, графити, опасност за полицајце да улазе у њих, велике количине ђубрета, по *Wilson*-у и *Kelling*-у, су „рањиви на криминалне инвазије“) у њему расте и страх од криминала. Овако формиран страх доводи до осећања несигурности, али и агресивности, а тиме дефинише и карактеристична понашања[575].

Страх и перцепција криминала у јавности, под утицајема медија[576], стварају *perpetum mobile* ефекат, проузрокујући моралну панику (нпр. према одређеним „криминогеним групама и појединцима“)[577].



Слика 10. Страх од криминала – узроци и последице

573 Scarborough K.B. Like-Haislip Z.T. Novak J.K. Lucas L.W. Alarid F.L. (2010), Assessing the relationship between individual characteristics, neighborhood context, and fear of crime, Journal of Criminal Justice, no. 38, pp. 819–826;

574 Wilson J. Kelling G. (1982), Broken windows: Atlantic Monthly, no.211, 29–38;

575 Roberts L.D. Indermaur D. (2012), Are Neighbourhood Incivilities Associated with Fear of Crime?, ed. Australia: Identity, Fear and Governance in the 21st Century, http://press.anu.edu.au/apps/bookworm/view/Australia%3A+Identity%2C+Fear+and+Governance+in+the+21st+Century/10171/cover.html, приступљено 17.1.2014;

576 Gomes S. Machado H., (2011), Media's made criminality: the construction of moral panic over gypsies and immigrants, http://www.inter-disciplinary.net/wp-content/uploads/2011/02/gomesppaper.pdf, приступљено 17.1.2014;

577 Sands L. (1998), Moral Panics, http://www.aber.ac.uk/media/Students/lcs9603.html, приступљено 17.1.2014;

Како истиче *Jackson*[578]*,* будућа истраживања треба да као **први циљ** испитају емоције и психологију ризика, односно: а) да ли су емоције и спознаја интерактивне или независне категорије при процени опасности за појединца и б) да ли су појединачне слике ризика од фундаменталног значаја за истраживање ризика и јавне анксиозности. **Други циљ** је утврђивање: а) како се презентација кривичног догађаја коју је доживео појединац претвара у његову личну слику ризика и б) како масовни медији стварају осећај распрострањености и природе криминала. Даље, ова истраживање могу утврдити и општије ставове према социјалној кохезији и друштвеним променама у одређеним заједницама или друштву. Страх може, с тога, бити изражен као искуствени феномен. Перцепција ризика је важан део ставова јавности, али и потпунијег разумевања психологије ризика и његовог културолошког значаја[579]. Наравно, резултати таквих истраживања могу касније постати основ за дефинисање националних стратегија, на пример, борбе против криминалаи превенције од криминала[580].

Пример истраживања у региону је пројекат **Страх од криминала у великим градовима** спроведен 2009. године, у главним градовима бивших југословенских република (Београд, Загреб, Љубљана, Сарајево и Скопље)[581] или током 2011. године **Страх од криминала међу студентима Правног факултета у Сплиту**[582]. У оба ова истраживања пошло се од социолошког и криминолошког аспекта феномена страха и пратила се линија теорија[583,] концепата[584] и модела[585] који га објашњавају. Узори су била међународна[586] и национална[587] истраживања.

---

578 Jackson J. (2006), Introducing Fear of Crime to Risk Research, Risk Analysis, Vol. 26, No. 1, pp. 253–264;

579 Chadee D. (1999), Fear of Crime, Safety and Community Integration: Another Fear-Safety Paradox? https://www.jiscmail.ac.uk/.../filearea.cgi, приступљено 17.1.2014;

580 Такав је документ Национална стратегија превенције криминала (Republika Srbija, Ministarstvo unutrašnjih poslova, (2009), Polazni okvir Nacionalne stretegije prevencije kriminala, http://www.bezbednost.org/upload/document/polazni_okvir_nacionalne_strategije.pdf), приступљено 18.1.2014;

581 Ђурић С. Поповић-Ћитић Б. (2013), Страх од криминала, родне разлике у перцепцији ризика, Социолошки преглед, vol. XLVII (2013), no. 4, стр. 537–554;

582 Getoš A.M. Giebel S. (2012), Strah od kriminala među studentima pravnog fakulteta u Splitu, Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012., str. 533.- 552;

583 Lee M. (2001), The Genesis of `Fear of Crime', Theoretical Criminology November 2001 vol. 5 no. 4, 467-485; *Criminol J.* (2010), Functional Fear and Public Insecurities About Crime, British Journal of Criminology, 50 (1) 1-22; Jackson J. Gousetl I. (2013), Fear of Crime, http://www.academia.edu/1815559/Fear_of_Crime_An_Entry_to_the_Encyclopedia_of_Theoretical_Criminology, приступљено 18.1.2014;

584 Нпр. Теорија моралне панике, Cohen S. (2002), Folk Devils and Moral Panics: The Creation of the Mods and Rockers, 3rd Edition, London, Routledge по Krinsky C., (2010), Introduction: The Moral Panic Concept, http://www.ashgate.com/pdf/SamplePages/Ashgate-Research-Companion-to-Moral-Panics-Intro.pd;

585 Garofalo J. (1981), op. cit., pp. 839 – 857;

586 Нпр. International Crime Victims Survey (UNICRI, http://www.unicri.it/services/library_documentation/publications/icvs/; European Crime Prevention Network, (2004), A Review of Scientifically Evaluated Good Practices For Reducing Feelings of in Security or Fear of Crime in the EU Member States, http://www.eucpn.org/pubdocs/review_reducing_feelings_insecurities_fear_crime_en.pdf, приступљено 18.1.2014;

587 Нпр. Attitudes to punishment: findings from the British Crime Survey, http://www.icpr.org.uk/media/10372/Attitudes%20to%20punishment,%20hors179.pdf; Attitudes to Crime and Punishment:

Истраживања забринутости, односно страха од криминала, перцепција јавности о криминалу и ризицима све више се усмеравају на поједине облике (организовани, транснационални, насилни, економски и слично)[588]. У првој половини 2000-тих почињу и прва праћења феномена cyber страха који је пун митова[589] и предрасуда. *Olm*[590] са својим митом о супер кориснику[591] (*folk devil*[592]) и *Wall*[593] са „реториком против реалности" истичу да се као митови који изазивају панику и моралну панику појављују:

A New Zealand Study, http://www.rethinking.org.nz/assets/Newsletter_PDF/Truth_in_Justice/V2/Auckland_Uni_Attitudes_crime_punishment.pdf, приступљено 18.1.2014;

588 Mass S. (1982), The Dilemma of the Intimidated Witness in Federal Organized Crime Prosecutions: Choosing Among the Fear of Reprisals, the Contempt Powers of the Court, and the Witness Protection Program, Fordham Law Review. Volume 50 | Issue 4, pp. 582 – 610, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4556&context=flr, приступљено 18.1.2014;

589 Wall D.S. (2008/11), Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime (revised Feb. 2011)', Information, Communication & Society (11): 861–884., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155, приступљено 18.1.2014;

590 Ohm P. (2008), The Myth of the Superuser: Fear, Risk, and Harm Online, UC Davos Law Review, Vol. 41, No. 4, pp. 1327–1402, http://heinonline.org/HOL/LandingPage?handle=hein.journals/davlr41&div= 36&id=&page=, приступљено 18.1.2014;

591 По *Ohm*–у "Супер корисник" је корисник рачунара који поседује моћ коју нема обичан корисник. Он може да контролише или промени рачунаре и мреже на невероватне начине. Супер корисник има тенденцију да има више времена, праксе, знања или приступа алатима од обичног корисника. Алати играју посебно важну улогу и комплексни су. Супер корисник често користи софистициране компјутерске програме (понекад креиране од њих, често креиране од стране других) да стекну моћ;

592 Cohen, S. (2002), op. cit.

593 Wall D.S. (2008b), op. cit., pp. 45-63;

Табела 31. Митови о cyber криминалу

Olm	Wall
Описи супер корисника су истовремено детаљни и нејасани. Опширно се описују догађаји, али изостављају имена, датуми и места потребна за потврду „приче“.	Cyber криминал је драматичан, футуристички и антиутопијски.
У опису супер корисника користе се неодређени придеви. као нпр. "обично", "уобичајено", "често" (нпр. "ујези често мењају постојеће *log-on* програме, тако да се корисничке лозинке копирају у фајл из које касније хакери могу да их преузму")	Cyber простор је патолошки, несигуран и криминоген.
Опис супер корисника се често понављања („као папагаји једни понављају исто што су и други рекли“).	Корисници су слаби и треба да буду заштићени од себе самих.
Опис супер корисника је често хипотетичан (нпр. "могу се замислити ситуације у којима хакери продиру у систем, у шифре података и потом траже новац за одавање кључа за декодирање")	Свемогућ (*darkside*) хакер или „супер корисник“.
	Хакери су постали део организованог криминала.
	Криминалци су анонимни и не могу да се прате.
	Криминалци пролазе некажњено и „извлаче“ се за учињени криминал.
	Постоји више дискурса о cyber криминалу: законодавни-академски-експертски-популарни.
	Дисинтермедијација извора вести и статистичких информација.
	Једно дело се налази „испод“ извештавања/пријављивања других дела од стране жртава.
	Ниски нивои профилисања учинилаца
	Јурисдикцијске разлике у погледу (а) дефинисања cyber криминала и (б) нивоа сарадње између полиција.
	Непостојање заједничких дефиниција cyber криминала.
	Низак ниво знања јавности о ризицима.
	Умрежене технологије доприносе реорганизацији кривичних активности/„рада“ на мрежи
	У три генерације је доживљена еволуција cyber криминала од традиционалног до *sui generis* cyber криминала.
	У cyber криминал спадају три групе кривичних дела са различитим карактеристикама (против интегритета, криминал помогнут рачунарима и везан за садржаје).

Митови су настали из страха, а он, између осталог, и из наразумевања суштине cyber простора и криминала и њих као великих непознаница. Страх од cyber простора се појачао и појавом cyber панка, као специфичне културе и специфичних група као што су *yahooboys* и *sakava,* али и cyber мафије[594] - „сада је cyber криминал царство мафијашких банди, суштински налик на међународни криминал, али уноснији од других, традиционалних, ризичних облика криминала. Они он-лајн лове банкарске идентификације и лозинке, они хакују рачунаре и смарт телефоне или профиле на друштвеним мрежама, као што су *Facebook* или *Twitter.*“[595.] Тај криминал је имао 1 милион жртава сваки дан.

Cyber страх и даље расте са порастом корисника друштваних мрежа, мобилних апликација и *cloud* рачунарства. Његова друга „грана“ је cyber криминал[596] и поједина дела (нарочито хакинг, вируси, крађа идентитета, cyber насиље[597], cyber рат, тероризам, надгледање). Овај се страх прати кроз уобичајене индикаторе, али с обзиром на његову „младост“ они су поједностављени (углавном су више демографски, него сложени). Мапирање и мерење страха, односно његовог интензитета и утицаја на перцепцију друштва постало је пратећа појава уз мерење и тумачење самог cyber криминала[598]. Тако, по студији Европске комисије из 2013. године, око 76% испитаника се слаже да је повећан ризик од постојања жртвама cyber криминала у последњих годину дана. Управо због тога је 70% корисника интернета широм ЕУ уверено у своју способност његовог коришћења за куповину или обављање банкарских трансакција преко мреже, али се само око 50% одлучило да то и уради[599].

---

594 Russian cyber crime market more organized, lucrative, (2012), SC Magazine, http://www.scmagazine.com/russian-cyber-crime-market-more-organized-lucrative/article/238100/; Group/IB, (2012), State and Trends of the Russian digital crime market 2011, http://www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf, приступљено 18.1.2014;

595 Cyber crime is Europe's 'big challenge', 2012, http://www.dw.de/cyber-crime-is-europes-big-challenge/a-15988087, приступљено 18.1.2014;

596 Страх од cyber криминала је по Alshalan A, 2005, Cyber-Crime Fear and Victimization: An Analysis of A national Survay, http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf (приступљено 19.1.2014), који цитира Ferraro K, 1995, Fear of Crime: Interpreting Victimization Risk, New York, SUNY Press „емоционални одговор страха или анксиозности на симбол злочина који неко лице асоцирана криминалом“;

597 Тако је у току априла 2014. године откривен малолетник који је основао скандалозну *Facebook* групу "Највеће дроље основних и средњих школа". У питању је малолетник из Хрватске, који је користећи лажни *Facebook* профил намамљивао девојчице из земаља у региону да му шаљу своје провокативне обнажене фотографије koje је објављивао са пуним именима и презименима. Група је за само пар дана прикупила око 60.000 “лајкова”, //www.telegraf.rs/vesti/1038765-fejsbuk-dozvolio-pedofiliju-fotke-polugolih-devojcica-nisu-krsenje-pravila-foto; или „ ... da su svake godine u SAD-u čak 850 tisuća ljudi – većinom žena, žrtve online bullyiniga“. http://znanost.geek.hr/clanak/internet-zlostavljanje-opasnije-od-klasicnog/#ixzz2zoB559fz, приступљено 19.1.2014;

598 Fafinski S. Dutton W.H. Margetts H, 2010, op. cit.; Hargreaves G., Prince D, 2011, Understanding Cyber Criminals and Measering Thair Future Activitiy, Developing Cyber crime Research, http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf, приступљено 19.1.2014;

599 Ladbury A, 2013, Fears over cybercrime rising among EU consumers, http://www.commercialriskeurope.com/cre/2832/239/Fears-over-cybercrime-rising-among-EU-consumers, приступљено 19.1.2014;

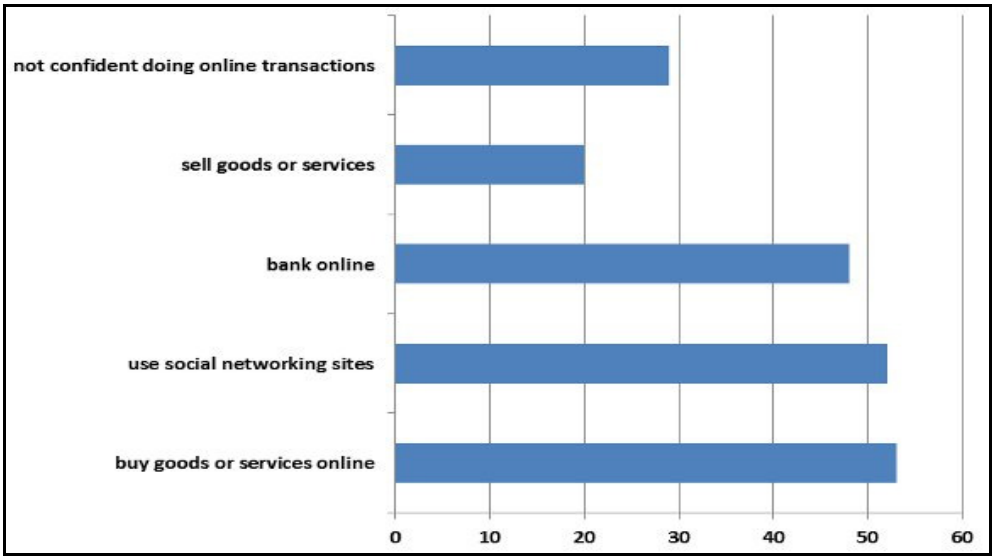


График 37. Активности грађана ЕУ на интернету[600]

Годину дана раније истраживање у ЕУ је показало да 89% корисника интернета избегава да открије своје податке о личности преко интернета, а 74% се слаже да је ризик да постану жртве cyber криминала повећан у последњих годину дана, између осталог јер је око 12% већ имало искуство са хаковањем својих профила на друштвеним мрежама или података у електронској пошти, као и он-лајн преварама, а 8% су били жртве крађе идентитета. Ипак, 53% нису променили своје он-лајн лозинке[601].

Даља истраживања cyber криминала довела су до развоја два модела: један који је комплекснији и везан за виктимизацију, а други, једноставнији, везан је за страх[602]. Поједини аутори (*Bernik, Dobovšek, Markelj*)[603] сматрају да се „страх од cyber криминала односи на процену личних опасности и процену трошкова ублажавања штетних последица ако неко постане жртва cyber криминалаца“. Посебно истичу „да постоји несклад између статистичких података о овом криминалу, утицају информативних медија, као и личних искуства појединаца активних у cyber простору.“ Са тих полазишта спровели су истраживање cyber криминала у Словенији и мерили страх од њега. Дефинисали су 3 категорије варијабли (неприкладно понашање, узнемиравање, активно угрожавање) које су испитаници оцењивали по одређеној скали.

600 Ladbury A., (2013), op. cit.

601 Saran C. (2012), Fear of cyber crime stops EU citizens doing business on the web, http://www.computerweekly.com/news/2240159331/European-citizens-afraid-of-online-crime, приступљено 19.1.2014.

602 Wynne T. (2008), An Investigation into the Fear of Crime: Is there a Link between the Fear of Crime and the Likelihood of Victimisation?, http://www.internetjournalofcriminology.com/Wynne%20-%20Fear%20of%20Crime.pdf, приступљено 19.1.2014.

603 Bernik I. Dobovšek B. Markelj B., (2013), To fear or not to fear on cybercrime, Innovative Issues and Approaches in Social Sciences, Vol. 6, No. 3., http://www.iiass.com/pdf/IIASS-2013-no3-art01.pdf, приступљено 19.1.2014.

Истраживање које је спроведено у мају 2013. године, у оквиру пројекта **Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије** обухватило је и посебну анкету о високотехнолошком (cyber) криминалу у оквиру које је било 69 питања, а од тога су 23 била везана за одређене облике злоупотреба интернета и друштвених мрежа, односно дела cyber криминала. Један део питања био је усмерен на добијање одговора о свести (перцепцији) опасности и постојању страха од тих опасности/cyber криминалу.

Табела 32. Питања анкете о cyber криминал

Питања која се односе на cyber криминал	*Укупан број питања*	*Питања о ставовима према cyber криминалу*	*Укупан број питања*
Приватност и интегритет података о личности	8	Злоупотребе мобилних уређаја /рачунара	3
Phishing	2	Мишљење о потребним знањима	2
Хакинг	2	Мишљење о потребним знањима	2
Крађа идентитета	1		
Злоупотербе платних картица	1		
Cyberbulling преко друштвених мрежа	1		
Говор мржње	1		

3.3.1. Ставови о хакингу

Крајем 80-их и почетком 90-их година прошлог века регистровани су први случајеви хаковања у Југославији[604]. Пошто тадашњи кривични закон није предвидео посебно кривично дело неовлашћеног приступа заштићеном компјутерском систему, не постоје званични записи како, када и коме се то десило[605]. Јавност није била обавештена о томе, јер су хакери своје активности „маскирали“ неким другим. Имали су и „помоћ“ од стране повређених кроз њихово ћутање и негирање инцидената. Вести су се спорадично појављивале само у стручним круговима, а понекад на „*SezamPro*“ (тада јединoм *BBS*-у у Југославији) или у ретким компјутерским часописима, у дискусијама између читалаца. Појава није била карактеристична за југословенску информатичку сцену, тако да ју је било тешко пратити и анализирати. Хакери су у то време претежно били студенти и „компјутерски фанови“. Упади су више били последица радозналости него „болесних/злочиначких намера“.

604 Drakulić M, 1996, op. cit., str. 451 – 457;

605 Drakulic M. Drakulic R. (1999), op. cit;

Средином 1996. године у Србији почиње ера интернета[606]. Наиме, успостављене рачунарске везе између два факултета Универзитета у Београду може се сматрати почетком рада Академске рачунарске мреже (АМРЕС)[607]. Након што су стекли нека искуства у раду са интернетом, корисници су почели да се укључују у различите активности на мрежи, међу којима је био и хакинг. Прва два забележена хакерска случаја су упади у чворишта Академске рачунарске мреже, који су проузроковали њен пад као последицу брисања појединих делова система. Спроведена је локална истрага од стране особља оштећених чворишта, јер полиција, услед мањкавости тадашњег кривичног законодавства, није имала могућности да је обави. Откривени су пропусти у систему заштите због којих је дошло до нарушавања безбедности и обуставе рада мреже и идентификовани су извршиоци - "деца" старости од 13 до 16 година. Међутим, нису то били било који „клинци“ већ деца запослених на Универзитету која су користила њихове налоге. Упозорени су да ће бити искључени са мреже уколико наставе са овим и сличним активостима. Због немогућности изрицања санкција, јер није било никаквих запрећених казни од стране државе за ова дела, извршиоци су наставили са својим „радом“. Круг се ширио. Са новим нападима понашање хакера је било све дрскије. Остављали су увредљиве поруке администраторима мреже, хвалили се својим подухватима он-лајн и оф-лајн и најављивали нове. Јавност која је имала других проблема (мобилизација, немаштина, инфлација...) није била ни узбуђена ни забрунута због нечег новог у слагалици јер већина није ни знала да она постоји. Чак се ни у стручним круговима информатичара и правника није придавало важности опасностима до којих такве активности могу довести. Они су их третирали као "несташлуке", „елементарне непогоде“ или „нужно зло“ који су последица „нове играчке“.

Није прошло много времена и отпочело је окупљање хакера са територија бивше Југославије, без обзира кроз шта су све прошли током ратних година. Изузетно сложена политичка и економска ситуација, до које је дошло након распада државе усмерила, их је још једном на „заједнички животни простор“. Прекинута комуникација између појединаца је поново успостављена, овај пут путем интернета, без обзира на страх од репресије у својим срединама. Помагали су једни другима у коришћењу одређених ресурса интернета, који нису били доступни из појединих земаља. Размењивали су искуства, причали о подухватима и организовали заједничке нападе на одређене мете. Међутим, слика у целини није била тако идилична.

Започели су први сукоби базирани на националистичкој основи. Конфронтација је била између хакера из разних делова Југославије (Србије и Хрватске нарочито). У почетку су то били пробоји у туђе сајтове, а онда је почело одмеравање моћи и способности. Даване су јавне изјаве и упућиване поруке. Тако је у јулу 1996. године Горан Катлевић, назван "краљем хрватских хакера", изјавио је да је: "провалио систем Југославије на други дан њеног уласка на интернет и да је то било смешно лако“. Он је био први појединац из бивше Југославије против кога је

606 Мада је „Прва интернетска веза у бившој Југославији успостављена 1991. године између Факултета организационих наука и Електротехничког факултета у Београду. Она је касније постала темељ српског академског интернета.“ по Раденковић Б, 2009, Интернет, два пута међу Србима, http://www.politika.rs/rubrike/Drustvo/Internet-dva-puta-medju-Srbima.sr.html, приступљено 19.1.2014;

607 https://www.amres.ac.rs/index.php?option=com_frontpage&Itemid=1, приступљено 19.1.2014;

покренута истрага. Овај вешти хакер провалио је у сајт Хрватске националне телевизије (ХРТ), повезао је са Србијом и поставио слике из часописа Плејбој. То је изазвало велики шок за посетиоце сајта. Овим чином је хтео да упозори на лошу заштиту сајтова у Хрватској и њеног тадашњег главног интернет провајдера "Карнет". Остављене поруке су требале да буде доказ успеха и престижа, али и „уклањање“ противника из игре (нпр. два случаја блокирања хрватске везе са интернетом). Одговор је био наводни упад у Академску мрежу у Београду. Истрага је показала да је то била лажна узбуна, али да и Академска мрежа није имала обезбеђене мере заштите. На жалост, из ових активности нису извучени одговарајући закључци.

Даље активности добијају нове димензије и одговарају политичким догађајима на територија Југославије, посебно Србије. Сукоб се окреће ка Косову. У октобару 1998. године презентација листа "Глас Косова" бива модификована. Било је то време велике неизвесности у Србији - да ли ће бити бомбардовање или не?[608] Претња војном интервенцијом подигла је присутност на мрежи не само у Југославији. Многи страни сајтови су имали своје верзије о будућем развоју догађаја. Савезна влада је поставила линкове на свом сајту ка сајтовима и вестима о злочинима који су чињени од стране албанских терориста. Отворени су посебни југословенски сајтови широм света, у циљу информисања шире међународне заједнице.

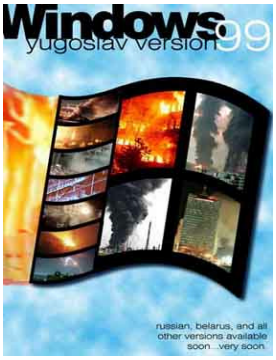
У исто време, на неколико познатих информативних агенција (*BBC, SKY, CNN*), омогућено је гласање о питању да ли НАТО треба да бомбардује Југославију, односно Србију[609]. Гласање је трајало један дан и показало је да је већина била за бомбардовање. Изузетак је био *BBC* који је омогућио да гласање траје неколико дана. У почетку је било више посетилаца који су мислили да је НАТО бомбардовање оправдано. Временом, ситуација се променила. На крају периода гласања 67% гласача је било против бомбардовања. У таквој напетој ситуацији све активности су изгледале сасвим нормалне. Једна од таквих активности били су упади хакера на сајтове на албанском језику. Током „посете“ постављен је грб Србије на насловну страну, заједно са неколико адекватних "порука“. Поруке су написане на српском и енглеском језику. Једна од порука је била: "Добродошли на сајт највећих светских лажова и убица", друга је била: "Браћо Шиптари, овај грб ћете имати на својој застави све док постоји." Поруке су биле на том сајту неколико сати. После су нестале заједно са комплетном презентацијом. Након извесног времена враћен је првобитини изглед сајта.

608 Dingarac D. (1999), Internetom protiv bombi, op. Cit;

609 Све вести су биле формиране тако да се створи јавно мњење о неопходности предузимања такве акције, нпр. World: Europe Nato to strike Yugoslavia (1999), http://news.bbc.co.uk/2/hi/europe/302265.stm; Gallup/CNN/USA Today Pollhttp (1999), www.pollingreport.com/serb9903.htm, приступљено 22.1.201;

Овај догађај је претходио упаду на званични сајт информативног центра Косова. Започео је хакерски рат који је у Србији проглашен добрим и који је јавно слављен[610]. Овај, а и сви даљи упади, приписани су хакерској групи која је сама себе назвала "Црна рука", алудирајући на истоимену организацију с почетка XX века. Она[611] је желела је да наследи репутацију претходника као патриота и ослободилаца. Постојало је чак објашњење да се овим активностима живот оригиналној „Црној руци“ продужио и да је то редак случај да таква организација прође "тест времена преко једног века".

"Црна рука" је наставила своје активности и до краја октобра 1998. године је „протресла“ сајт Хрватске новинске агенције "Вјесник" остављајући поруку: "Црна рука жели да промени лажну слику која кружи планетом да су Срби зликовци". Даље су изјавили да они не значе рат и да не желе никакво зло. "Вјесник" је одмах известио да су припадници "Црне руке" откривени. Истовремено, тврдећи да је то учињено са рачунара на два факултета указали су на српску академску мрежу тврдећи да хакери и даље путују и делују у њој.



Мини истрага спроведена на именованим факултетима, показала је да је вест "Вјесника", око локације извршилаца, била нетачна. Новинари београдског часописа "Свет компјутера", после опсежне потраге и контактирања са бројним појединцима су успели да направе контакт преко *chat room*-а са двоје чланова који су им „открили“ појединости о "преуређеним" презентацијама и својим разлозима. Наводно им је главни мотив био електронска одбрана интереса Југославије. Ипак, и даље се не зна ко су били чланови ове хакерске групе, мада су кружиле различите приче у српском хакерском подземљу.

Рат се проширио и на друге делове земље и против других противника. Занимљив случај је "летећег хакера" који је направио хаос у једном од градова Републике Српске и активирао боје које је *UNPROFOR* користио као систем извештавања (зелена - нормална ситуација, наранџаста – спрема се сукоб и црвено – узбуна). Провалио је лозинке и кодове и, остављајући црвену боју, изазвао блокирање путева и улица.

610 Pelemiš D. (1999), Prvi hakerski rat, http://www.sk.rs/1999/09/skin01.html, приступљено 22.1.2014;

611 Dingarac D. Stančević T. (1998), op. cit;

У следећих неколико година било је бројних „чарки“ између хакерских група и појединаца на Балкану. Иако су били кратко присутни на интернету, југословенски хакери су отворили нову страницу ратовања. Занимљиво је да је у време НАТО бомбардовања већина YU корисника интернета, без обзира на политичку припадност, стручност, старост покушала на разне начине да га користи за помоћ својој земљи. Њима су се придружили и они који су отишли, без обзира што су многи отишли због неслагања са постојећом политиком, због незапослености или малих плата (просечна месечна плата у Србији је била око 70 DEM). Предњачили су млади. Стотине њих је данонoћно било на мрежи и слало поруке очаја, молби, информација о томе шта се у земљи дешава[612]. Провајдери су пружали бесплатне услуге (иначе за коришћење интернета су се плаћале накнаде). Многи комерцијални сајтови су се преко ноћи преорјентисали у информативне[613], и то не само за подручје Југославије и дијаспору, него и за цео свет (текстови су поред обавезног енглеског, превођени и на многе друге светске језике, а преводиоци су то бесплатно радили). Формиране су екипе које су одговарале на хиљаде е-порука. Неки су чак своје знање и искуство искористили за недозвољене, али оправдане активности – хакерисање, не би ли и на тај начин скренули пажњу на то што се тих дана бомбардовања дешавало. Отворени су и посебни инострани сајтови на којима се изражавало негодовање са бомбардовањем[614]. Поред бројних појединаца и неколико постојећих хакерских група, формирале су се и нове чије се деловање осетило много пута, нарочито на сајтовима у земљама НАТО чланица[615]. У групама су, поред извесног броја професионалних хакера (који су свој хакерски стаж започели много раније), били и новоформирани хакери (студенти, ђаци, професори ...), од којих су многи, након завршетка бомбаровања, престали са овим активностима. Не тако велика југословенска заједница, више српска интернет заједница, у то време, била је компактна целина. Можда једна од најзанимљивијих је била група “Српски анђели” која се формирала у току бомбардовања и која је, између осталог, имала изузетно добру *mailing* листу, преко које су на хиљаде адреса слали вести о томе шта се дешава (вести су мењали на сваких 5 минута и стално имали слоган: **Свима желимо мирно небо и чврсте мостове**, "**Српски анђели**"). Сајт им је био изузетно ажуран (имали су неколико адреса које су све водиле до основног сајта), тако да је многима служио за информисање шта се у ком делу земље и главног града дешава. Последњи пут са вестима су се јавили 14. јуна 1999. године (са комплетним Кумановски мировни споразумом, који није у целини био одмах доступан преко регуларних медија), да би се корисницима листе поново јавили ради честитања Нове 2000. године. Само неколико дана након завршетка

612 Procitajte pismo iz Beograda i Nemacke, (1999), http://premaks.tripod.com/Bombing/bomb02.htm, приступљено 12.11.2013;

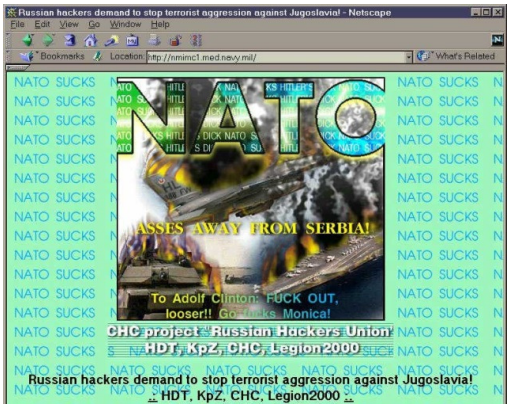
613 www.inet.co.yu;

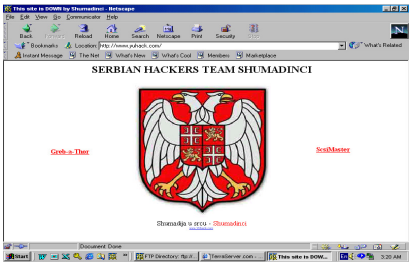
614 Anti-NATO-War Site of the Group Neue Einheit, (1999), http://www.neue-einheit.com/english/anti-nato-war.htm, приступљено 22.1.2014;

615 Dingarac D, 1999, Na Mreži, na položaju, op. Cit;

бомбардовања издали су *CD* под називом "**Истина о рату**" са текстовима, сликама, аудио и видео-материјалима невиђеним у току 80 дана рата (на њиховом, као и на другим сајтовима у току бомбардовања, налазили су се снимци погођених објеката, повређених људи, извештаји из склоништа, болница и са других места, звучни записи у току напада, разговори са појединцима и слично). На хиљаде ових *CD*-ова (тачније 10.000) бесплатно је подељено школама, појединцима, институцијама, факултетима и свакоме ко им се јавио. Специфичност њиховог деловања била је у томе што су, паралелно са овим активностима (информативним, доброчинитељским), учествовали и у "ратним" операцијама (укључивши се у све облике cyber рата). Један од знакова који су остављали на хакерисаним сајтовима био је модификовани знак *Windows*. "Српски анђели" нису своје активности јавно оглашавали и популарисали.

„Српским анђелима" (чије је деловање више личило на џентлменско) придружиле су се и друге групе (Црна рука, Српска војска интернета – хакерска група устројена као војна формација, нетипично за хакерске групе[616]) које су биле много агресивније, а њихове акције спектакуларније и усмерене искључиво на "субверзивне" активности (преусмеравање линкова, искључивање из употребе сајтова, онемогућавање приступа, промена садржаја, убацивање вируса ...). Овим групама касније су се придружили појединци и групе из Украјине, Русије, Кине. За разлику од сарадње и повезивања хакера-појединаца из различитих земаља, што је иначе честа појава, ова хакерска алијанса више личи на груписање земаља у току стварних ратних операција. При томе, то вероватно није био резултат преговора и договора држава и армија, већ специфичних групација и имао је карактеристике ослободилачких покрета, помешаних са терористичким активностима, посебно припремљеним и изведеним. Претпоставља се да је алијанса деловала *ad hoc* и да се распала након завршетка догађања која су им била повод уједињења.

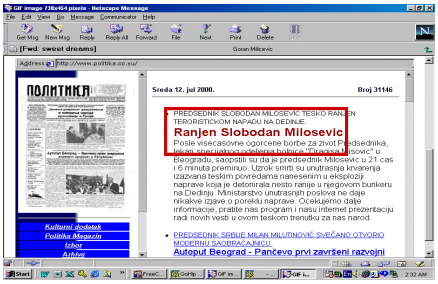




Након престанка бомбардовања cyber армија се повукла са попришта, остављајући по коју групицу за нека друга деловања. Међутим, хакерске активности које су стизале из југословенског cyber простора и у њему самом нису јењавале. Усмеравале су се на стране сајтове, али све више и на домаће. Један од напада извршен је почетком априла 2000. године, када је хакер по имену *Shumadinac*

616 Bubanja B, 1999, Iza kulisa, http://www.sk.rs/1999/07/skin01.html, „Osnovan u okviru fonda „Kapetan Dragan" *Net centar* postavio je jednu od najposećenijih Web stranica kod nas – www.yu." , приступљено 12.11.2013;

извршио модификовање информација неких домена регистрованих код *Network Solutions*. Наиме, 15 априла *Chris Oakes* обавештава о "*Balkan War in Domain Attacks?*" претпостављајући да је преко 2000 домена, од којих је највише албанских, хрватских, али и других (adidas.com, jamesbond.com, mafia.com, france.com, italy.com, spain.com, slovenia.com, croatia.com, sarajevo.com, kosova.com, washington.com, and bosnia.com) било преусмерено. Посебан "рат" се водио против црногорског сајта Montenegro.com због политичких несугласица са противницима владајуће коалиције у Србији. Интересантно је да је, након прилично велике осуде југословенске интернет заједнице, он послао свом провајдеру писмо извињења у коме се каје због штете коју је нанео, између осталог и угледу земље и обећава да то више неће радити.



Са страних сајтова хакери се усмеравају и на домаћи cyber простор. Тако је 12. јула 2000. године био ухакован сајт најстарије српске новинске куће "Политика". Непознати хакер или хакери су променили садржај дневних вести објављујући на насловној страни обавештење о "тешком рањавању председника Милошевића". У даљем тексту јављају и да је умро. Тиме се наставља унутрашњи пропагандни рат.

Године које су следиле вратиле су српске хакере из херојске у криминалну стварност. Ипак, трагови „херојских" времена виде се и данас.

Без обзира што су у стручним часописима, али и у информативним новинама присутни подаци о хакерима и њиховим активностима, што су многи медији имали бројне прилоге, што су снимани и емитовани филмови и подаци из истраживања, у Србији указују на недовољну упознатост са овим обликом cyber криминала. На питање шта је хакинг, свега је 37% испитаника одговорило потврдно, а од тога је било више мушке популације (55,2%) него женске (44,8%). При томе је више испитаница од испитаника одговорило да је чуло, али да не зна ништа о томе. Иначе, о бројним темама, нпр. о политици, жене су мање информисане и како истичу истраживачи са *Goldsmiths Leverhulme Media Research Centre at the University of London* предвођени професором *James Curran* „политички јаз у знању између полова је глобални феномен", између осталог и зато што су мушкарци више цитирани у медијима (нпр. само је 30% жена цитирано на ТВ)[617]. Тиме се оне демотивишу за већу укљученост и заинтересованост. Што се хакинга тиче, жене се, по бројним истраживањима, мање баве хакингом од мушкараца и мање су за њега заинтересоване јер је он више у техничком домену[618], што се рефлектује и на њихов страх и информисаност. Такође, њима мањка време да се баве овим проблемима.

617 Daugherty A., (2013), Women know less about politics than men, study finds (that goes for Canada, too), http://www.theglobeandmail.com/life/the-hot-button/women-know-less-about-politics-than-men-study-finds-that-goes-for-canada-too/article12947354/, приступљено 22.1.2013;

618 Tiku N. (2012), Paul Graham Says Women "Haven't Been Hacking For the Past 10 Years", http://valleywag.gawker.com/paul-graham-says-women-havent-been-hacking-for-the-pa-1490581236, приступљено 12.1.2014;

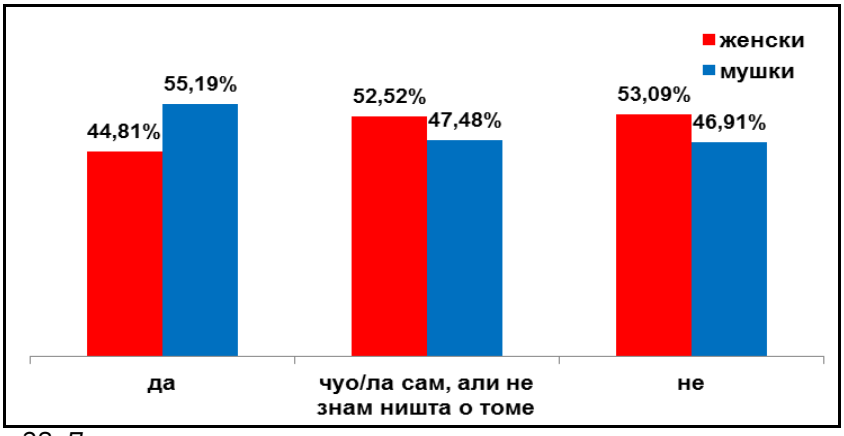


График 38. Познавање хакинга, по полу, испитаника

Највећи проценат (55%) који о хакингу ништа не зна је оних између 18 и 30 година старости, затим следе они који имају мање од 18 (35%), па преко 45 (23%), а од 30 до 45 година свега је 6% оних који не знају ништа. У групи испитаника до 18 година, најмањи проценат је оних који не знају шта је хакинг у популацији од 14 до 16 година, али процентуално, у целој овој популацији, они су и групација која највише зна шта је то (скоро 54%). Када се ови подаци упореде са забринутошћу за постајање жртвом неког типа злоупотреба, по подацима Европске комисије, млађи испитаници су чешће него старији забринути због хаковање друштвених мрежа и електронске поште (48% од оних између 15 и 24 година старости)[619].

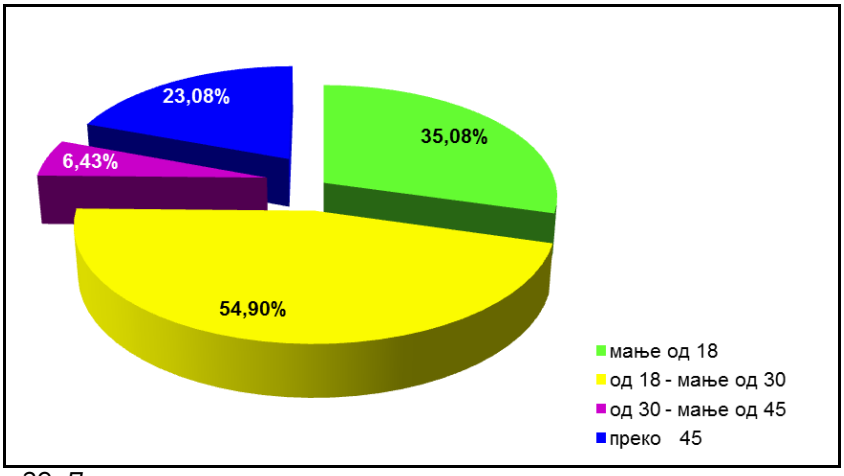


График 39. Познавање хакинга по годинама старости испитаника

У односу на величину места пребивалишта, преко 44% свих испитаника зна шта је хакинг без обзира на величину тих места. Најмање знају испитаници из места мањих од 5000 становника (36,1%), највише из места од 5000 до 20.000

619 European Commission, 2013, op. cit;

становника (52,8%), а од њих мање знају они из већих места. Зачуђујуће мало о хакингу знају испитаници из Београда (43,1%), што се може тумачити и неконтролисаном жељом за великим бројем он-лајн пријатеља, а истовремено и великом отуђеношћу[620] или бољом информисаношћу о другим, новим медијима и мрежама (нпр. WhatsApp, WeChat, KakaoTalk)[621].

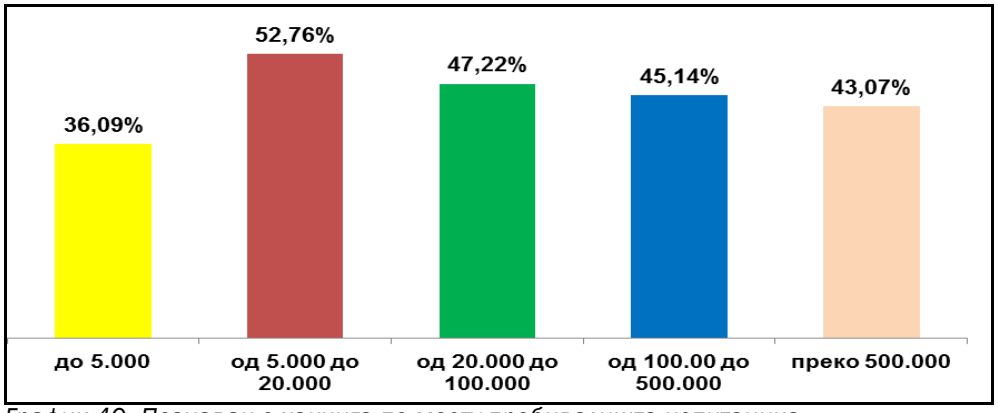


График 40. Познавање хакинга по месту пребивалишта испитаника

Ако се заједно посматра познавање хакинга у зависности од година старости и пола, може се уочити да је 25,4% жена, које су одговориле да знају шта је хакинг, између 18 и 35 година старости, а мушкараца 29,3% у истој доби.

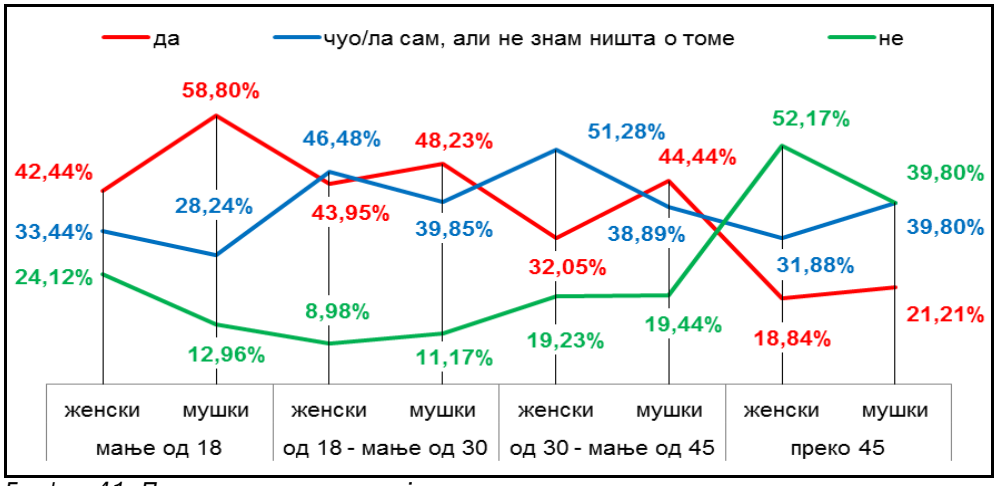


График 41. Познавање хакинга заједно по полу и старости испитаника

620 Alienation, http://psychology.jrank.org/pages/22/Alienation.html; Here's Where Teens Are Going Instead Of Facebook, http://www.forbes.com/sites/parmyolson/2013/11/12/heres-where-teens-are-going-instead-of-facebook/, приступљено 22.1.2014;

621 Olson P. (2013), Teenagers say goodbye to Facebook and hello to messenger apps, http://www.theguardian.com/technology/2013/nov/10/teenagers-messenger-apps-facebook-exodus, приступљено 22.1.2014;

Значи, кад је у питању познавање хакинга испитаници су релативно добро упознати, с тим што су боље упознати мушкарци и то из мањих места (између 5000 и 20.000 становника), а најмање из популације између 18 и 30 година.

На питање о неопходности посебних специјалистичких информатичких знања за хакинг укупно је одговорило преко 95% испитаника. Од тог броја њих 64,4% је дало потврдан одговор, од тога је било 45,1% жена, односно 54,9% мушкараца, што се готово не разликује од расподеле код претходног питања.

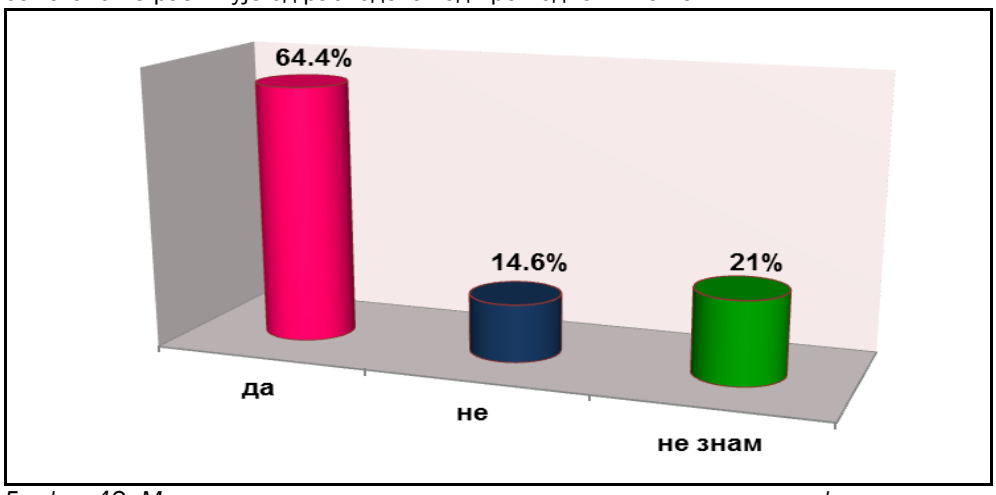


График 42. Мишљење испитаника о неопходности поседовања специфичних информатичких знања за хакинг

Структура одговора на исто питање у оквиру мушке и женске популација испитаника указује да је потврдан одговор дало мање жена него мушкараца и да су оне мање информисане о томе (скоро 60%), што улази у сферу предрасуда, јер се многа од тих знања могу једноставно наћи на интернету са комплетним упутствима за примену. Само треба бити заинтересован!

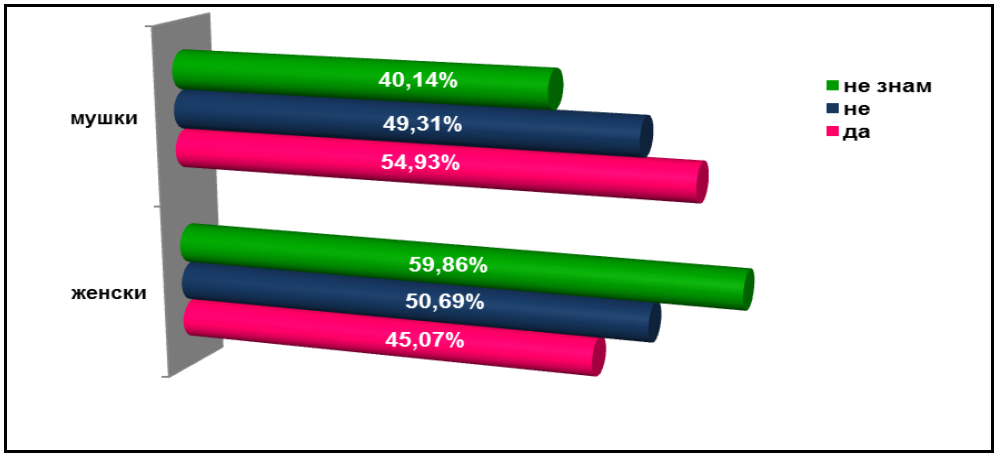


График 43. Мишљење испитаника, по полу, о неопходности поседовања специфичних информатичких знања за хакинг

На исто питање одговарали су испитаници различитих година старости. Највише оних који су мислили да су потребна специфична знања било је између 18 и 30 година (59%), што је и нормално јер је и међу запосленим у *ICT* сектору више младих, а они поседују та знања (само 13.7% запослених у 2011. години је старости између 50 и 64 године, што је мање од 26,1% како је у целој привреди)[622]. Следећа велика група са потврдним одговором је група до 18 година (27%). Остале две су имале мали проценат 8%, односно 6%.

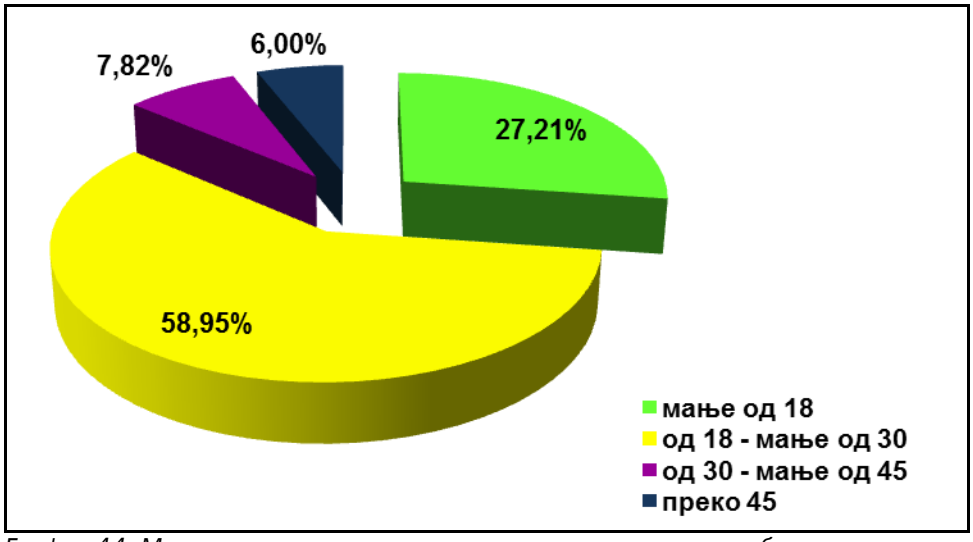


График 44. Мишљење испитаника по годинама старости о потребним специфичним информатичким знањима за хакинг

Кад је у питању став према специфичним информатичким знањима за хакинг, 64,8% испитаника сматра да је оно потребно када се посматра величина места пребивалишта испитаника. Од тога 69,2% је из градова преко 500.000 становника, што је потпуно другачије у односу на познавање хакинга. Најмање позитивних одговора су дали испитаници који долазе из места испод 5000 становника, мада је то и код њих више од 50%.

622 EU Skills Panorama Analytical Highlight, (2012), op.cit.

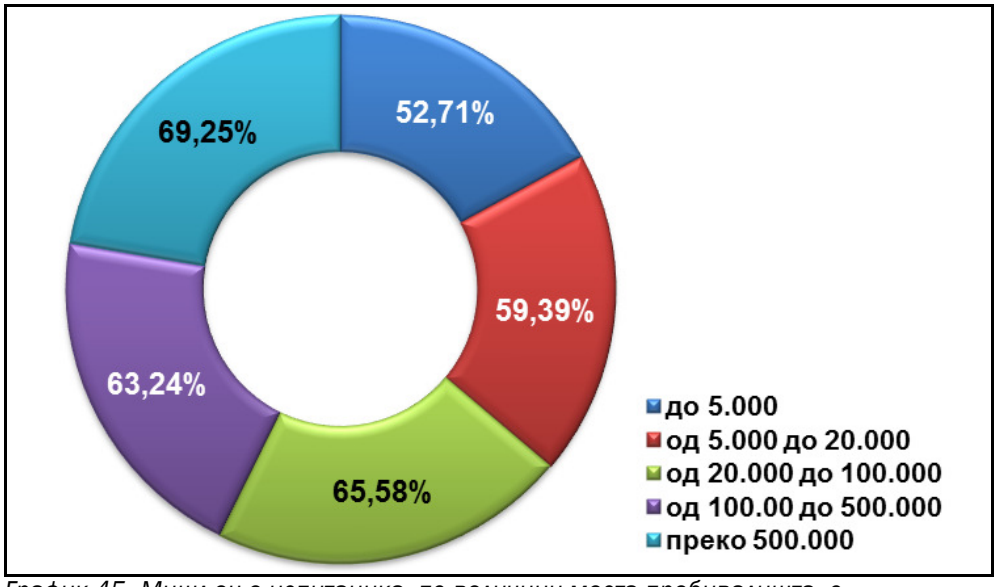


График 45. Мишљење испитаника, по величини места пребивалишта, о неопходности поседовања специфичних информатичких знања за хакинг

Значи, кад су у питању мишљења испитаника о неопходности поседовања специфичних информатичких знања за хаковање највећи број испитаника који је дао потврдан одговор је мушког пола, старости између 18 и 30 година и живе у градовима изнад 500.000 становника.

Ако се заједно посматра мишљење испитаника о потребним специфичним информатичким знањима за хакинг, у зависности од пола и величине места пребивалишта, уочава се да је најмање са негативним одговором мушкараца из места до 5000 становника и између 5000 и 20.000 становника (по 0,6%) и жена из места од 20.000 до 100.000 становника (испод 0,5%). Највећи проценат са позитивним одговором су мушкараци из места са преко 500.000 становника (14,1%).

Посматрајући заступљеност одговора у односу на пол и место пребивалишта испитаника, види се да нема велике разлике у ставу о потреби посебних специфичних информатичких знања да би неко био хакер код мушкараца из било ког места (62,9% и 68,6%). Код жена је дијапазон већи и креће се од 43,3% до 62,2%, зависно од величине места њиховог пребивалишта.

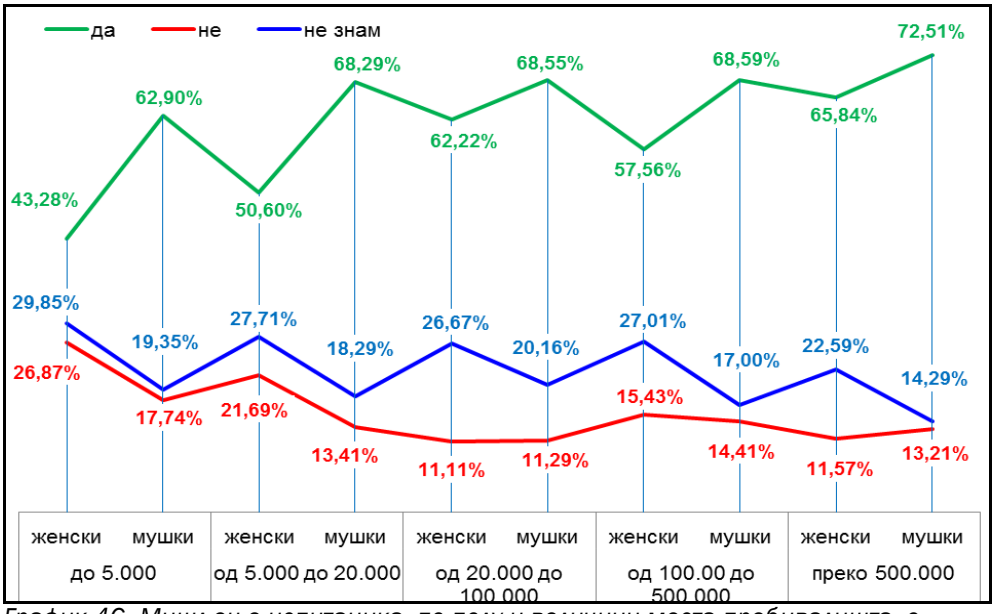


График 46. Мишљење испитаника, по полу и величини места пребивалишта, о неопходности поседовања специфичних информатичких знања за хакинг

На питање "Поседујете ли ви та знања?" свега њих 7,7% је дало потврдан одговор. Њих је десет пута мање у односу на оне који немају та знања (78,1%), што је сасвим нормално јер су испитаници били из разних старосних категорија, па и деца и старији од 60 година.

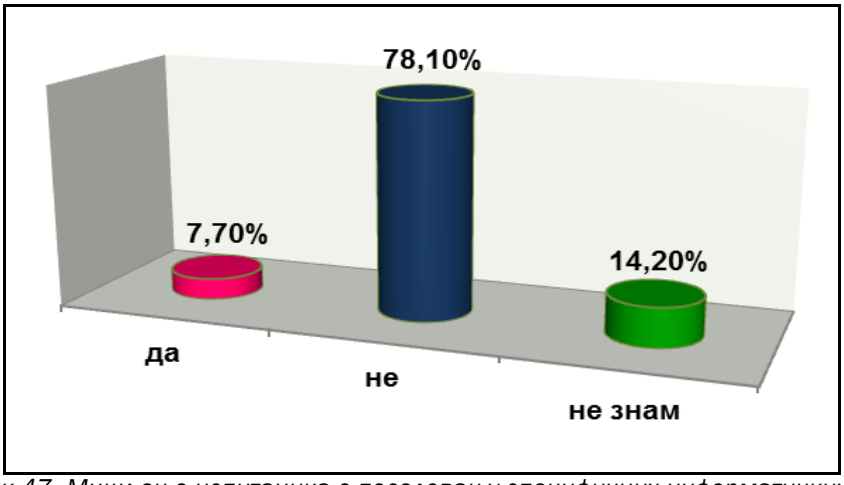


График 47. Мишљење испитаника о поседовању специфичних информатичких знања за хакинг

На питање да ли они поседују та знања од оних који су дали потврдан одговор 11,6% мушкараца је одговорило да га има, а код жена је то три пута мање (3,7%). Да не поседују ова знања сматра 72,9% мушкараца, док је то изјавило 83,4% жена. То и даље не разбија слику „белог мушкарца за рачунаром“ када се помисли на хакера. Међутим, та слика се полако и све више мења јер почиње ера cyber феминизма, који користи и хакинг у својој борби за бољу позицију[623].

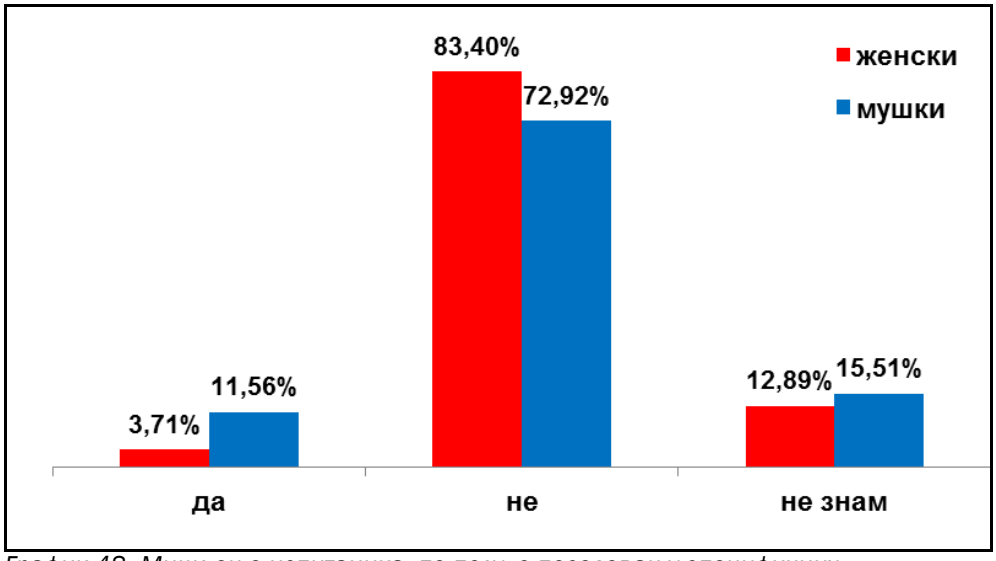


График 48. Мишљење испитаника, по полу, о поседовању специфичних информатичких знања за хакинг

Кад су у питању године старости, од оних који су дали потврдан одговор да поседују хакерска знања, највише их је, или су најсамоуверенији, из групе до 18 година мада је тај број низак, само 11,3%, а најмање знају они преко 45 година(3%). Све групе су одговориле са преко 68% да не поседују ова знања. Интересантно је да су се две групе (18-30 и 30-45 година) готово подједнако изјасниле да не поседују хакерска знања (између 82,6% и 82,7%). Ако се упореде подаци о учиниоцима cyber криминала код нас и у свету (*График 13*) то су и групе из којих су највише и регрутовани.

Табела 33. Мишљење испитаника, по годинама старости, о поседовању специфичних информатичких знања за хакинг

		Потребна специфична информатичка знања			Тотал
		Да	Не	Не знам	
Пол	Женски	59,26%	15,12%	25,62%	100%
	Мушки	69,37%	14,13%	16,50%	100%

623 Sollfrank C. (1999), Women Hackers, http://www.obn.org/hackers/text1.htm; Knight A., (2014), Where are the female hackers?, http://www.smh.com.au/small-business/franchising/where-are-the-female-hackers-20140228-33ogc.html, приступљено 25.4.2014;

Величина места пребивалишта испитаника нема утицаја на поседовање специфична знања за хакинг јер између 74,7% и 79,4% је одговорило да их не поседују.

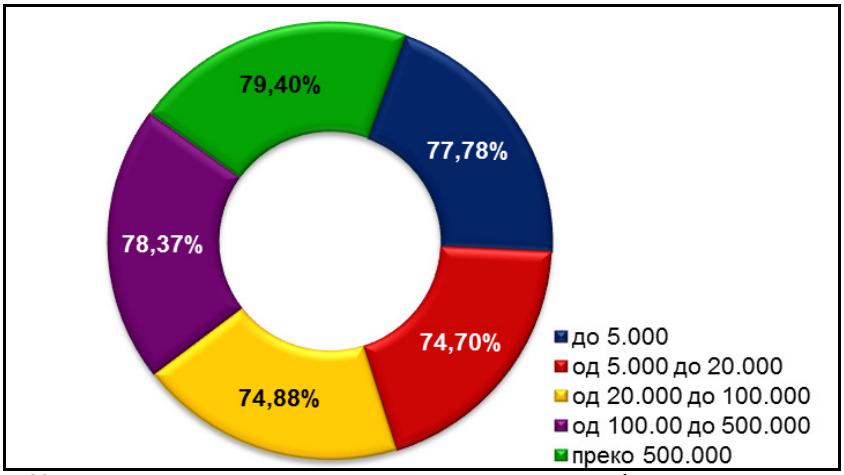


График 49. Мишљење испитаника, по величини места пребивалишта, о поседовању специфичних информатичких знања за хакинг

По прегледу заступљености специфичних информатичких знања за хакинг, зависно од пола и година страости, између 65,8% и 85,6% испитаника свих узраста је одговорило да га не поседују. Најмањи број испитаника који је одговорио да та знања не поседује су мушкарци стари до 18 година. Интересантно је да ни једна жена преко 45 година није одговорила да поседује та знања, али ова групација је дала и најмање одговора да их не поседује (66,7%).

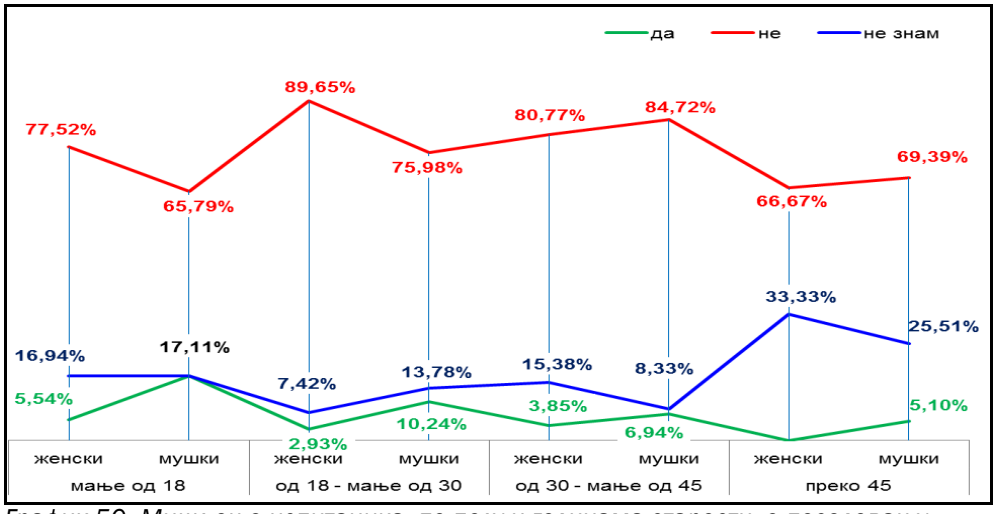


График 50. Мишљење испитаника, по полу и годинама старости, о поседовању потребних специфичних информатичких знања за хакинг

Последње питање из групе питања везаних за хакинг било је и питање "Да ли сте некада били жртва хакинга?". На ово питање њих 61,2% је дало одричан одговор (укупно није одговорило 3,2% испитаника), с тим што не треба занемарити ни 24,9% њих који не знају. Ипак је, на први поглед, релативно велики проценат оних који су одговорили да јесу било жртва (13,9%).

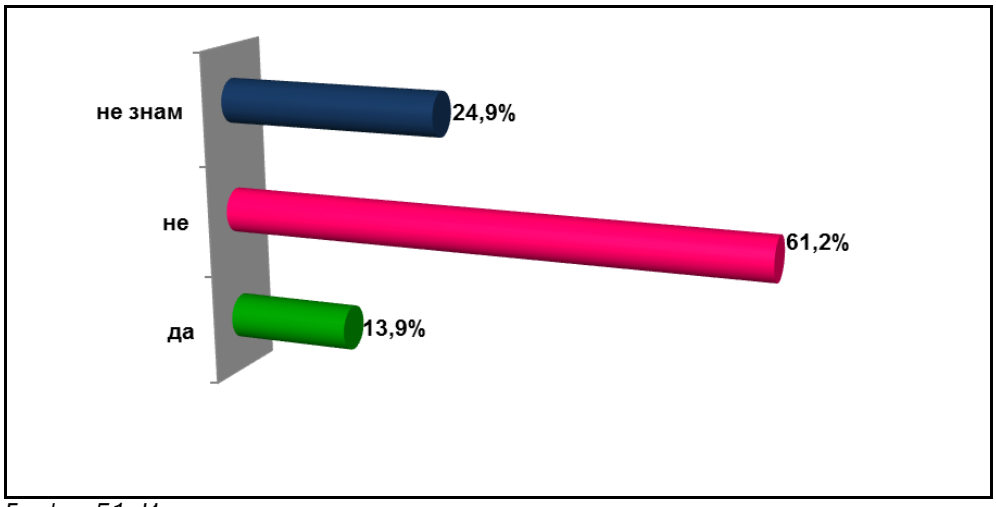


График 51. Испитаници као жртве хакинга

То значи, с једне стране, да ова појава и даље код нас није искорењена, напротив (од укупног броја поднетих кривичних пријава до августа 2012. године, 35,7% је било за кривично дело неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података од укупно поднетих пријава за дела cyber криминала)[624]. С друге стране, ово би и могла бити реална бројка с обзиром да је преко 40% испитаника одговорило да зна шта је хакинг, што може значити да је то проистекло из личног искуства. Ако се то упореди са искуством везаним за хакинг у Европској унији, подаци из 2012. године показују да је 12% корисника интернета имало искуства са хаковањем њихових налога на друштвеним мрежама или електронској пошти. У земљама чланицама цифре се крећу од 19% у Великој Британији, 18% у Шведској и Белгији, 16% у Холандији до скоро занемарљивих 3% у Грчкој и 6% у Бугарској[625]. Много више је оних који су забринути[626] због могућности да постану жртве хакинга (45%). При томе треба посебно нагласити да у српском истраживању није био специфициран циљ напада, за разлику од европског у коме јесте (налога електронске поште), тако да разлика која се појављује није велика (> 3,4%).

624 Њима треба додати још 5 пријава у 2013. години, односно свих кривичних пријава је било 1365 од 2009. године до 31. јануара 2014. Укупно је од 2009. било 29 кривичних дела из члана 302, што значи да је 21,24%;

625 European Commission, (2013), op. cit;

626 AFP, (2012), Hacking victim talks about perils of digital age, http://www.hindustantimes.com/technology/gadgets-updates/hacking-victim-talks-about-perils-of-digital-age/article1-911989.aspx, приступљено 22.1.2014;

Од укупног броја испитаника који су одговорили на ово питање, жене су у 14,7% одговора потврдиле да су биле жртве и 13% је то био случај са мушкарцима[627]. Бројни су примери у САД-у, да су жене често жртве хакинга и не само да им се неовлашћено улази у рачунаре него иза тога стоје и друга дела (нпр. принуда/уцена, за коју већ постоји и посебан термин - "*sextortion*"[628] да приказују своје наге фотографије)[629]. Доминантан за обе категорије испитаника је негативан одговор (мушкарци 62,7%, а жене 59,7%). За одговор „не знам" испитанице су се определиле за 1,3% више него испитаници (25,6% : 24,3%).

Табела 34. Испитаници, по полу, као жртве хакинга

		Да ли сте некада били жртва хакинга?			*Тотал*
		Да	Не	Не знам	
Пол	Женски	14,74%	59,67%	25,59%	100%
	Мушки	13,04%	62,65%	24,31%	100%

Потврдан одговор да су били жртве хакинга највише је дало испитаника из групе до 18 година (19,8%), али су из исте категорије и у скоро истом проценту одговорили да не знају да ли су то били или не (19,6%). Друга истраживања показују да је иста категорија, али са много већим процентом, била угрожена или је била жртва. По тим истраживањима 30% тинејџера и одраслих младих су имали ухаковану или шпијунирану електронску пошту, *Facebook* и друге он-лајн налоге, али то нису доживљавали као опасност, с тим што 72% жртава шпијунаже и 65% хакинга знају извршиоце[630]. Најмање су жртве хакинга, по мишљењу испитаника, били они преко 45 година (0,6%). То се уклапа и у констатацију да што је популација старија

627 То се разликује од резултата на које се позива *Hanna Rosin* која констатује „Нова студија открива да су мушкарци често жртве сексуалног злостављања, а жене су често злостављачице", Rosin H., (2014), When Men Are Raped, http://www.slate.com/articles/double_x/doublex/2014/04/male_rape_in_ america_a_new_study_reveals_that_men_are_sexually_assaulted.html, приступљено 25.4.2014;

628 Термин потиче од *sexual exploitation* и први пут се појавио 50-их година у Калифорнији. У суштини означава да је у питању „врста експлоатације која укључује присилу у изнуђивању сексуалних услуга од жртве. То је, такође, врста уцене у којој се сексуалне слике или видео користе да присиле жртве на сексуалне услуге", Lohmann R., (2014), Psychology, answered on behalf of Top 10 Social HealthMakers, http://www.sharecare.com/health/parenting-teens/what-is-sextortion; То је један од "злочин избора", који чине интернет предатори користећи приступ приватном животу своје жртве. Предатори обично циљају тинејџере или младе одрасле особе на сајтовима за друштвено умрежавање, као што су *Facebook* или *MySpace,* присиљавајући своје жртве да им дају експлицитне сексуално фотографије и/или услуге у замену за њихову тајну или за обећање да престати са даљим притиском, Edgington S., (2014), Pediatrics, answered, http://www.sharecare.com/health/ parenting-teens/what-is-sextortion, приступљено 22.1.2014;

629 U.S. Attorney's Office, Central District of California, (2013), Glendale Man Who Admitted Hacking into Hundreds of Computers in Sextortion Case Sentenced to Five Years in Federal Prison, http://www.fbi.gov/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison, приступљено 22.1.2014;

630 North A. (2007), Three In Ten Young People Victims Of Hacking, But Many Don't Care, http://jezebel.com/5847775/three-in-ten-young-people-victims-of-hacking-but-many-dont-care, приступљено 22.1.2014;

све мање изјављују да су били жртве[631], мада су и мање присутни на мрежи, а и уопште[632] кад је у питању било који криминал[633]. Обрнута је ситуација када је у питању одговор „не знам“, какав су дали старији од 45 година у највећем броју случајева такав одговор (50%).

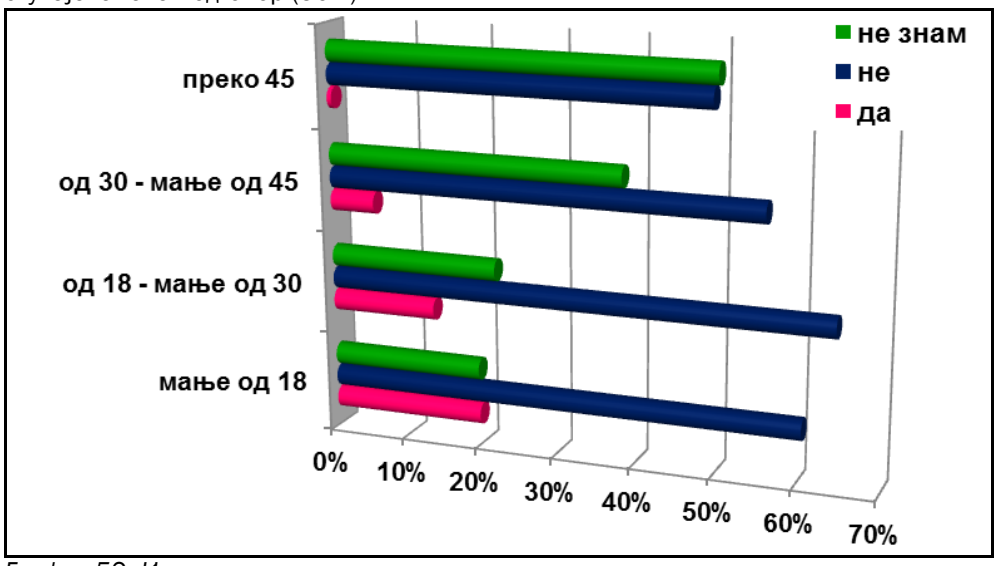


График 52. Испитаници, по старости, као жртве хакинга

У местима до 5000 становника исти број испитаника је потврдио да не зна да ли су били или нису жртве хакинга (20,9%). То је присутно и код испитаника из места од 5000 до 20.000 становника (18,1%). Највише испитаника у свим групама се определи за одричан одговор и крећу се између 58,1% (из места до 5000 становника) до 63,9% (из места 5000 до 20.000).

Табела 35. Испитаници, по величини места пребивалишта, као жртве хакинга

		Да ли сте некада били жртва хакинга?			Тотал
		Да	Не	Не знам	
Величина места пребивалишта испитаника	До 5.000	20,93%	58,14%	20,93%	100%
	5.000 - 20.000	18,07%	63,86%	18,07%	100%
	20.000 - 100.000	12,04%	58,33%	29,63%	100%
	100.00 - 500.000	12,63%	61,05%	26,32%	100%
	Преко 500.000	13,68%	61,29%	25,03%	100%

631 Rutherford A. (2014), 4,766 crimes against the elderly, but 96% of cases remain unsolved, Shocking statistics spark call for tougher sentences, http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/4766-crimes-against-the-elderly-but-96-of-cases-remain-unsolved-30063796.html, приступљено 25.4.2014;

632 По Канадској студији из 2009. године „2% од свих Канађана старости од 55 и старији је пријавио да је било жртва насилног криминала, и то много више физичког него сексуалног злостављања“, Brennan S. (2012), Victimization of older Canadians, 2009, http://www.statcan.gc.ca/pub/85-002-x/2012001/article/11627-eng.pdf, приступљено 22.1.2014;

633 Република Србија, Републички завод за статистику, (2013), op. cit;

Сваке секунде најмање 12 корисника интернета у свету постају жртве cyber криминалаца и тај број се повећава сваке године[634] (по Касперском 62% испитаника је имало бар један инцидент са покушајем крађе финансијских информација)[635]. Од опасности које долазе споља за организације, на четвртом месту су мрежни упади (24% у 2013. и 2011, а 23% у 2012. години). У таквој безбедносној ситуацији у свету и у појединим земљама важно је видети и шта су испитаници из Србије одговорили на питање да ли су били жртве хакинга, а у вези са годинама старости и по величини места пребивалишта, као и упоређењем да ли жртве хакинга уопште знају шта је то.

Кад се упореде одговори испитаника, зависно од година старости и величине места пребивалишта, највећи проценат негативних одговора (75%) дали су они који живе у местима до 5000 становника и имају између 30 и 45 година, с тим што нико од њих није ни био жртва. Највећи број жртава хакинга било је у групи од 18 до 30 година, у местима до 5000 становника (23,2%). Следећа група која је била мета напада су млади испод 18 година, у градовима преко 500.000 становника (22%). На трећем месту су млади испод 18 година, из места до 5000 становника (20,6%). Они су и четврти кад су у питању места од 20.000 до 100.000 становника (20%). Очигледно је да су најугроженија категиорија млади до 18 година без обзира на величину места пребивалишта. Онда је јасно зашто је јавност забринута због учесталости и заступљености ове популације интернет корисника који су били жртве *sextortion* активности[636].

634 12 cybercimes a second: Beware rise in mobile app fraud, Russian anti-hacking czar warns, (2014), http://rt.com/news/cybercrime-victims-number-grow-427/, приступљено 25.4.2014;

635 Kaspersky Lab, (2013), Global Corporate IT Security Risks: 2013, http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf, приступљено 22.1.2014;

636 U.S. Attorney's Office, Public Affairs Specialist Laura Eimiller, (2013), Temecula Student Arrested in Sextortion Case Involving Multiple Victims, http://www.fbi.gov/losangeles/press-releases/2013/temecula-student-arrested-in-sextortion-case-involving-multiple-victims, приступљено 22.1.2014;

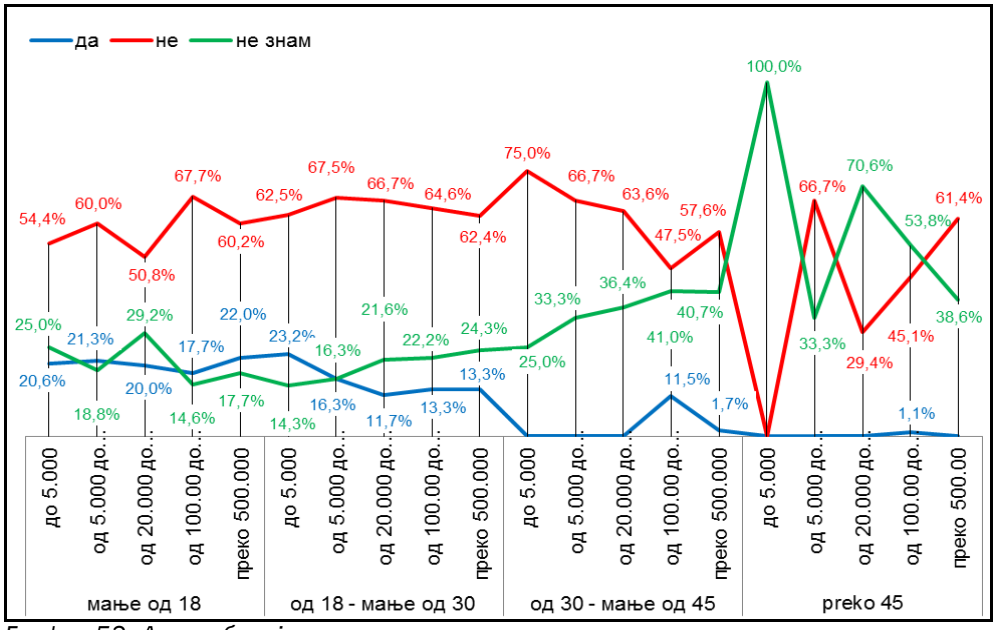


График 53. Дистрибуција одговора испитаника, по старости и величини места пребивалишта, као жртава хакинга

Испитаници који су били жртве хакинга одговорили су да знају шта је хакинг у 68,7% случајева, а њих 28% су чули, али не знају шта је. За оне који не знају да су били жртве 27,1% зна шта је хакинг, 40,3% је чуло, али не зна ништа о томе и 32,6% не зна шта је то.

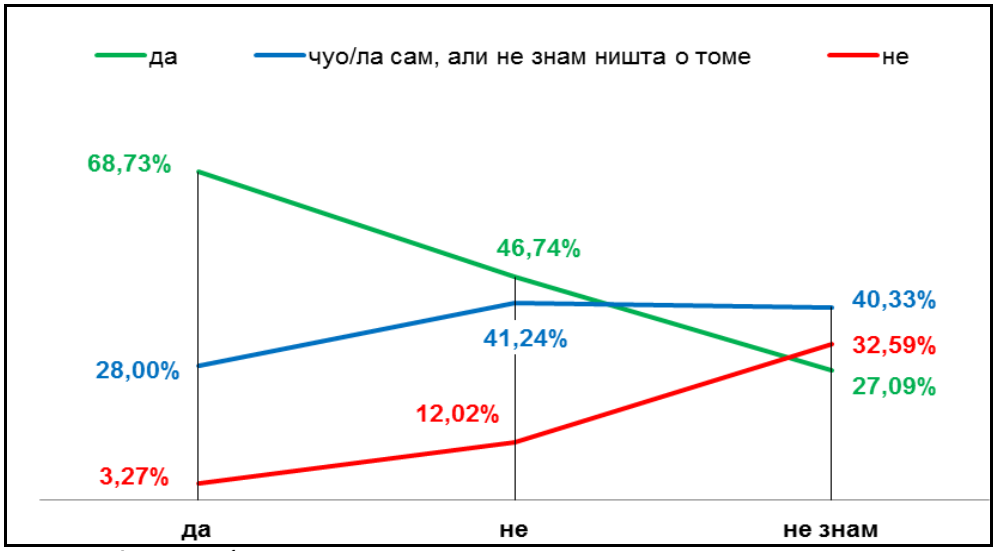


График 54. Дистрибуција одговора испитаника као жртава хакинга о познавању хакинга

3.3.2. Ставови о phishing-у

Phishing је врста социјалног инжењеринга (*social engineering*) који је у суштини врста преваре у оквиру које потенцијалне жртве откривају одређене податке о себи (банкарски рачун, корисничко име, лозинку, идентификациони, односно матични број, и слично)[637], а које се потом користе за друга дела cyber криминала. Од почетка 90-их, када су забележени први случајеви, до данас, *phishing* је постао један од најбрже растућег и забрињавајућег феномена. Тако је, на пример, само у јуну 2007. године Анти *phishing радна група* из САД-а (*Anti-Phishing Working Group - APWG*) примила 28.888 извештаја о *phishing*-у и идентификовала 31.709 посебних *phishing* сајтова, од којих је око 32% потицало из САД-а, а још 80% истрага се водило против 14 специфичних финансијских институција. Процене губитака потрошача од ових активности је тада био око 2,8 милиона долара годишње[638]. По извештају ове радне групе за почетак 2013. године[639] забележен је пад броја *phishing* напада. У јулу исте године се број попео на 49.480 откривених напада, у августу их је било мање (48.752), а у септембру се пад наставља (45.155)[640]. *APWG* у извештају за трећи квартал 2013. године констатује[641]:

- *phishing* активност генерално расту за 20%, иако је за 8% смањен број брендова који се нападају, с тим што је било најмање 115,565 *phishing* напада широм света, а то је готово 60% од напада у првом кварталу 2013. године;
- број уобичајених *phishing* напада опада, што може бити последица анти *phishing* реакација/акција*,* иако су били близу историјских токова у 2012. години;
- само око 2.3% од свих домена који су коришћени за *phishing* везан је за садржаје брендова, мада је број брендова који су на мети *phishing-a* драстично опао од априла (441) до септембра (379) 2013. године и са једним међупадом у јулу (390);
- тројанци и даље остају најчешће коришћени злонамерни софтвери – *malware* (више него црви, вируси, *adware*[642]*/spyware*) за *phishing, a* инфекције њима су достигле рекордне нивое (по подацима *Luis Corrons,*

637 McQuade C.S. III, (2009), op. cit;

638 McQuade C.S. III, (2009), op. cit;

639 *APWG*, (2013), Phishing Activity Trends Report, 1st Quarter 2013, http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf, приступљено 22.1.2014;

640 EMC&RSA (The Security Division of EMC), (2014), 2013 a Year in Review, January 2014, www.emc.com/rsa, констатује се „сведоци смо повећања од 160% у 2011. години која је била рекордна година ро обиму *phishing-a*. Иако није очекивано да ће 2012. довести до даљег смањења то се десило, али је 2013. донела повећање од око 1%. Праћење трендова *phishing-a* на кварталној основи показује његов константан раст током целе 2013. године, поготово у четвртом кварталу";

641 *APWG*, (2014), Phishing Activity Trends Report, 3rd Quarter 2013. Unyfing of Global Response to Cybercrime, https://www.google.rs/search?hl=sr&q=,+Phishing+Activity+Trends+Report,+3rd+Quarter+2013.+Unifying+of+Global+Response+to+Cybercrime&gbv=2&sa=X&as_q=&nfpr=&spell=1&ei=eV9oU5LfEcGGONOwglAL&ved=0CBwQvwU, приступљено 22.1.2014;

642 *advertising support software;*

PandaLabs Technical Director, Trends Report), рачуна се да је то скоро 80% свих инфекција (по подацима *PandaLabs* почетком 2013. године било је око 6,5 милиона злонамерних софтвера који су заразили око 31% свих рачунара на свету), а у 9 месеци 2013. године проценат је био већи него у целој 2012. години – 78%, с тим што је највећа инфекција забележена у Кини у којој је 59% рачунара заражено овим софтверима и одговорни су за 85% регистрованих *phishing* домена;

- 42% домена коришћених за *phishing* је .com али је то нешто мање него у претходном кварталу када их је било 44%;
- земље у којима је највећи проценат инфекције су, поред Кине, Турска, Перу и Русија;
- већина *phishing-a* је са хакованих или компромитованих веб-сервера из САД-а који је наставио да буде на врху држава у којима се они хостују (у првом кварталу је испред Немачке, Велике Британије, Канаде, Турске, Француске, Русије, Бразила, Литваније, Холандије), с тим што се у трећем кварталу на другом месту смењују Француска, Канада и Холандија, јер се велики проценат светских сајтова и домена у њима хостује;
- мете *phishing-a* су највише услуге плаћања јер се проценат повећао у односу на раније квартале и на финансијске услуге, а опао у односу на друштвене мреже (0,41%) и игре (0,8%, које, иначе, бележе највећи пад, од 5,7% у првом кварталу 2013. до 0,8% у трећем).

Табела 36. Статистика phishing-a у другом кварталу 2013. године

	July	August	September
Number of unique phishing websites detected	49,480	48,758	45,115
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	61,453	61,792	56,767
Number of brands targeted by phishing campaigns	390	400	379
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	35.24%	73.51%	56.22%
No hostname; just IP address	0.15%	3.20%	1.73%
Percentage of sites not using port 80	0.04%	0.32%	0.86%

Слика је мало другачија кад је у питању светски тренд. По истој радној групи, за другу половину 2013. године, карактеристично је[643]:

- било је најмање 115.565 напада широм света, што је повећање скоро 60% у односу на прву половину 2013. године, али мање од напада у другој половини 2012. када их је било 123.486, као резултат подељених виртуелних сервера на више домена;
- напади су били усмерени на 82.163 домена што је мање од 89.748 напада који су забележени у другом кварталу 2012. (број домена у свету је

643 Aaron G., Rasmussen R., (2014), Global Phishing Survey 2H2013: Uni fying the Global Response To Cybercr ime Trends and Domain Name Use, http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf, приступљено 20.2.2014;

порастао са 261 милиона у априлу 2013. године на 271.5 милиона у новембру исте године), због смањених хакинг инцидената на виртуелним серверима;

- детектовано је 2.394 напада на 837 IP адреса (не домена), с тим што је број напада који користе *IP* адресе остао стабилан за три и по године;
- од 53.685 *phishing* домена, идентификовно је 12.173 оних који су регистровани само због тога, дупло више него у другом кварталу 2012. године, што је последица наглог повећања кинеских домена, остали су скоро сви хаковани или компромитовани у оквиру рањивих веб-хостинга;
- просечна дужина *phishing* напада варира – почетком 2012. године је било 44 сата и 39 минута, у другој половини исте године 26 сати и 13 минута, да би почетком 2013. био 12 сати и 52 минута, а у другој половини те године 28 сати и 43 минута;
- *phishing*-ом је погођено 210 домена највишег нивоа (*TLD*), али и 89% регистрованих злонамерних домена (20.284) је у само 6 тих домена: *.com, .tk,* .pw, *.info,* .net, и .cf;
- само око 1,8% од свих домена који су коришћени за *phishing* садржао је брендове или њихова варијације;
- мета је било 681 институција, у првој половини 2013. године било их је 720 (скоро половина испитаника у другој половини узорка није била нападнута у другој половини 2013.), за разлику од другог квартала 2012. године када је било 611;
- мете су највише биле банке (32,9%), е-пословање (26,2%), трансфер новца (17,5%), друштвене мреже (16,8%) и други (6,6%);
- од 16 регистратора злонамерних домена 11 је из Кине, 3 из САД и по један из Индије и Немачке (по проценту на 10.000 регистрованих домена);
- 82 домена од 82.163 су интернационални домени (idns);
- коришћење *URL* за *phishing* се поново повећава (у првој половини 2013. године је опало).

Табела 37. Статистика светских трендова phishing-а у другој половини 2013. године[644]

	2H2013	1H2013	2H2012	1H2012	2H2011	1H2011
Phishing domain names	82,163	53,685	89,748	64,204	50,298	79,753
Attacks	115,565	72,758	123,476	93,462	83,083	115,472
TLDs used	210	194	207	202	200	200
IP-based phish (unique IPs)	837	1,626	1,981	1,864	1,681	2,385
Maliciously registered domains	22,831	12,173	5,833	7,712	12,895	14,650
IDN domains	82	78	147	58	36	33
Number of targets	681	720	611	486	487	520

644 Aaron G., Rasmussen R., (2014), op. cit;

Упоређујући *phishing* нападе и број нападнутих домена и злонамрних домена од 2010. до краја 2013. године, могу се констатовати осцилације у нападима (растао је од прве половине 2010. до прве половине следеће године, да би опао у другој половини 2011, а онда растао до друге половине 2012, кад је забележен и највећи пораст, па пад и пораст у 2013. и нападнутим доменима, као и у броју злонамерних домена.

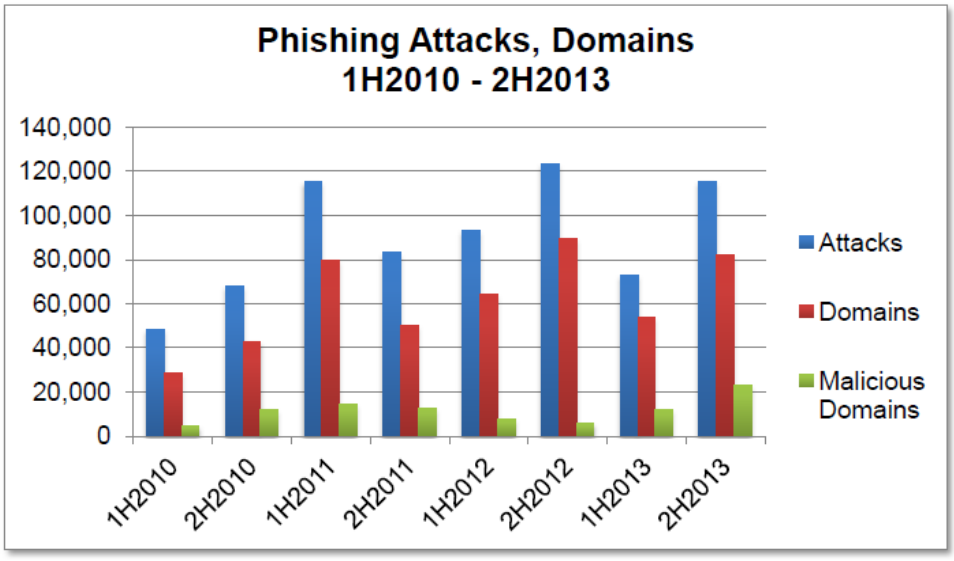


График 55. Број phishing напада, домена и злонамерних домена[645]

По светским статистикама домен *.rs* у другој половини 2013. године имао је 45 *phishing* напада, 37 домена са којих су вршени напади[646], 82.700 регистрованих домена, 4.5 напада на 10.000 регистрованих, 5.4 злонамерних домена на 10.000 регистрованих, 20.01 сати просечног трајања напада и 11.39 сати средњег времена трајања напада (Црна Гора је имала, нпр. 2077 напада, Македонија 23, Босна и Херцеговина 27, Хрватска 185, Словенија 92)[647].

Phishing је променио и своје карактеристике и *modus operandi*[648]. Тако је до средине 2003. године већина напада била преко текстова слатих електронском поштом у којима су били „лажни“ сајтови[649]. Често је комбинован са хакингом и

645 Aaron G., Rasmussen R., (2014), op. cit;

646 Највећи број напада сем са домена *.net* као генеричког (6340) има *Tokelay* (5251), који, такође, има и највећи број домена са којих се извршавају напади (5010), где је регистован и највећи број домена (20.109.953);

647 Aaron G. Rasmussen R. (2014), op. cit., pp 22-30;

648 Vijayashankar H. (2013), Modus Operandi of a Phishing Fraud, http://www.naavi.org/wp/?p=1072; Goh Guan Gan G. Nya Ling T. Choon Yih G. Cyril Eze U. (2008), Phishing: A Growing Challenge for Internet Banking Providers in Malaysia, Communications of the IBIMA, Volume 5, pp. 133 – 142., http://www.ibimapublishing.com/journals/CIBIMA/volume5/v5n17.pdf, приступљено 22.1.2014;

649 Kierkegaard S., (2008), Swallowing the bait, hook, line and sinker: Phishing, pharming and now ratting, по Goh Guan Gan G. Nya Ling T. Choon Yih G. Cyril Eze U., (2008), op. cit;

spam-ом. Временом се напади мењају[650]. Данас, захваљујући *cloud* инфраструктури лако променљиви и изнајмљивани *botnet* смањују трошкове масовних *phishing* кампања[651]. Сваки напад се добро планира и садржи неколико фаза:

Слика 11. Фазе phishing напада

У мајском истраживању у Србији, поред *phishing* напада који се дешавају и крећу са сајтова .rs домена, постављено је питање о његовом познавању, испитаници су одговарали у великом проценту да не знају (65,3%) или да су чули, али ипак не знају шта је то (25%). Зачуђујући мали број је оних који тврде да знају шта је *phishing*.

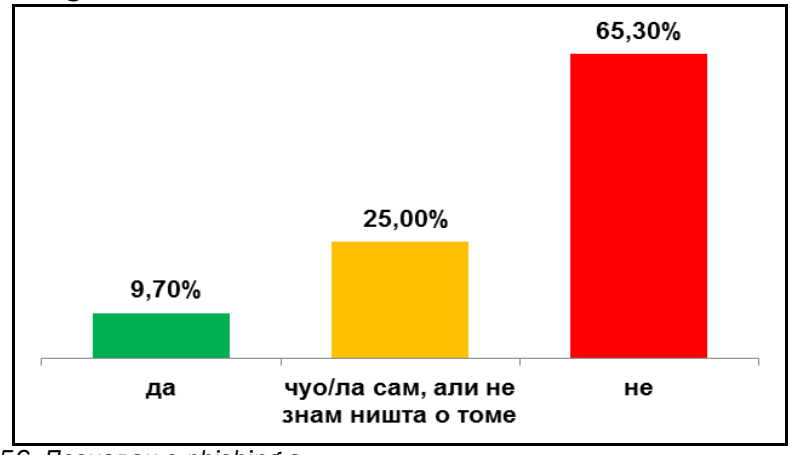


График 56. Познавање phishing-а

650 Sheng S. Holbrook M. Kumaraguru P. Cranor L. Downs J. (2010), Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interve, http://lorrie.cranor.org/pubs/pap1162-sheng.pdf, приступљено 22.1.2014;

651 Leonard C. (2013), New Phishing Research: 5 Most Dangerous Email Subjects, Top 10 Hosting Countries, https://community.websense.com/blogs/websense-insights/archive/2013/12/10/new-phishing-research-5-most-dangerous-email-subjects-top-10-hosting-countries.aspx, приступљено 22.1.2014;

Познавање *phishing*-а зависно од пола испитаника скоро се не разликује, односно минимално (од стране мушкараца) се разликује кад је у питању варијанта негативног одговора, па иако су чули/е не знају шта је то (25,%:25%). Нешто већа је разлика код потпуно негативног одговора (69,3%:61,6%), с тим да их је дало више испитаница него испитаника. Овакво стање је прилично зачуђујуће с обзиром на релативно велику присутност на интернету (и испитаница и испитаника) и малу разлику између њих (35%, односно 39% су свакодневно присутни до 5 сати). Испитаници, иако у малом проценту, знају више шта је *phishing* (13,4%) од испитаница (5,7%).

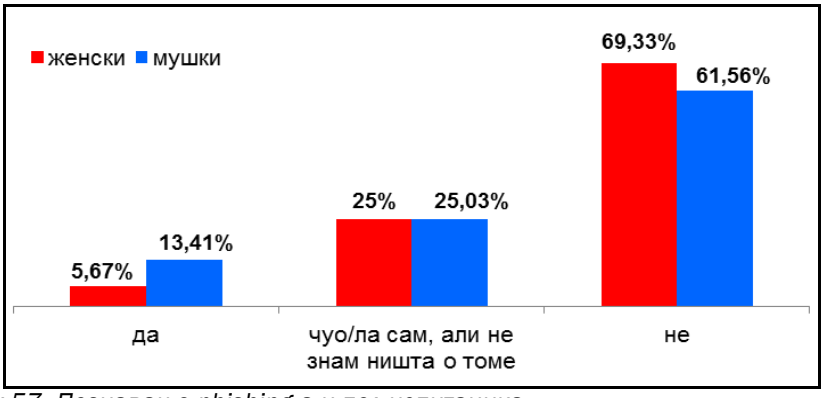


График 57. Познавање phishing-а и пол испитаника

Испитаници различитих година су различито одговарали на питање шта је *phishing*. Дистрибуција се креће од 62,2% (од 18 до 30 година) до 83,9% (преко 45 година). Ближа овој групи од 18 и 30 година је група од 30 до 45 (63,9%). Најмлађи нису и најекстремнији јер су се у 66,1% случајева изјаснили негативно.

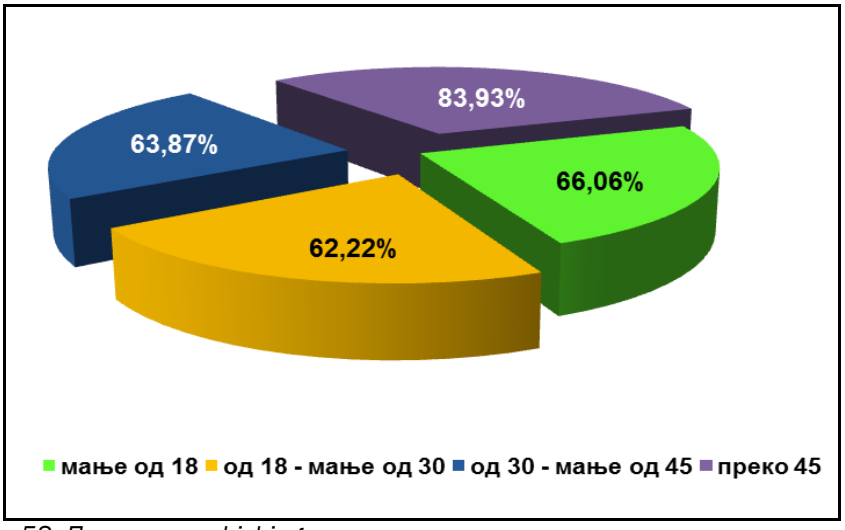


График 58. Познавање phishing-а и старост испитаника

О *phishing*-у највише знају они из места између 20.000 и 100.000 (10,63%) и између 100.000 и 500.000 становника. Најмање знања је код испитаника из места до 5000 становника. У великим градовима (изнад 500.000 становника) било је очекивано да су боље информисани о овом феномену и његовим опасностима, међутим нису (10%). Распон између 5,5% и 10,6% је толико минималан, али индикативан – испитаници у Србији изузетно мало знају о *phishing*-у. Овим бројкама могу се додати и оне који се односе на испитанике који су чули, али ништа не знају (28%). Потпуно негативни одговор дали су испитаници из места свих величина и крећу се између 63,7% (од 100.000 и 500.000) и 72,7% (до 5000). Очигледно је да су сви који би могли да утичу на ниво знања подбацили – од школа, факултета, родитеља до медија. Упоређењем знања о *phishing*-у и о хакингу, јасно је да је незнање много присутније код *phishing*-а.

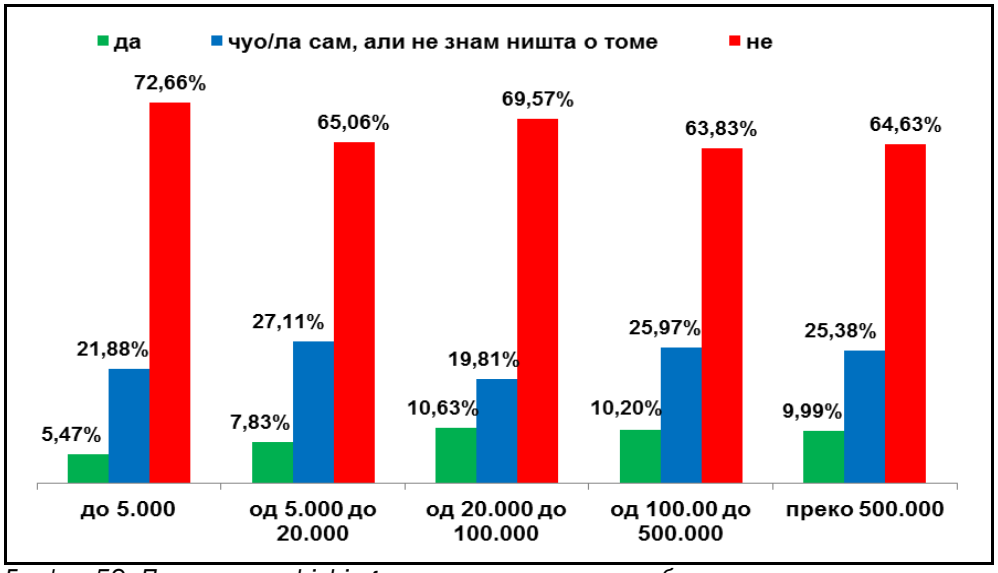


График 59. Познавање phishing-а и величина места пребивалишта испитаника

Наравно, још више забрињавају подаци о познавању *phishing*-а узети заједно, у зависности од пола и година старости. Најкритичније су испитанице старији од 45 година јер њих 91,3% не зна уопште шта је *phishing*. Испитанице су још лошије информисане, али је присутно и незнање – 28% младих испод 18 година женског пола се определило за овај одговор. Позитивног одговора у свим категоријама је изузетно мало, с тим што га ипак има, са незнатних 15,28% и то највише код мушкараца између 30 и 45 година. Најмање позитивних одговора дале су младе испитанице до 18 година, а највише између 30 и 45 година.

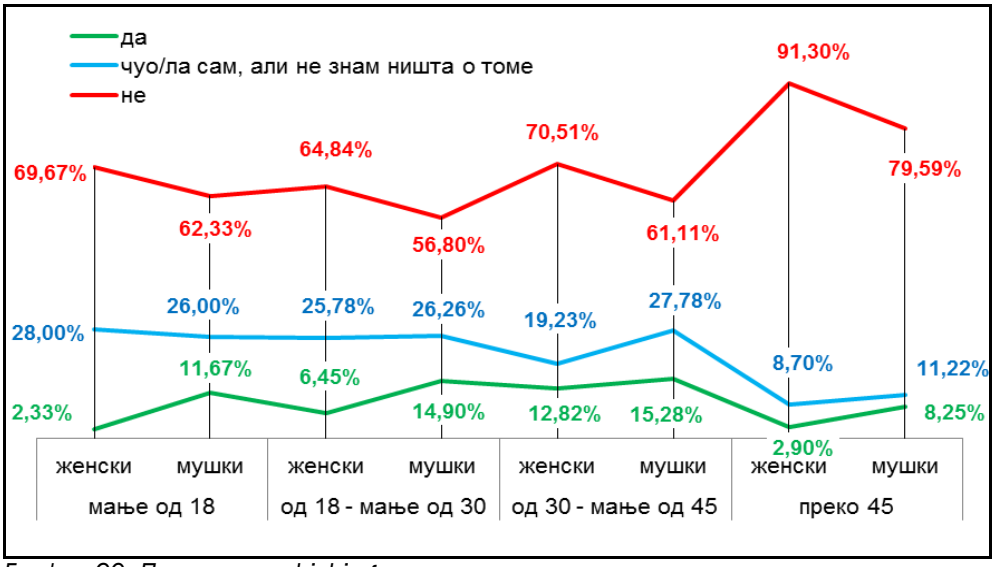


График 60. Познавање phishing-а, по полу и старости, испитаника

На питање "Да си су потребна специфична информатичка знања да би неко то радио?" испитаници су највише одговорили да не знају (57,8%) и мање је било одричних него потврдних одговора.

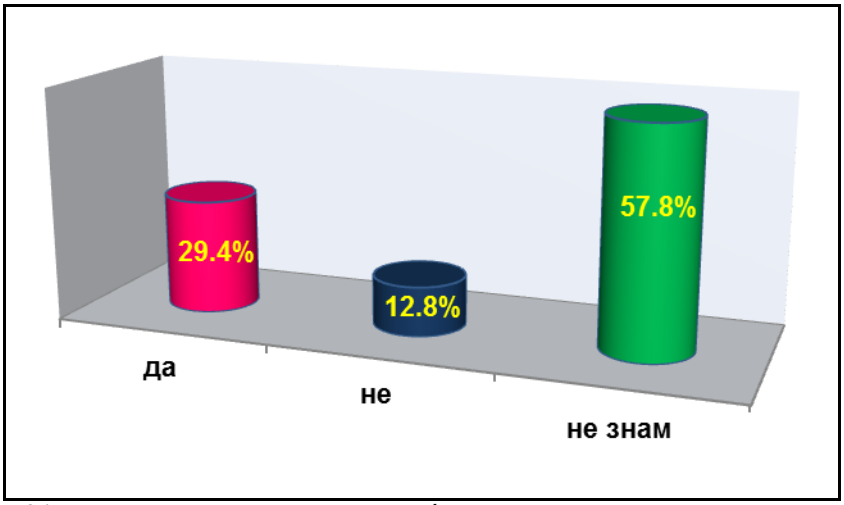


График 61. Мишљење испитаника о потреби специфичних информатичких знања за phishing

Одговор на ово питање који су дали испитаници, разликује се од одговора испитаница. Највише потврдних одговора дали су испитаници (35,0%), неки су се изјаснили и да не знају (49,6%), док су испитанице дале више одговора да не знају (66,4%).

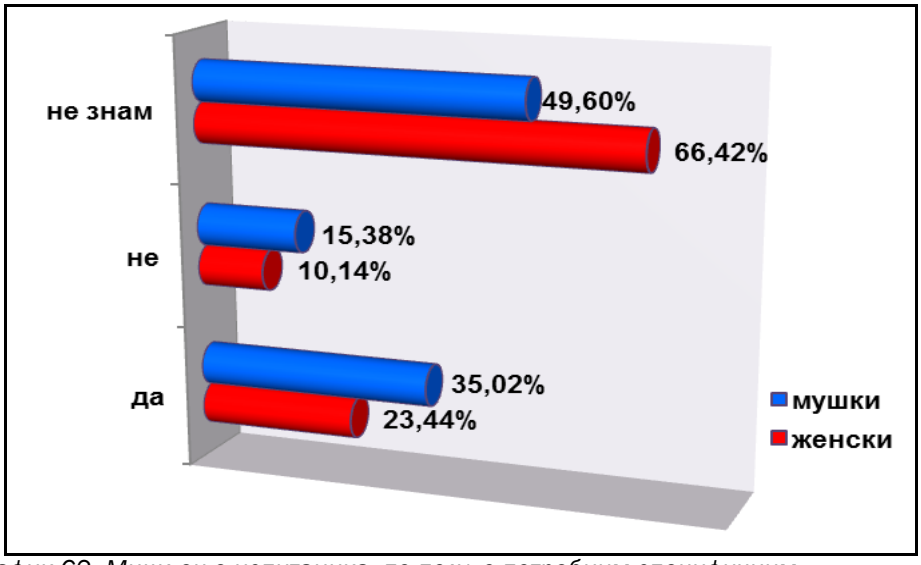


График 62. Мишљење испитаника, по полу, о потребним специфичним информатичким знањима за phishing

Ако се анализирају одговори на ово питање, али по годинама старости испитаника највише позитивних одговора дали су испитаници између 18 и 30 година (32,36%), затим следе млађи од 18 година (27,29%), нешто мање они између 30 и 45 година (26,9%), а најмање позитивних одговора дали су они преко 45 (18,45%).

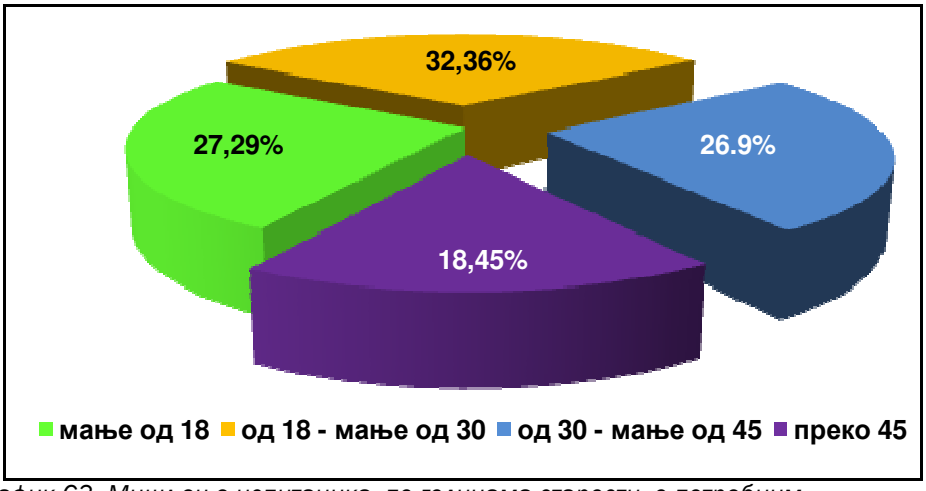


График 63. Мишљење испитаника, по годинама старости, о потребним специфичним информатичким знањима за phishing

Највише испитаника не зна да ли су за *phishing* потребна специфична информатичка знања (од 56,4% до 59,1%). Потврдно су највише одговорили

испитаници из места између 20.000 и 500.000 становника (30,0%), а најмање до 5.000 становника (26,8%). Негативни одговори су „нагомилани“ до 15%, само је један изнад (15,7%). Осцилације између одговора по величини места пребивалишта испитаника су веома мале.

Табела 38. Мишљење испитаника, по величини места пребивалишта, о потребним специфичним информатичким знањима за phishing

		Потребна су специфична информатичка знања			Тотал
		Да	Не	Не знам	
Број становника у месту у коме живите	до 5.000	26,77%	15,75%	57,48%	100%
	5.000 - 20.000	29,22%	11,69%	59,09%	100%
	20.000 - 100.000	28,97%	14,49%	56,54%	100%
	100.00 - 500.000	30,05%	13,46%	56,49%	100%
	преко 500.000	29,58%	11,67%	58,75%	100%

Кад се заједно посматрају мишљења испитаника по полу и годинама старости највише одричних одговора дали су испитаници између 18 и 30 (16%), а најмање испитанице преко 45 година (4,4%). Управо иста популација испитаника је дала одговор и да јесу неопходна специфична информатичка знања (37,4%), а једино код њих је присутан и одговор да не знају (испод 50%).

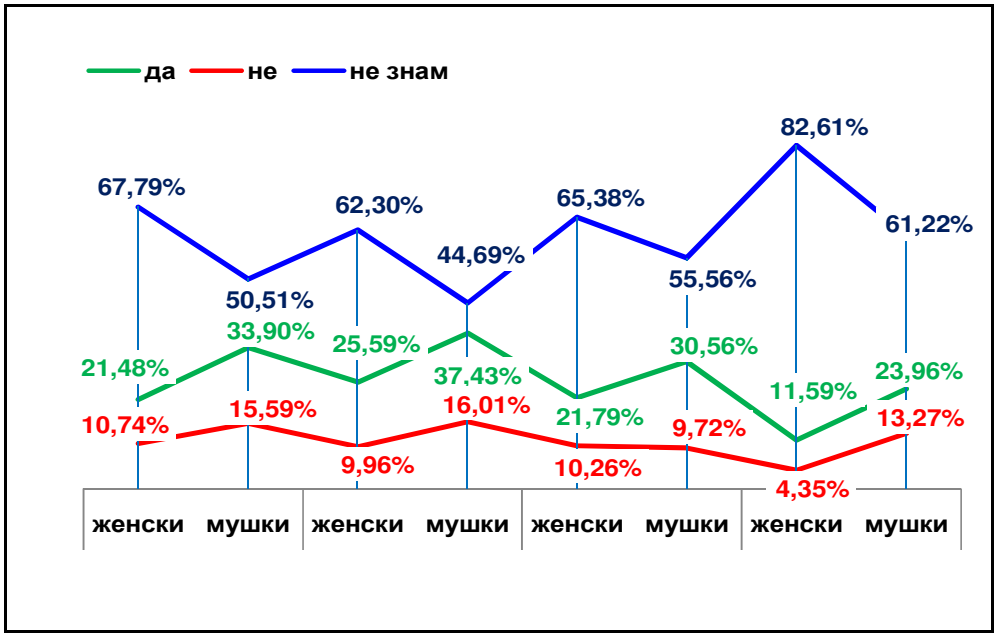


График 64. Мишљење испитаника, по полу и годинама старости, о потребним специфичним информатичким знањима за phishing

На питање да ли поседују та знања, већина испитаника је одговорила да не поседује (62%) или да не зна (30,7%). С обзиром да су за ово дело cyber криминала стварно потребна специфична информатичка знања, то указује да су испитаници у Србији свесни да их не поседују.

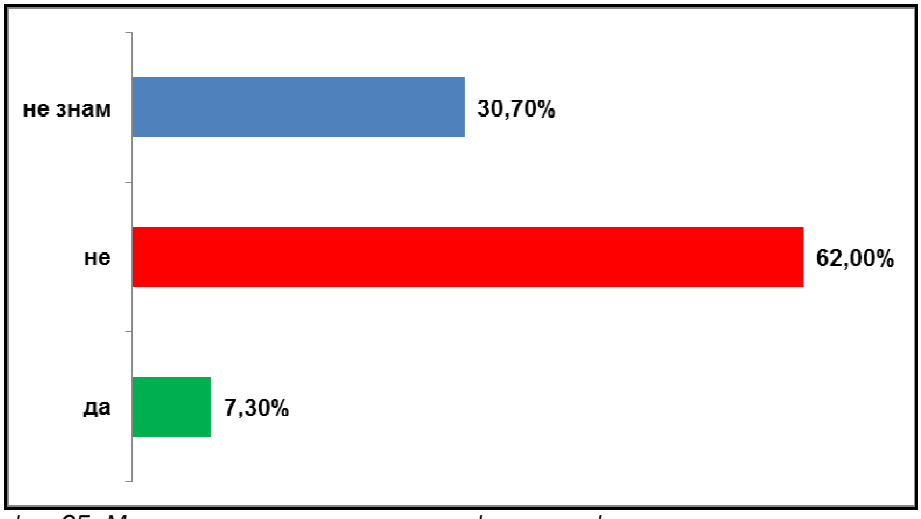


График 65. Мишљење о поседовању специфичних информатичких знања за phishing

На ово питање да ли поседују специфична знања више су одговориле испитанице (64,7%). Оне су више него испитаници одговориле да не знају (31,5%). Највише позитивних одговора дали су испитаници (10,6%).

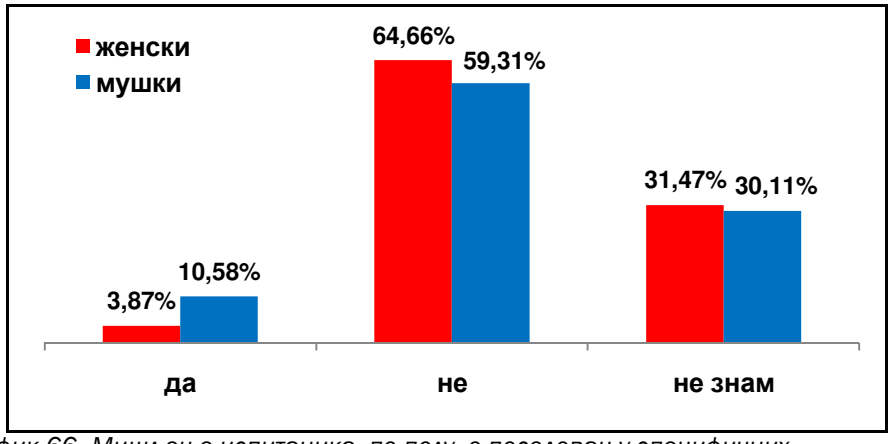


График 66. Мишљење испитаника, по полу, о поседовању специфичних информатичких знања за phishing

На исто питање, у зависности од година старости, највише су потврдно одговорили млади до 18 година, иако је и то мали проценат (чак испод 10%).

Највећи број свих испитаника је негативно одговорио (између 55% и 67%), док се одговори „не знам“ крећу између 27% и 37% у свим категоријама, односно највише, 36,71% код младих до 18 година. Иако су најчешћи корисници друштвених мрежа, али и игара (игрица), они су и најугроженија категорија, тако да поседовање знања за *phishing* истовремено значи да је то групација из које се регрутују нови *phishing* активисти, али и жртве. Следећа група је старија од 45 година.

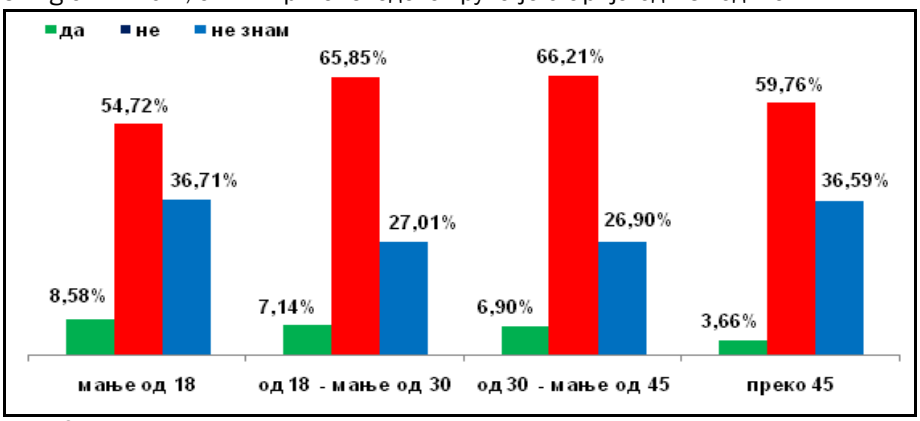


График 67. Мишљење испитаника, по годинама старости, о поседовању специфичних информатичких знања за phishing

Ако се анализирају одговори на питање да ли поседују специфична информатичка знања по величини места пребивалишта испитаника, најзаступљенији је одговор да не поседују и то у местима свих величина. Дистрибуција је између 55% и 69%, при чему је најнижи проценат код оних из места између 20.000 и 100.000 становника (55%), а највиши код испитаника из малих места величине до 5000 становника (68,8%), што је уз одговор не знам (24,8%), веома висок проценат. Највећи проценат испитаника који не знају је из места између 5000 и 20.000 становника (36%). Посебну пажњу неопходно је посветити испитаницима који су дали потврдан одговор, иако се сви проценти крећу испод 10%. Најнижи проценат (5,5%) је код испитаника из места преко 500.000 становника, што је зачуђујуће јер су њима разни медији најдоступнији. С друге стране, можда су они најсвеснији нивоа својих (не)знања.

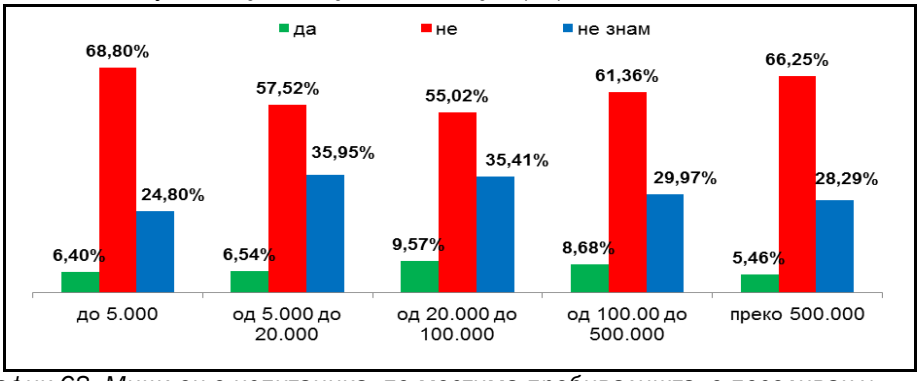


График 68. Мишљење испитаника, по местима пребивалишта, о поседивању специфичних информатичких знања за phishing

Посматрано заједно мишљења испитаника по полу и годинама старости, уочава се да је свест о незнању најјаснија код мушкараца између 30 и 45 година, а најмања код старијих од 45 година. Испитанице између 18 и 30 година су се највише определиле за одричан одговор (65,6%), а испитанице преко 45 година за одговор да не знају (40,6%).

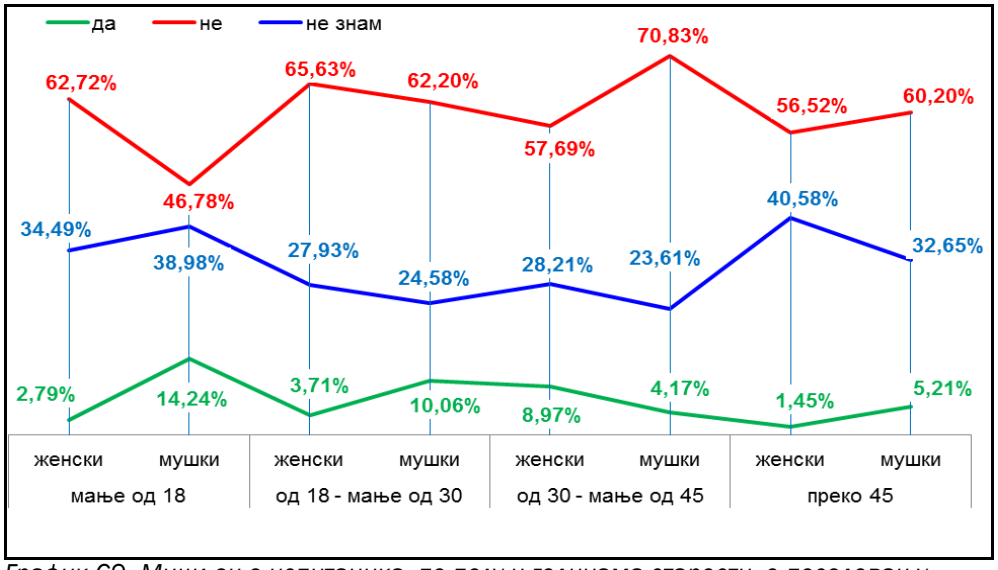


График 69. Мишљење испитаника, по полу и годинама старости, о поседовању специфичних информатичких знања за phishing

Позитивни одговори у односу на године старости и величину места пребивалишта испитаника су сконцентрисани на испитанике између 30 и 45 година старости, из места до 5000 становника (25%), с тим што нико од њих није одговорио да не зна (значи да су били децидирани: или их имају или не). Поседовање знања из *phishing*-а је најмање код испитаника из места између 5000 и 20.000 становника, старих између 30 и 45 година (0%), а минимална знања имају (1,7%) имају они из места преко 500.000 становника. Сви испитаници изнад 45 година и места до 5000 становника су одговорили да не поседују знања из *phishing*-а.

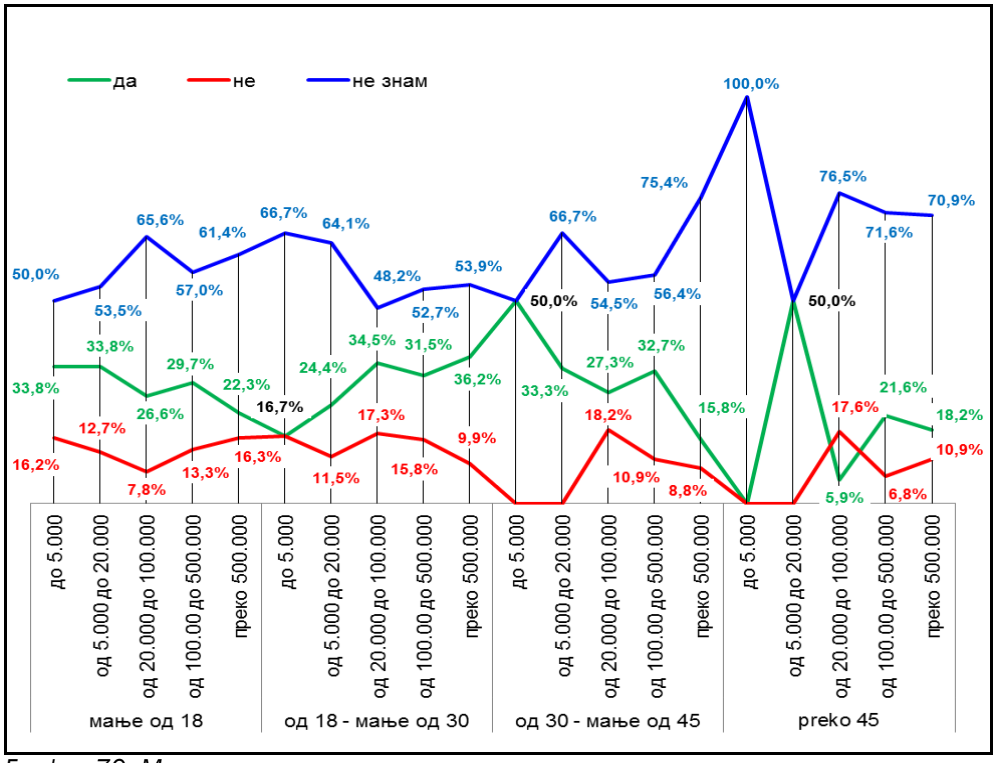


График 70. Мишљење испитаника, по старосним групама и величини места пребивалишта, о поседовању специфичних информатичких знања за phishing

На питање о томе да ли су били жртве *phishing*-а већина испитаника је одговорило да не зна (51,8%). Изузетно мали проценат (3,4%) је оних који су одговорили да су били жртве чиме су се уклопили и у податке о броју *phishing* напада у Србији и сајтова са којих напади крећу.

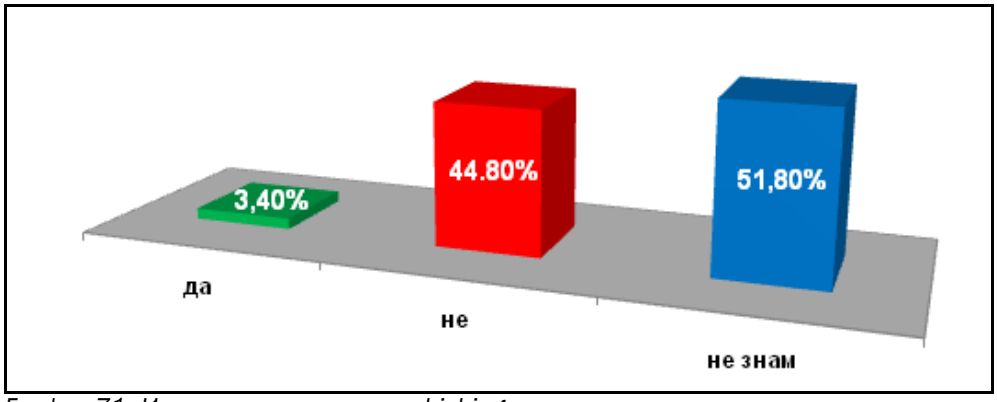


График 71. Испитаници као жртве phishing-а

Највећи проценат испитаника оба пола је одговорио да не знају да су били жртве *phishing*-а (жене 55,8%, мушкарци 48%) што кореспондира са њиховим непознавањем овог феномена. Испитаници су скоро исто (само за 0,3% разлике) одговорили да не знају и да нису били жртве.

Табела 39. Испитаници, по полу, као жртве phishing-а

		Да ли сте некада били жртва phishing-а?			Тотал
		Да	Не	Не знам	
Пол	Женски	3,87%	64,66%	31,47%	100%
	Мушки	10,58%	59,31%	30,11%	100%

Посматрано по старосним групама испитаници су више од 50% одговарали да не знају да су били жртве, изузев оних до 18 година чији су одговори минимално били испод овог процента (48,9%). Да нису били жртве *phishing*-а испитаници су готово уједначено одговарали од 39,8% (преко 45 година) до 46,6% (до 18 година).

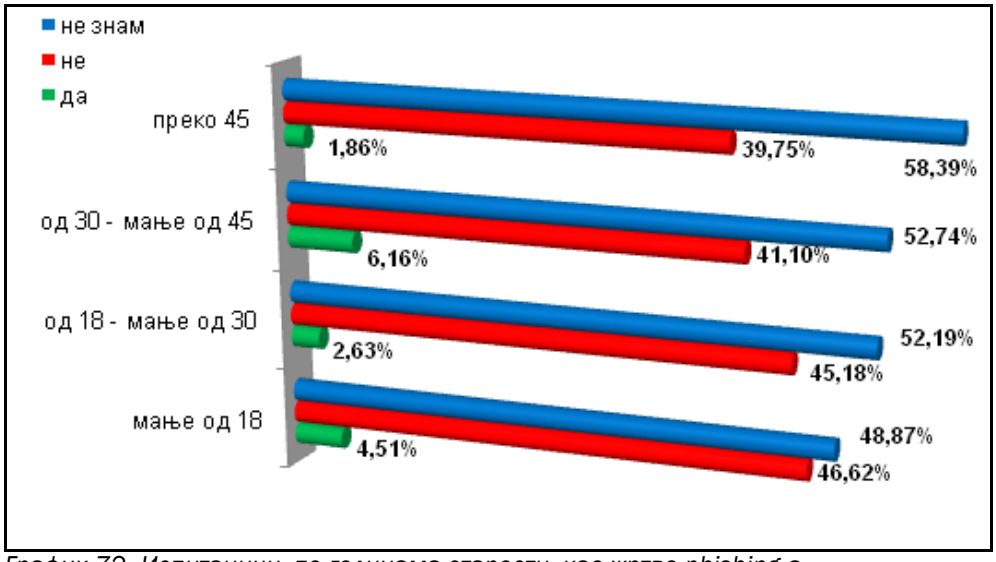


График 72. Испитаници, по годинама старости, као жртве phishing-а

Структура одговора на питање да ли су били жртва *phishing*-а, зависно од величине места пребивалишта испитаника, указује да су доминантни одрични одговори за места од 5000 до 20.000 становника, јер у местима са више од 20.000 становника најчешћи одговор је да не знају да су били жртва (50% и > %).

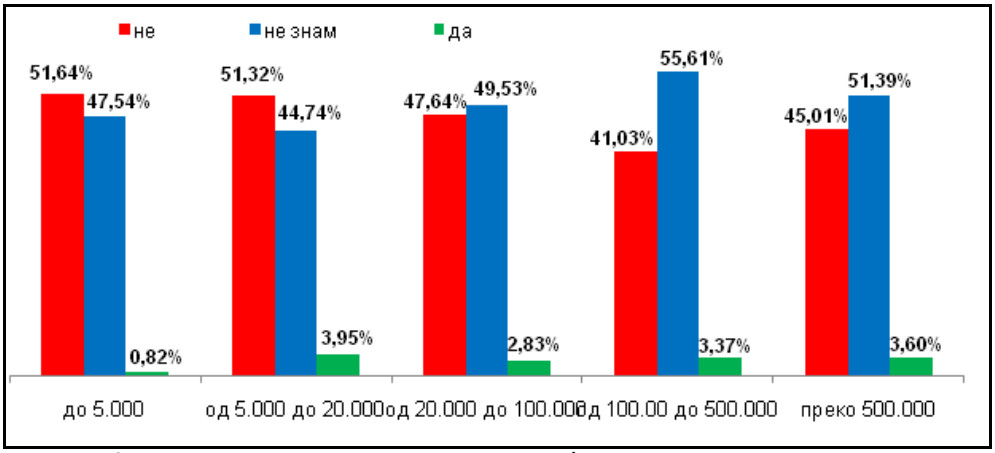


График 73. Испитаници, по величини места пребивалишта, као жртве phishing-а

Када се анализирају заједно одговори по полу и годинама старости испитаника, доминантни су одговори „не знам“ и „нисам“. Мало их је одговорили да јесу, с тим што су се мушкарци до 18 година највише изјаснили да су били жртве, мада је и то изузетно мали проценат (6,8%). Жене од 30 до 45 године старости су се мање (6,4%) изјасниле да су биле жртве *phishing-а.*

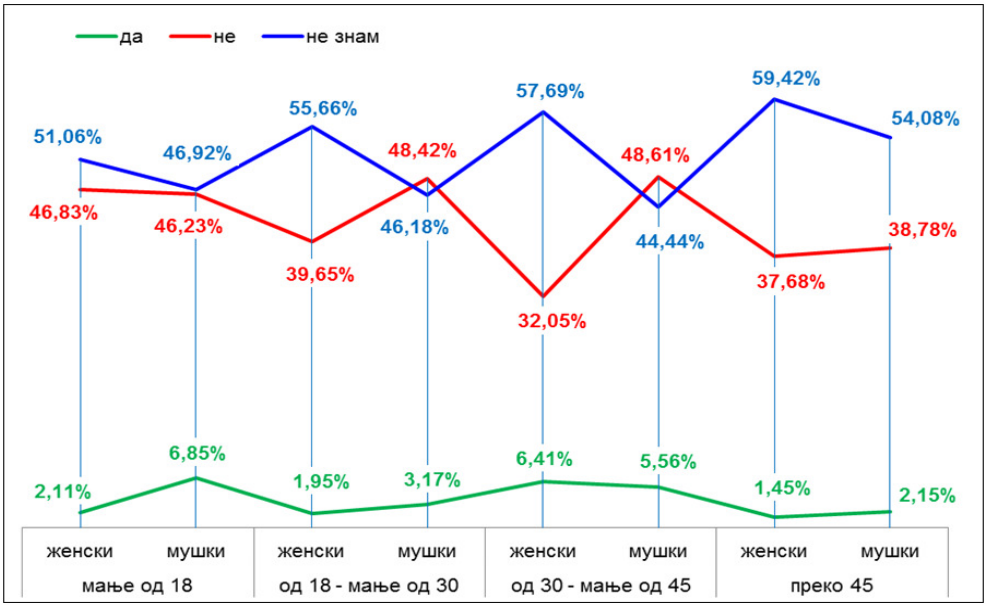


График 74. Испитаници, по полу и годинама старости, као жртве phishing-а

Ако се прате одговори на исто питање, али заједно по полу и величини места пребивалишта сазнање да су били жртве имају у процентима већим од 6% само мушкарци из места између 5000 и 20.000 становника (6,5%) и преко 500.000 (6,3%).

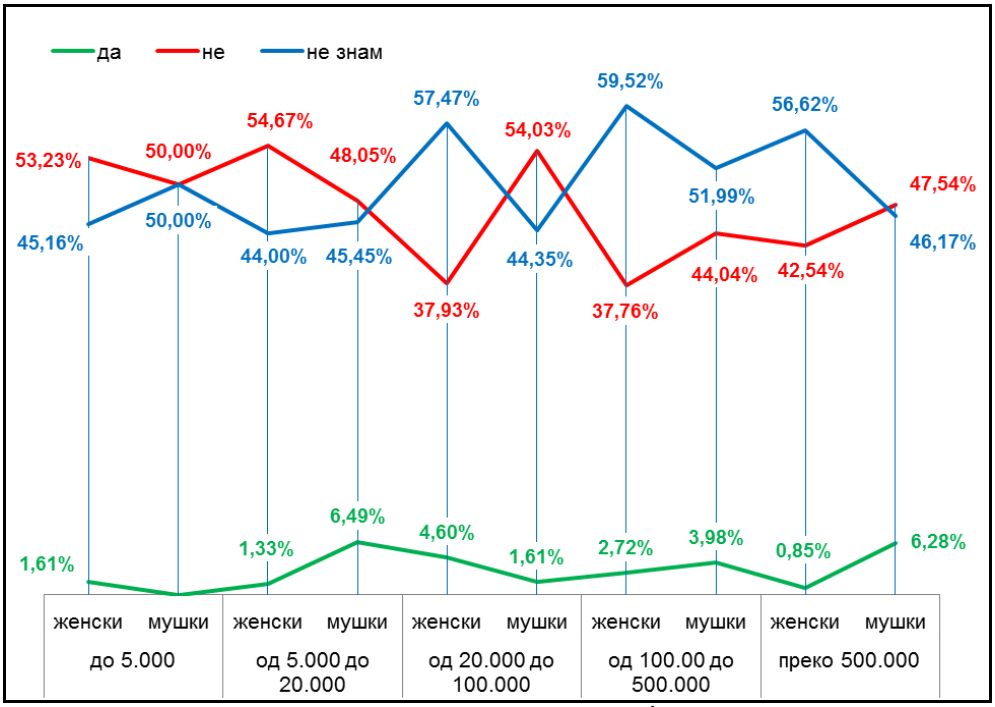


График 75. Испитаници, по полу и величини места пребивалишта, као жртве phishing-a

Значи, сви испитаници имају веома мало сазнања да ли су или не били жртве *phishing*-а.

3.3.3. Ставови о cyber малтретирању

Присутни смо развоју малтретирања или злостављања већ неколико векова. Тачније, реч *bully*[652] потиче из 1530. године, а од XIX века означава директно (*peer-to-peer*) узнемиравање „укључујући две особе, насилника и жртву“[653]. Феномен cyber малтретирања појавио се са интернетом, а замах добио са мобилним телефонима и

652 Реч *bully* - насилник/силација, појављује се у холандском језику (broeder "*brother*"), слично у немачком (buole "*brother*") где је означавала "љубавника, брата". У оригиналу је значила "душу/драгог" и примењивала се на оба пола. У 17. веку добија значење "финог момка" и "хвалисавца" па потом "узнемиравача слабијих" (грубијан, силеција). Касније се везује за „бика“, да би временом добијала значење "љубавника", затим "силецију", "заштитника проститутки". Израз добија изначење "достојан дивљења, весео," (1864. године у САД-у употребљава се сленг израз „bully for you!“). Реч *bullying*, у данашњем смислу, почиње да се користи од 1802. године, Harper, D. (2008), *Online etymology dictionary,* http://www.etymonline.com/index. php?allowed_in_frame =0&search=bully&searchmode=none, приступљено 23.1.2014;

653 Donegan R. (2012), Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis, http://www.elon.edu/docs/e-web/academics/communications/research/vol3no1/04DoneganEJSpring12.pdf, приступљено 22.1.2014;

друштвеним мрежама. То је појава која је изазвала многе дебате и дискусије, несугласице у одлукама судова, али и промене у националним законодавствима. Нпр. у САД-у[654], од октобра 2010. године 49 федералних држава је донело законе против малтретирања, 20 против cyber малтретирања и у 5 је у припреми, као и федерални[655] закон, као и у Канади, Финској, Сингапуру[656], на Филипинима[657], док је у Аустралији у току потписивање петиције за његово доношење[658]. ЕУ, УН[659], УНИЦЕФ[660] предузимају заједничке акције у регулацији овог облика cyber криминала полазећи од премисе да cyber малтретирање представља облик малтретирања/злостављања коришћењем информационо-комуникационих технологија и да су најугроженија деца, тинејџери, млади адолесценти[661]. Формирају се различите формалне и неформалне, државне и невладине организације, асоцијације, савети, алијансе, а све у циљу спречавања, информисања, едуковања, усаглашавања заједничких акција, пријављивања, регулисања ове појаве. У неколико протеклих година обављају се опсежна истраживања о учиниоцима, жртвама, узроцима, факторима, облицима (умрежавање сајтова, текстуалне поруке, "*sexting*"[662], инстант поруке)[663] размерама cyber малтретирања. Посебно се проучавају специфичне групе[664] које су жртве ове

---

654 Hinduja S. Patchin W.J. (2014), State Cyberbullying Laws, A Brief Review of State Cyberbullying Laws and Policies, http://www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf;

655 Назван и *Megan Meier Cyberbullying Prevention Act* (*Megan Meier* је била четрнаестогодишња жртва cyber малтретирања преко MySpace 2006. године), H. R. 1966, A BILL To amend title 18, United States Code, with respect to cyberbullying, (2009), http://www.gpo.gov/fdsys/pkg/BILLS-111hr1966ih/pdf/BILLS-111hr1966ih.pdf, приступљено 18.1.2014;

656 Singapore to legislate against cyber bullies, (2014), http://www.out-law.com/articles/2014/march/singapore-to-legislate-against-cyber-bullies/, приступљено 18.1.2014;

657 Republic of the Philippines, (2013), An Act Requiring All Elementary And Secondary Schools To Adopt Policies To Prevent And Address The Acts Of Bullying In Their Institutions, http://www.gov.ph/2013/09/12/republic-act-no-10627/, приступљено 18.1.2014;

658 Mastronardi E., (2014), Charlotte's Law - Tougher Cyber Bullying Legislation, https://www.change.org/en-AU/petitions/malcolm-turnbull-charlotte-s-law-tougher-cyber-bullying-legislation, приступљено 26.2.2014;

659 У 2009. години у оквиру УН организован је семинар везан за говор мржње и Cyber малтретирање, 2009. Unlearning Intolerance Seminar Cyber Hate: Danger in Cyber Space, http://www.un.int/wcm/content/site/ui/, приступљено 19.1.2014;

660 UNICEF Canada, (2012), Bullying And Cyberbullying: Two Sides of the Same Coin, Brief submitted by UNICEF Canada to the Standing Senate Committee on Human Rights, http://www.unicef.ca/sites/default/files/imce_uploads/TAKE%20ACTION/ADVOCATE/DOCS/cyberbulling_submission_to_senate_committee.pdf, приступљено 19.1.2014;

661 Јединствене дефиниције у законима и другим правним актима, за сада нема, али се убрзано ради на томе да се то превазиђе, Williams C.J. (2010), Court tightens definition of cyber-bullying, Appellate panel rules 2 to 1 that hostile comments left on a Harvard-Westlake School student's website aren't protected by the 1st Amendment, http://articles.latimes.com/2010/mar/18/local/la-me-cyber-speech18-2010mar18, приступљено 19.1.2014;

662 "Sexting" означава дељење сексуално сугестивних текстуалних порука или слика помоћу електронског уређаја;

663 Standing Senate Committee on Human Rights, (2012), Cyberbullying Hurts: Respect for Rights in the Digital Age, http://www.parl.gc.ca/Content/SEN/Committee/411/ridr/rep/rep09dec12-e.pdf, приступљено 19.1.2014;

664 Након пуцања у школи 1999. године почиње да се прати ова појава као озбиљан проблем, Arseneau C. The History of Cyberbullying, http://www.ehow.com/about_6643612_history-cyberbullying.html, приступљено 19.1.2014;

појаве[665]: жене, деца/млади, *LGBT* популација, црнци, психички болесници, хендикепирани[666] и његови ефекти, односно последице[667].

У истраживању *Ditch the Label*[668] из 2013. године анкетирано је преко 10.000 младих у Великој Британији и констатовано[669]:

- 7 од 10 младих људи су били жртве cyber малтретирања;
- 37% младих људи се често суочава са овим видом малтретирања;
- 20% младих свакодневно доживљава неки екстремни облик cyber малтретирања;
- нова истраживања показују да су од њега подједнако угрожени млади мушкарци и жене;
- два пута су веће шансе да буду угрожени од cyber малтретирања млади на *Facebook*-у него на било којој другој друштвеној мрежи;
- 54% младих људи који користе *Facebook* су изјавили да су доживели cyber малтретирања на овој мрежи;
- утврђено је да су друштвене мреже *Facebook, Twiter, Ask, Snapchat*[670] највероватнији извори cyber малтретирања;
- cyber малтретирање, како је утврђено, има катастрофалне последице на самопоштовање и друштвени живот до 70% младих;
- процењује се да је 5,43 милиона младих људи доживело неки вид cyber малтретирања, а да је 1,26 милиона изложено свакодневном изузетном cyber малтретирању.

У истој земљи, на основу владиних извештаја и спроведених истраживања[671], све је већи број младих и деце који пријављују случајеве и покушавају да се извуку из „круга cyber малтретирања".

На европској конференцији одржаној 2013. године у Мадриду, у организацији *The Confederation of Family Organisations in the European Union - COFACE*[672],

665 Parr M. Dagley J. Pogrund A. MacDonell L. (2012), Bullying: A Report from the Huntington Beach Human Relations Task Force, http://www.surfcity-hb.org/government/boards_commissions/pdf-files/2800-May-2012-Bullying-Report.pdf, приступљено 19.1.2014;

666 Aune N. (2009), Cyberbullying, http://www2.uwstout.edu/content/lib/thesis/2009/2009aunen.pdf, приступљено 25.1.2014;

667 Siderman M.L., (2013), Pathways to Cyber Bullying from Bystander to Participant: Secondary School Students' Perspectives, http://www.cybersmile.org/resources/155/Pathways-to-Cyber-Bullying-from-Bystander-to-Participant_-Seconda.pdf, приступљено 25.1.2014;

668 Ditch the Label, (2013), The annual cyberbullying survey, http://www.ditchthelabel.org/annual-cyber-bullying-survey-cyber-bullying-statistics/, приступљено 25.1.2014;

669 У 2012. години: 46% деце и младих су изјавили да су били малтретирани у школи; 38% деце са инвалидитетом је било забринуто да ће бити злостављани; преко половине (55%) лезбејки, гејева и бисексуалних младих људи су искусили хомофобична шиканирања у школи; 82% њих су покушали да интервенишу; Statham H., (2012), The experiences of gay young people in Britain's schools in 2012, http://www.stonewall.org.uk/documents/school_report_2012(2).pdf, приступљено 25.1.2014;

670 Cyber bullying trends force parents to keep up, (2013), http://www.stuff.co.nz/dominion-post/news/9251149/Cyber-bullying-trends-force-parents-to-keep-up, приступљено 22.3.2014;

671 Statistics on bullying, (2013), http://www.nspcc.org.uk/Inform/resourcesforprofessionals/bullying/bullying_statistics_wda85732.html, приступљено 22.3.2014;

672 Conference report, (2013), European conference on cyberbullying, http://deletecyberbullying.files.wordpress.com/2013/09/euconference-cyberbullying-28-may-madrid-conference-final-report1.pdf, приступљено 23.3.2014;

размењивана су искуства жртава овог облика малтретирања, али и начина како се у земљама ЕУ боре против ове појаве. Анализирани су резултати Извештаја *Family Online Safety Institute's - GRID* у оквиру кога је идентификовано 26 глобалних ризика и изазова, а ризик број један је cyber малтретирање[673].

У Европској унији је 2010. године формирана радна група *ENISA* (*The European Network and Information Security Agency*), а 2011. објављен документ *Cyber-Bullying and online Grooming: helping to protect against the risks, A scenario on data mining / profiling of data available on the Internet*[674].

Како истиче *Justin W. Patchin* истраживање презентирано 9. априла 2014. године у облику докумена *Summary of Our Research (2004-2014)*[675] на сајту cyberbullying.us указује да су „прикупљени подаци од ученика/студената средњих и високих школа од 2002. године, да је анкетирано скоро 15.000 појединаца широм САД. У графиконима су приказани проценти испитаника који су доживели cyber малтретирање".

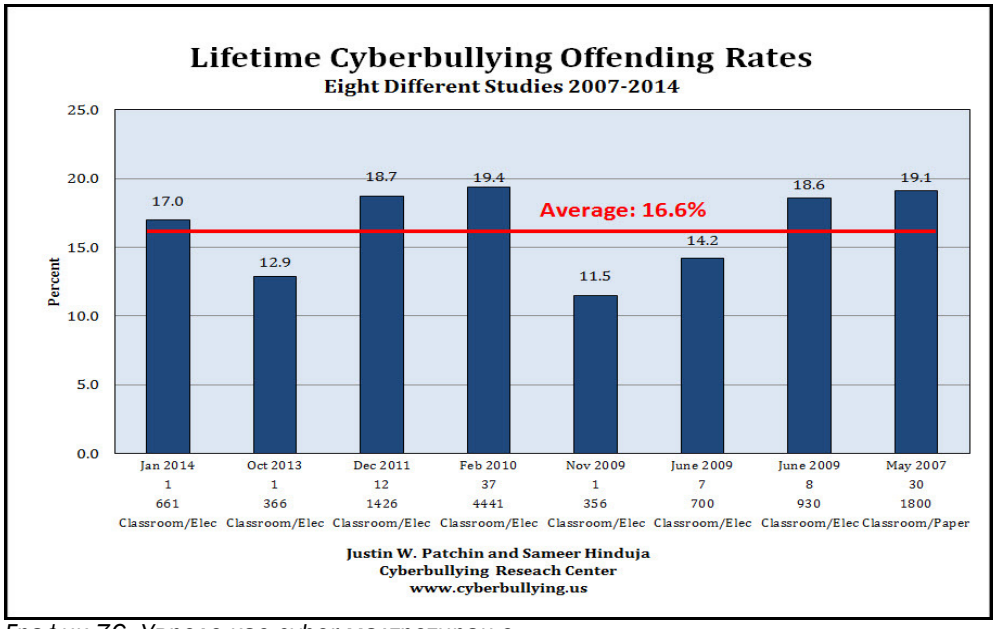


График 76. Увреде као cyber малтретирање

Стопа виктимизације је варирала током година. У просеку око 25% појединаца су изјавили да су били жртве, с тим да је почетком 2014. године то било 34,6%, у мају 2007. године 18,8%, а у фебруару 2012. је било 20,8%.

673 GRID Report: Q1 2014, http://www.fosigrid.org/files/fosigrid-q1-2014-report.pdf, приступљено 23.1.2014;

674 ENISA, (2011), New report: Cyber bullying & online grooming: 18 protective recommendations against key risks, http://www.enisa.europa.eu, приступљено 23.3.2014;

675 http://cyberbullying.us/summary-of-our-research/;

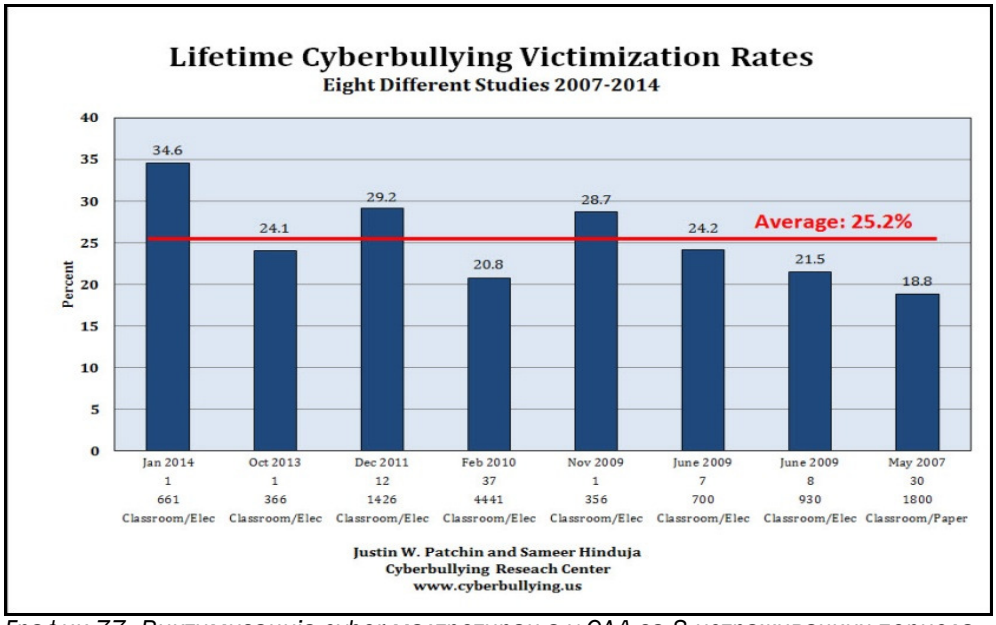


График 77. Виктимизација cyber малтретирања у САД за 8 истраживачких периода

Као и у многим другим земљама и у Србији постоје случајеви cyber малтретирања. О њима се много више извештава у медијима него што се покрећу истражне и судске процедуре. Ипак, велики помак у приступу малтретитању/злостављању настаје 2010. године када је донет **Правилник о Протоколу поступања у установи у одговору на насиље, злостављање и занемаривање**[676] у коме су, поред осталог, дефинисани: установа (предшколска установа, основна и средња школа и дом ученика); простор установе (простор у седишту и ван седишта установе у ком се остварује васпитно-образовни, образовно-васпитни и васпитни рад, као и друге активности установе); обезбеђење услова за сигурно и подстицајно одрастање и развој детета и ученика (заштита од свих облика насиља, злостављања и занемаривања и социјална реинтеграција детета и ученика које је извршило, односно било изложено насиљу, злостављању или занемаривању); забрана насиља, злостављања и занемаривања у установи, насиље и злостављање (сваки облик једном учињеног, односно понављаног вербалног или невербалног понашања које има за последицу стварно или потенцијално угрожавање здравља, развоја и достојанства личности детета и ученика или запосленог); ко чини насиље и злостављање (запосленог према детету, ученику, другом запосленом, родитељу, односно старатељу или другом лицу које је преузело бригу о детету и ученику, детета и ученика према другом детету и ученику или запосленом; родитеља према свом детету, другом детету и ученику и према запосленом); облик насиља и злостављања (физичко, психичко/емоционално и социјално, електронско) и друго. Оно што је изузетно битно дефинисано је и **електронско насиље и злостављање** *као злоупотреба информационих технологија*

676 Правилник о Протоколу поступања у установи у одговору на насиље, злостављање и занемаривање, Службени гласник РС, бр. 30/2010;

која може да има за последицу повреду друге личности и угрожавање достојанства и остварује се слањем порука електронском поштом, СМС-ом, ММС-ом, путем веб-сајта (web site), четовањем, укључивањем у форуме, социјалне мреже и слично. Поред овог акта донети су и други који на посредан или непосредан начин регулишу овај феномен.

Слика 12. Регулација cyber малтретирања у Републици Србији

Од конкретних мера интересантан је пројекат Центра за превенцију девијантног понашања „Таргет“ из Новог Сада, *„Електронске дроге – превенција сајбер злостављања“*. Рађена су разна истраживања од стране различитих субјеката (нпр. 2009. тадашње Министарства за телекомуникације и информационо друштво, Ебарт консалтинг и слично) или УНИЦЕФА *„Школа без насиља – ка сигурном и подстицајном окружењу за децу*[677].

Све је више сајтова на којима се разматра овај проблем, објављују подаци, постављају чланци, објашњења, упозорења, упутства за децу/младе, родитеље, просветне раднике, друге субјекте[678].

У истраживању обављеном у мају 2013. године у Србији је постављано и питање везано за електронско малтретирање (са 10 понуђених одговора - 8 потврдних и 2 одрична). Скоро 90% испитаника је одговорило да нису били жртве, али знају да су то неки доживели (53,5%) и да никад нису за то чули (35,7%). Остали понуђени одговори су изузетно мало бирани. Треба поменути и 3 одговора који су преко 2%: да, гледао/ла сам више пута клипове и фотографије малтретирања (2,9%); да, „шалимо“ се често због разних „глупости“ које неки постављају (2,5%) и 2,1,% испитаника је одговорило да је учествовало о томе, што је крајње

677 Попадић Д. (2009), Насиље у школи, Институт за психологију, УНИЦЕФ; www.unicef.rs/files/nasilje-u-skolama-za-web.pdf, приступљено 23.3.2014;

678 Нпр. http://nasaucionica.wordpress.com/2012/04/26/drustvene-mreze-i-bezbednost-dece/; https://bezbedannet.wordpress.com/tag/cyber-bullying/; http://www.sbn.rs/za-ucenike/digitalno-nasilje-6; http://kliknibezbedno.wordpress.com/2013/05/27/e-nasilje/, приступљено 23.3.2014;

забрињавајуће[679]. Иако мали, ови проценти одражавају, с једне стране, ниво развоја и пенетрације интернета и других информационо-комуникационих технологија, а са друге, да се у Србији овај облик понашања на интернету појављује и да није редак. То је свакако последица утицаја разних фактора и може се тумачити са одговарајућим „паралелама“:

- да се насиље, па и cyber, учи;
- да корене често вуче из породице или групе;
- да може бити резултат дејства социокултурних утицаја;
- да постоје генетске предиспозиције и слично[680].

Ако се томе додају и подаци из страживања из 2009. године по коме: 36% ученика одговора на поруке непознатих особа, 58% их је прихватило позив за пријатељством од непознатих особа, 11% их је бар једном изашло на састанак са непознатом особом, **12% их је искусило насиље на интернету**, 8% је искусило снимање мобилним телефоном, 7% је примило узнемиравајуће поруке и 12% је примило узнемиравајуће поруке преко телефона и **84% је било пасивни посматрач дигиталног насиља**[681], очигледно је да су млади изузетно угрожени, али и необавештени или несвесни.

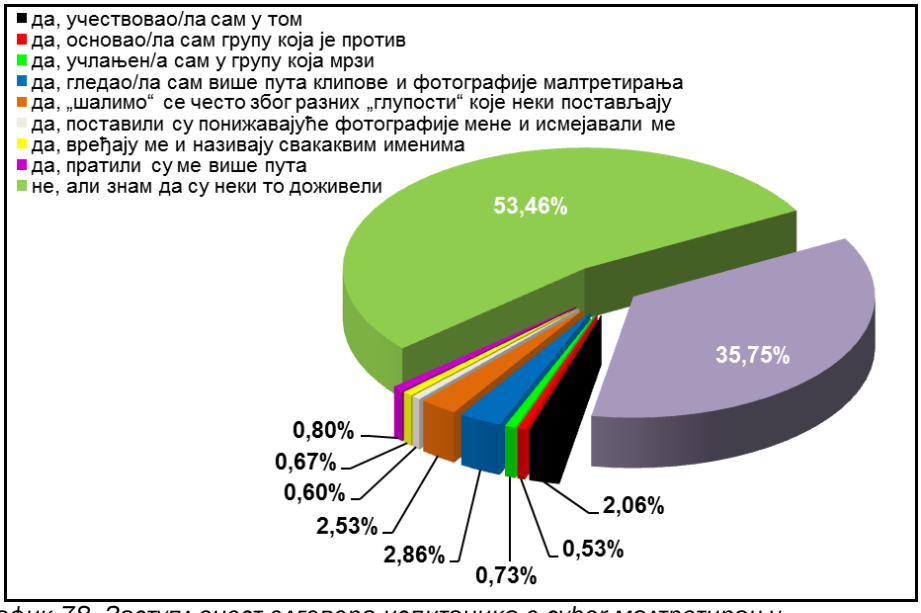


График 78. Заступљеност одговора испитаника о cyber малтретирању

679 Fairlie W.R., Kalil A. (2014), The Effects of Computers on Cyberbullying and Social Participation among Schoolchildren: Evidence from a Field Experiment, http://www.iza.org/conference_files/riskonomics 2014/fairlie_r1726.pdf, приступљено 13.5.2014;

680 Попадић Д. (2009), op. cit;

681 Srpski školarac na internetu-zabrinajvajuće brojke!, (2013), http://bezbedannet.wordpress.com/ 2013/05/22/srpski-skolarac-na-internetu-zabrinajvajuce-brojke/, приступљено 23.3.2014;

У истраживању из 2010. године[682] на питање да ли су били и у ком облику малтретирани у предходних 30 дана, 20,8% испитаника (старости између 10 и 18 година са југа САД-а) одговорило је потврдно: највише, 17%, једном или више пута; 14,3% повређујућим коментарима; 13,3% гласинама; а најмање, 5%, да су им постављене слике[683].

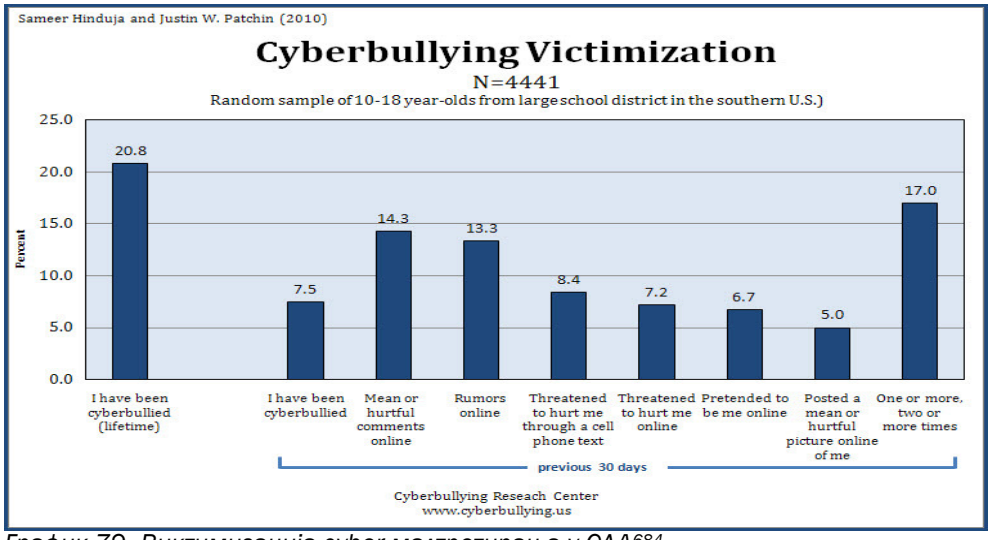


График 79. Виктимизација cyber малтретирања у САД[684]

Највећи проценат испитаника оба пола у Србији је одговорио да нису били жртве cyber малтретирања, али да знају неке који јесу: 26,8% испитанице и 25% испитаници. Интересантно је да никад нису чули за појаву cyber малтретирања „подједнако“ и мушки (18%) и женски (17,7%) испитаници. У 1,6% случајева испитаници су активно учествовали у овом облику малтретирања и пасивно 2% („шалили ...“). У поређењу са истраживањем у САД из 2010. године дистрибуција одговора, по полу, о облицима cyber малтретирања се разликује јер су се испитанице изјасниле у већем проценту од испитаника за већину понуђених облика (за 5 од 8).

682 Hinduja S. Patchin W.J. (2010), Cyberbullying, Identification, Prevention and Response, http://www.mbfxc.com/uploads/4/1/8/4/4184069/hinduja_and_patchin.pdf, приступљено 23.3.2014;

683 Study surveyed a random sample of 4441 youth between the ages of 10 and 18 from a large school district, Summary of our cyberbullying research from 2004-2010, (2010), http://www.cyberbullying.us/ research.php, приступљено 22.3.2014;

684 Hinduja S. Patchin W.J. (2010), op. cit;

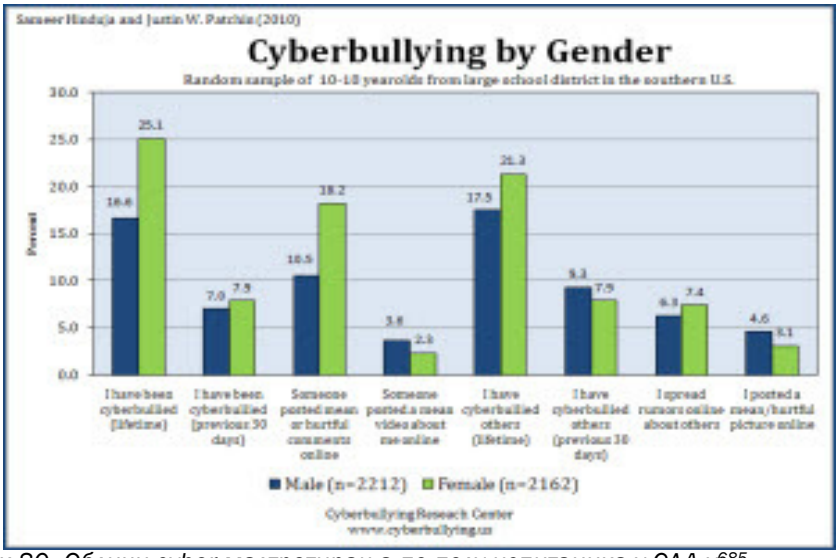


График 80. Облици cyber малтретирања по полу испитаника у САД-у[685]

Посматрано по старосним групама највећи проценат испитаника између 18 и 30 година одговорило је да нису били жртве, али знају неке који јесу (58,3%). Готово половина (49,1%) оних преко 45 година старости никад није чула за cyber малтретирање. За све остале одговоре ирелевантне су старосне групе.

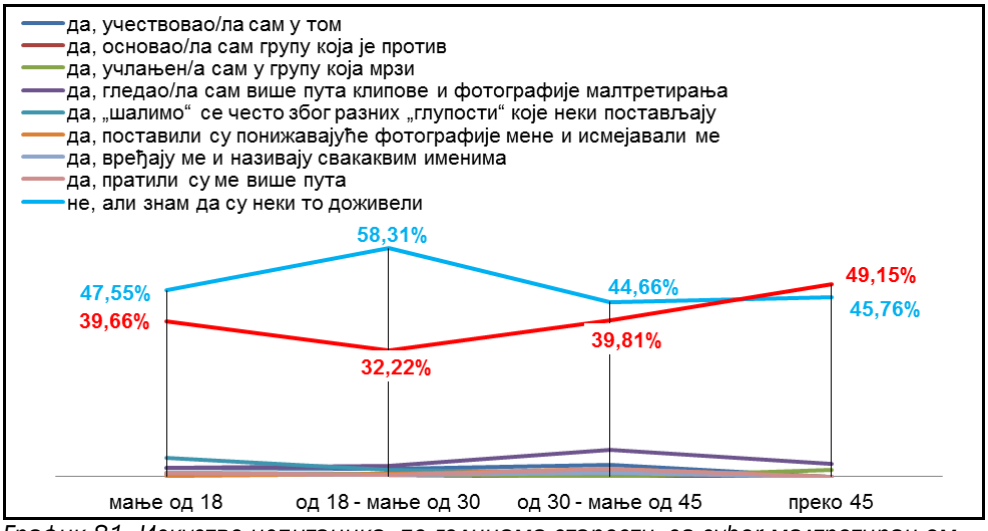


График 81. Искуство испитаника, по годинама старости, са cyber малтретирањем

Највише испитаника из свих места се определило за одговор да нису били жртве (50 и више %), али да знају неке који су то доживели. Изузетак су испитаници

685 Hinduja S., Patchin W.J., (2010), op. cit;

места до 5000 становника који су се за овај одговор определили у 43% случајева. Иста групација је у нешто мањем проценту (40%) одговорила и да није чула за cyber малтретирање. Сви остали испитаници су у мањем проценту изабрали овај одговор.

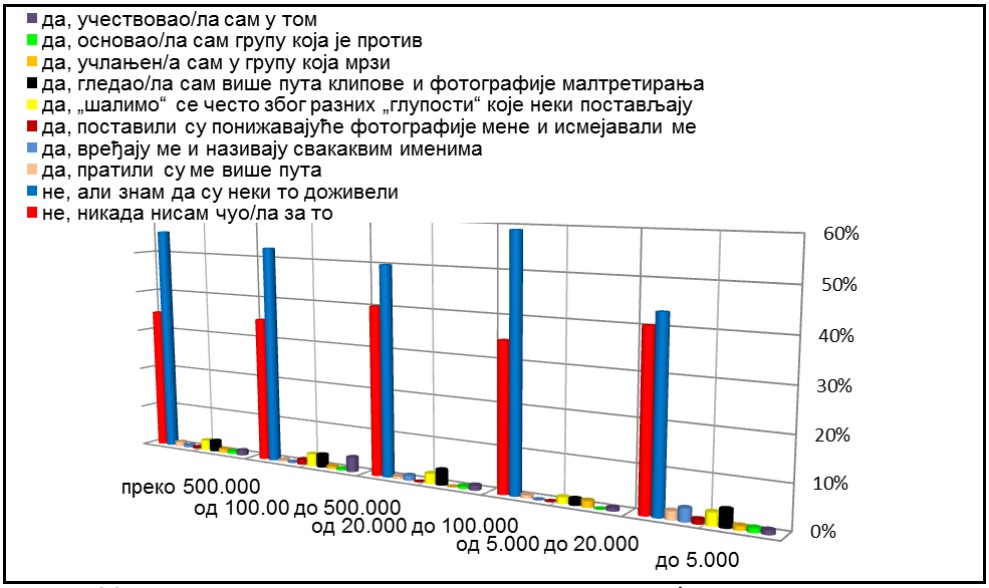


График 82. Искуство испитаника, по величини места пребивалишта, са cyber малтретирањем

Кад се заједно посматрају искуства испитаника по полу и годинама старости најизраженија су два одговора. Највећи проценат да нису доживели/е али знају ко јесте су жене између 18 и 30 година (62,8%). Непознавање интернет малтретирања је најизраженије код испитаница старости преко 40 година (52%). Интересантно је да су испитаници преко 45 година подједнако одговорили да знају да су неки други били жртве ове појаве иако никад за њу нису чули (47,1%).

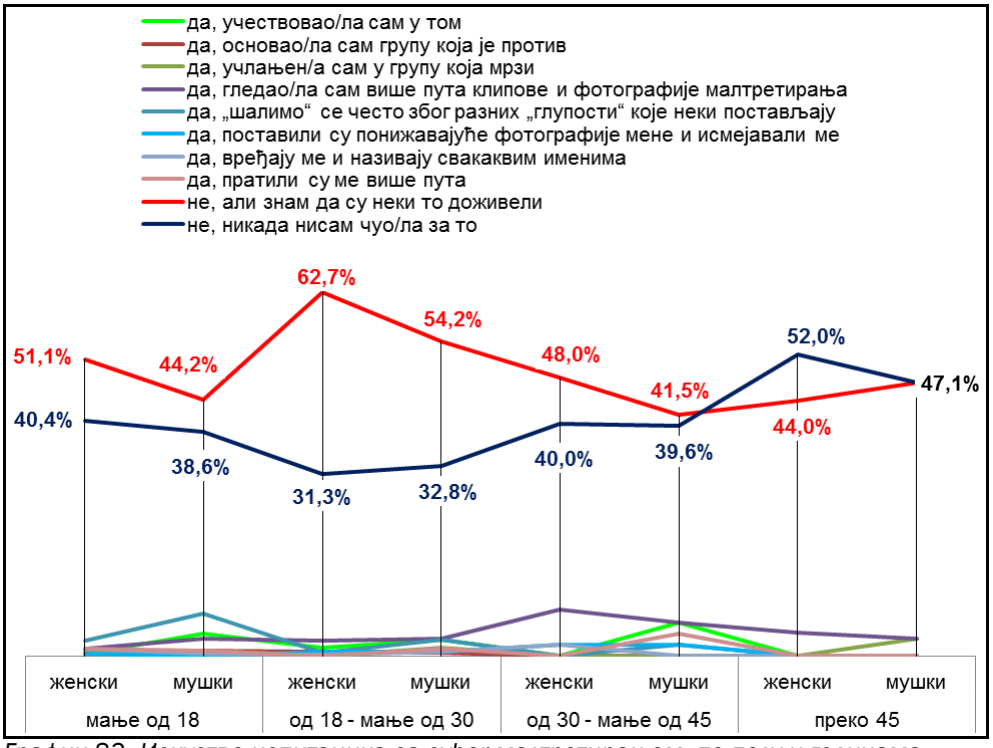


График 83. Искуство испитаника са cyber малтретирањем, по полу и годинама старости

Подаци добијени од испитаника различитих полова и величине места у којима имају пребивалиште, указују да је преко 50% испитаница одговорило да то нису никад доживеле, али да знају неког ко јесте у свим местима која су праћена по величини. Изузетак су места до 5000 становника где је проценат овог одговора био 44,2%. Најмањи проценат од свих испитаника који нису чули за електронско малтретирање су испитанице из места од 5000 до 20.000 становника (30,9%). Испитаници из било којих места су просечно необавештенији од испитаница.

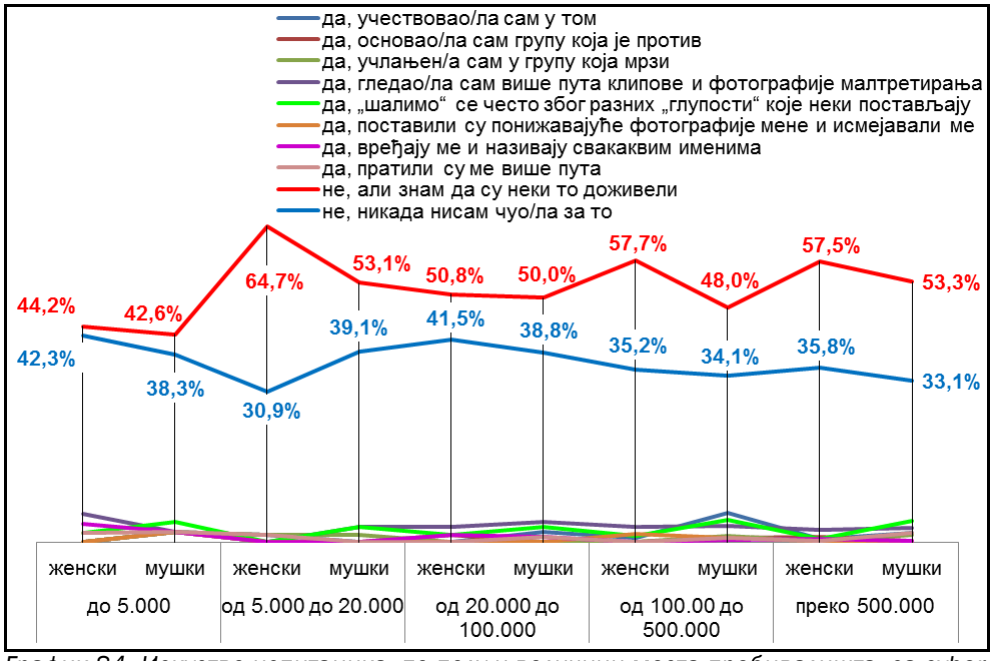


График 84. Искуство испитаника, по полу и величини места пребивалишта, са cyber малтретирањем

Анализа одговора испитаника по годинама старости и величини места пребивалишта показује да су оних који никад нису чули за ову појаву има 50% и становници су места са 500.000 становника, у старосној групи од 30 до 45 година (52,8%) и преко 45 година (63%). Најбоље су обавештени (25%) испитаници од 18 до 30 година у местима од 5000 до 20.000 становника.

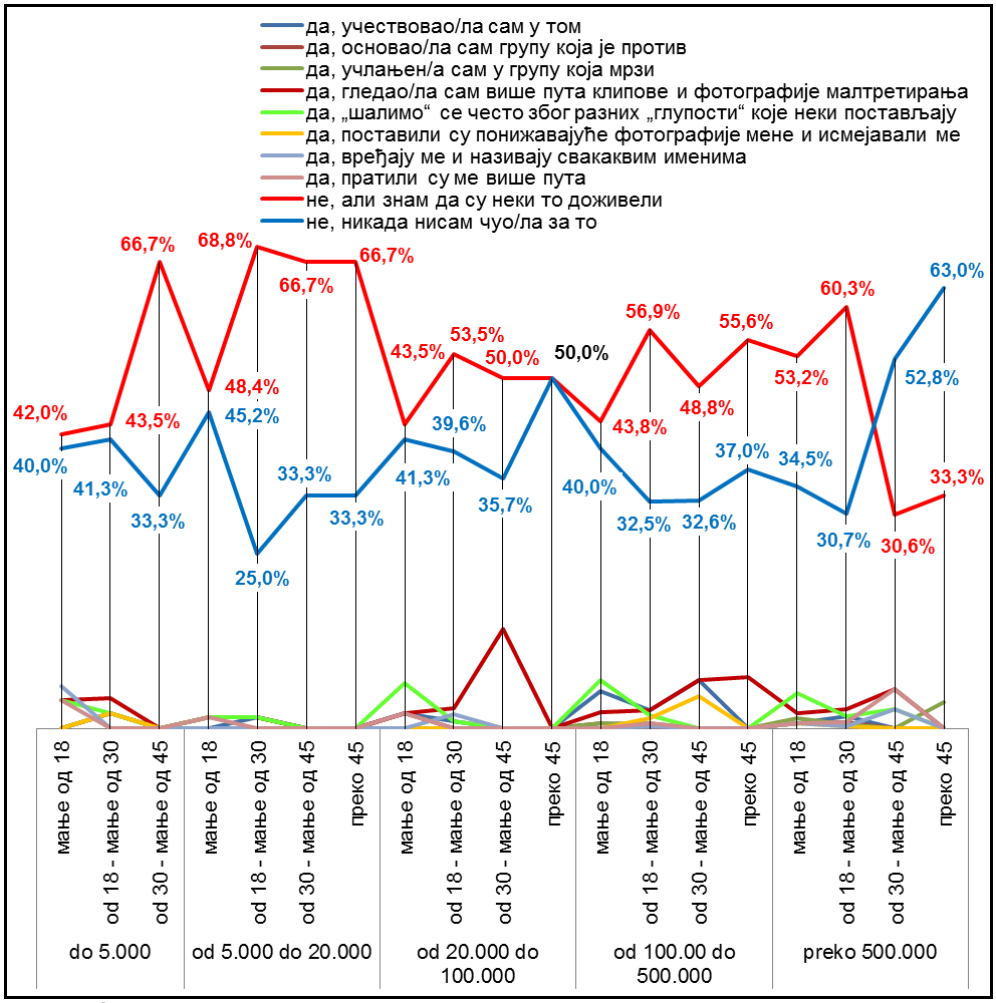


График 85. Искуство испитаника, по годинама старости и величини места пребивалишта, са cyber малтретирањем

Значи, о cyber малтретирању испитаници нису добро обавештени, али и нису често били његова жртва. Неки, ипак, познају неког ко је то био. У незнатном броју су учествовали у томе, основали су групу која је против насиља, гледали су више пута клипове и фотографија малтретирања, често су се „шалили“ због разних „глупости“ које је неко други поставио, постављали њихове понижавајуће фотографије и исмејавали их, вређали их и називали свакаквим именима или добијали претње више пута. Искуства која су стицали не зависе од величине места из којих су, али у неким случајевима зависе од пола и година старости.

3.3.4. Ставови о говору мржње/cyber мржња

Cyber мржња је само једна модификација или вид мржње, односно говора мржње, ***а он злочина мржње.*** Истовремено је и друга, тамна страна медаље - слободе говора. Појавом интернета слобода говора, као и многа друга права и слободе добијају ново значење и нове облике. Њих још више компликују друштвене мреже које изазивају све већу потребу за бројним ограничењима[686]. Због размера које добија cyber мржња постаје комплексан предмет регулације међународних организација какве су: УН[687], ОЕБС[688], ЕУ[689], Савет Европе[690] (који је формирао и специјализовано тело каква је Европска комисија против расизма и нетолеранције[691]). У оквиру аката Савета Европе дата је и дефиниција[692] овог облика мржње (извор: Додатни протокол уз Конвенцију о cyber криминалу)[693] као

686 Drakulić M. Drakulić R. (2010), Regulacija interneta, op. cit;

687 Human Rights Council, (2012), Twentieth session, Agenda item 3, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, https://geneva.usmission.gov/2012/07/05/internet-resolution/ (усвојена и гласом Србије која није чланица Савета за људска права); Human Rights Council (2009),Twelfth session, Agenda item 3, Promotion And Protection Of All Human Rights, Civil, Political, Economic, Social And Cultural Rights, Including The Right To Development, Resolution adopted by the Human Rights Council, 12/16; Freedom of opinion and expression, http://www.globalgovernancewatch.org/docLib/20091216_US-Egypt_Compromise-1.pdf.; United Nations, (1969), International Convention on the Elimination of All Forms of Racial Discrimination, General Assembly resolution 2106 (XX) of 21 December 1965, entry into force 4 January 1969, in accordance with Article 19, http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/218/69/IMG/NR021869.pdf?OpenElement, приступљено 22.1.2014;

688 Нпр. ова организација за европску безбедност и сарадњу је за борбу против говора мржње и трговине децом формирала по 3 посебне канцеларије и секретаријата и од 2004. године се укључује у борбу против ширења говора мржње, односно укључује се у акцију против cyber мржње. Основ за то је Декларација Савета Европе о слободи комуникација на интернету (*Declaration on freedom of communication on the Internet*), као и Препорука бр. 6 Европске комисије о борби против ширења расистичких, ксенофобичних и антисемитских материјала путем Интернета (*Recommendation No. 6 on Combating the Dissemination of Racist, Xenophobic and Antisemitic material via the Internet*), као и Одлука против анти семитизма ОЕБС-а (*Decision No. 607 Combating Anti-Semitism*); Drakulić M., Drakulić R., (2010), Regulacija interneta, op. cit;

689 Van Blarcum C.D. (2005), Internet Hate Speech: The European Framework and the Emerging American Haven, http://law.wlu.edu/deptimages/Law%20Review/62-2VanBlarcum.pdf, приступљено 5.4.2014;

690 McGonagle T., (2013), The Council of Europe against online hate speech: Conundrums and challenges, http://www.ivir.nl/publications/mcgonagle/Expert_paper_hate_speech.pdf; Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, (1950), amended by its Protocol No. 14 (CETS No. 194), (2010), http://conventions.coe.int/treaty/en/Treaties/Html/005.htm, приступљено 5.4.2014;

691 ECRI General Policy Recommendation No. 7 on national legislation to combat racism and racial discrimination, (2003), http://www.coe.int/t/dghl/monitoing/ecri/activities/gpr/en/recommendation_n7/ ecri03-8%20recommendation%20nr%207.pdf, приступљено 5.4.2014;

692 ELSA International Online Hate Speech Competition, (2012), Online Hate Speech: Hate or Crime?, Legal issues in the virtual world - Who is responsible for online hate speech and what legislation exists that can be applied to react, counter or punish forms of hate speech online?, www.elsa.org/.../Online_Hate_Speech_Essay_Competition_runner_up.pdf, приступљено 5.4.2014;

693 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, (2003), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, приступљено 5.4.2014;

он-лајн "било који писани материјал, слика или свако друго представљање идеја или теорија које заговарају, промовишу или подстичу мржњу, дискриминацију или насиље, против било којег појединца или групе појединаца, на основу расе, боје коже, или националног или етничког порекла, као и религије". Мада је највише цитирано одређење оно које је дато у *Recommendation No. R (97) 20 of the Committee of Ministers on "Hate Speech"*[694]. Циљ регулације, како истиче *Tarlach McGonagle*[695], је „да се спречи мешање са другим правима и да се спречи настајање штете. На првом месту, неопходно је разграничити говор мржње од других људских права или "оперативних" јавних вредности: достојанства, недискриминације и равноправнти, (ефективна) учешћа у јавном животу (укључујући и јавне дискурсе), слободе изражавања, удруживања, религије, итд. Други важан циљ је да се спрече одређене штете које може претрпети појединачна жртава: психолошке, самопоштовање, инхибираност самоиспуњења, страха и слично".

Међутим, све су бројније и значајни активности различитих специјализованих организација (npr. *INHOPE - The International Association of Internet Hotlines* или *INACH - The International Network Against CyberHate, Anti-Defamation League*[696]) којима је спречавање ове појаве у фокусу рада. Многе државе, нпр. САД[697] и Канада, објавиле су листе група које шире мржњу и cyber мржњу и чије се активности прате (нпр. *The Skinhead International: Canada*[698]).

У документу Борба млади против он-лајн говора мржње (*Young People Combating Hate Speech On-line*), истиче се да су границе говора мржње ван граница националних законодавстава, као и слободе изражавања, а да стратегије које доносе организације које се овим феноменом баве иду ка већим рестрикцијама везаним за садржаје, које треба да се „протегну" и на оф-лајн говор мржње[699].

694 Council of Europe, (1997), Committee of ministers, Recommendation no. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech", http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1997)020&expmem_EN.asp, приступљено 5.4.2014;

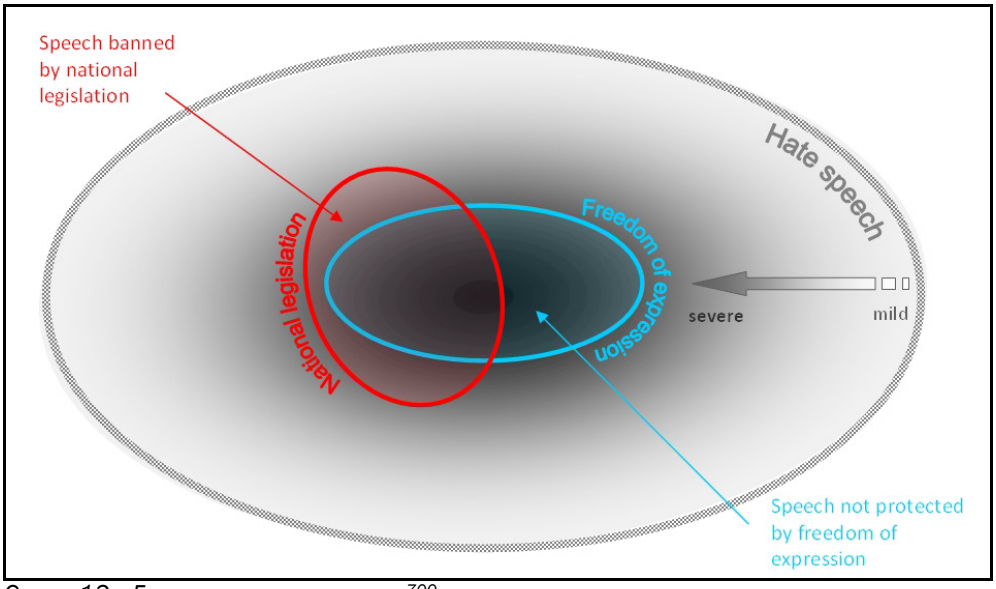
695 McGonagle T. (2013), op. cit;

696 Anti-Defamation League, (2011), Extremism in Florida: The Dark Side of the Sunshine State, http://www.adl.org/assets/pdf/combating-hate/ExtremismFloridaINSIDE.pdf, приступљено 5.4.2014;

697 United States Action Yahoo Group, (2000), List of Active US Hate Groups as of 2000, (Alphabetical List of Groups by USA State), (research from Southern Law Poverty Center Intelligence Report), http://www.unitedstatesaction.com/list-us-hate-groups.htm, приступљено 5.4.2014;

698 The Nizkor Project, (2012), The Skinhead International: Canada, http://www.nizkor.org/hweb/orgs/american/adl/skinhead-international/skins-canada.html, приступљено 5.4.2014;

699 British Institute of Human Rights for Council of Europe, (2012), Young People Combating Hate Speech On-line, Mapping study on projects against hate speech online, www.coe.int/.../2012_Mapping_projects_against_Hate_Speech.pdf, приступљено 5.4.2014;



Слика 13. Границе говора мржње[700]

У истом документу истичу се и форме и методе реализације cyber мржње и наводе да су то[701]:

- **сајтови мржње** које је, нпр. 2009. године, посетило 12% младих од 11 до16 година из Европе, а тај број расте на 20% оних између 15 и 16 година;
- **блогови и он-лајн форуми** на којима се све више појављују и *CMC*- поруке са великом дозом мржње (у Украјини је само „изникло“ неколико таквих сајтова од почетка протеста 2014. године, нпр. http://www.politicalforum.com/showthread.php?t=350562&page=4);
- **електронска пошта и личне поруке** – број порука, број прималаца и пошиљалаца расте јер је ово и најтежи медиј за контролу;
- **игрице** – оптрећене насиљем и порукама мржње усмерене на децу на које и највише утичу (нпр. *Manhunt* или *Grand Theft: Auto,* http://www.rockstargames.com/grandtheftauto/)[702];
- **сајтови друштвених мрежа**[703] (*Facebook, Youtube+*[704]);

700 British Institute of Human Rights for Council of Europe, (2012), op. cit;

701 British Institute of Human Rights for Council of Europe, (2012), op. cit;

702 Drakulić M. Drakulić R. (2010), Regulacija interneta, op. cit;

703 Jaishankar K. (2008), Cyber Hate: Antisocial networking in the Internet, International Journal of Cyber Criminology, Vol 2 (2): 16–20, http://www.cybercrimejournal.com/editorialijccjuly2008.pdf; Solomon J., (2010), Hate speech infiltrates social-networking sites, report says, http://edition.cnn.com/2010/TECH/03/15/hate.speech.social.networks/, приступљено 5.4.2014;

704 Simon Wiesenthal Center, (2009), Facebook, Youtube+: How Social Media Outlets Impact Digital Terrorism and Hate, http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=lsKWLbPJLnF&b=4441467&ct=7131713, приступљено 5.4.2014;

- **видео и музика**, нпр. на сајту http://www.last.fm/tag/skinhead могу се наћи листе, видео снимци и музика разних британских група skinheads-a (Music tagged "white power", Music tagged "skinhead reggae" и слично).

Наравно да ови облици нису само карактеристични за младе, али су они највише угрожени њиховим коришћењем и најрањивији њиховим порукама.

Истраживање и праћење[705] злочина мржње (са говором мржње) које је спроведено у Великој Британији 2009/2010. и 2010/2011. године од стране *British Crime Survey* (*BCS*) показало је да[706]:

- 0,5% одраслих је било жртва злочина мржње 12 месеци пре интервјуа, у поређењу са 22% одраслих који су најмање једном били жртве других облика криминала;
- мотивација извршилаца најчешће је везана за расу жртве (у односу на око просечних 136.000 инцидената годишње);
- злочин мржње више су доживеле породице него појединци (37% жртава су биле породице и то више од једном, 19% су појединци) што је више него када су у питању други облици криминала (29% породице, 21% појединци).

Истраживање cyber мржње у Бугарској 2012. године, које је обавила Европска фондација за младе (*European Youth Foundation*), обухватило је 315 студената/ученика и младих људи од којих 150 девојака и 165 младића узраста 15 - 19 година указује да[707];

- жртве сајбер мржње доживљавају далекосежне негативне последице - неки од њих су одговорили да „мрзе са мржњом", док су се други повукли у себе и преживљавају сами; 80% испитаника нису били жртве сајбер мржње, 15% је одговорио са јесте и 5% да је лично нису „искусили", али имају пријатеље који јесу; већина испитаника је одговорила да не зна шта би требало да уради уколико постану жртве, а врло мало њих зна где да траже остваривање својих права и како да их бране;
- пронађено је више од 500 случајева он-лине мржње и дискриминације у *Web* 2.0 окружењу и настављају да расту текстуални и видео садржаји на друштвеним мрежама;
- многи су лично коментарисали на форумима и друштвеним мрежама да оне подстичу мржњу према политичким странкама и њиховим лидерима, јавним личностима, људима са другачијом сексуалном оријентацијом, као и етничку нетрпељивост према Ромима и Турцима.

---

705 Многи национални органи прате стање са злочином и говором мржње. Тако је ФБИ 2012. објавио Узвештај о злочину мржње (Uniform Crime Reporting Program, Hate Crime Statistics, 2012, http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2012/topic-pages/victims/victims_final.pdf, приступљено 5.4.2014;

706 Smith K. Lader D. Hoare J. Lau I., (2012), Hate crime, cyber security and the experience of crime among children: Findings from the 2010/11 British Crime Survey, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116463/hosb0612.pdf, приступљено 5.4.2014;

707 Report – analysis "levels of cyber hate in Bulgaria, (2012), nohate.ext.coe.int/.../2012%20-%20REPORT%20-%20ANALYSIS%20„LEVELS%20OF%20CYBER%20HATE%..., приступљено 5.4.2014;

- У извештају *INACH-а,* на пример, у мају 2014. године констатовано је[708]:
- на *Twitter* платформи расте антисемитизам као мржња на друштвеним медијима;
- исламофобија цвета на интернету (САД);
- због своје боље рачунарске писмености млади лакше прихватају информације (Холандија) па и такве са говором мржње;
- годишњи извештај о антисемитизму у Чешкој указује на нагли пораст напада са интернета;
- *Wikipedia edit*-у са владиних рачунара стижу увреде муслимана (В.Британија);
- да је *Ben Garrison* објавио нови цртеж *Ben Garrison on Facebook Trolls* (*Online Hate Prevention Institute's Cartoonist in Residence*)[709];
- шведски адвокати прате и наплаћују нето тролове, а шведска полиција трага за cyber неонацистичким бегунацима.

У Србији cyber мржња је не само изузетно присутна већ је у комбинацији или као последица традиционалних облика говора мржње и „резултат" кризе, транзиције, тешких 90-их, ратова, утицаја пропагандне машинерије која је своје постојање оправдавала преко свих медија (како истиче *Mike Harris*[710]*: „Током европске историје, говор мржње је веома проблематичан, из искуства и последица холокауста кроз директно* ***подстицање етничког насиља преко државних медија током ратова у бившој Југославији****. Међутим, неопходно је истаћи да су закони за регулацију говора мржње у складу са циљем заштите слободе изражавања"*)[711], већ и урушавања вредносног система и непостојања правних и етичких норми којим би се ова појава боље ограничила и разграничила. Под изговором права на слободу изражавања и слободних медија cyber мржња се несметано шири и, као свуда у свету, највише угрожава децу и младе. Но, ни посебне групе (*LGBT*, националне мањине, Роми, хендикепирани и слично) нису поштеђени[712].

Веб-сајтови, *YouTube, Facebook,* али и многи други, у Србији су често права „ризница" брутално cyber мржње:

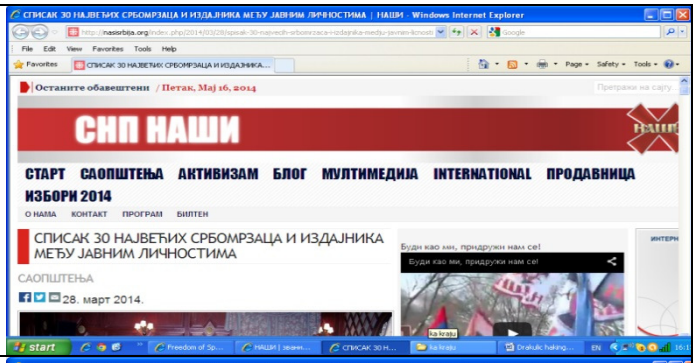
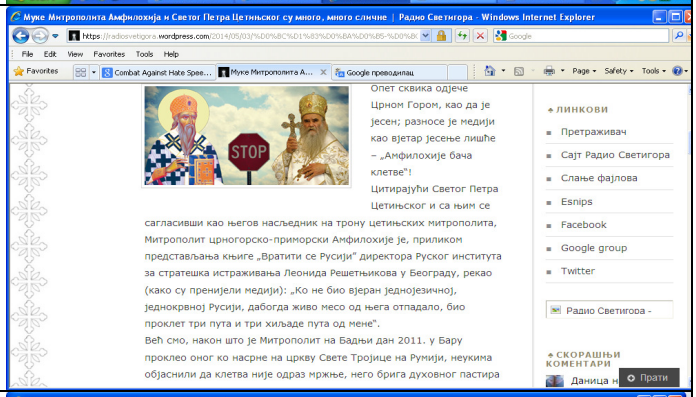
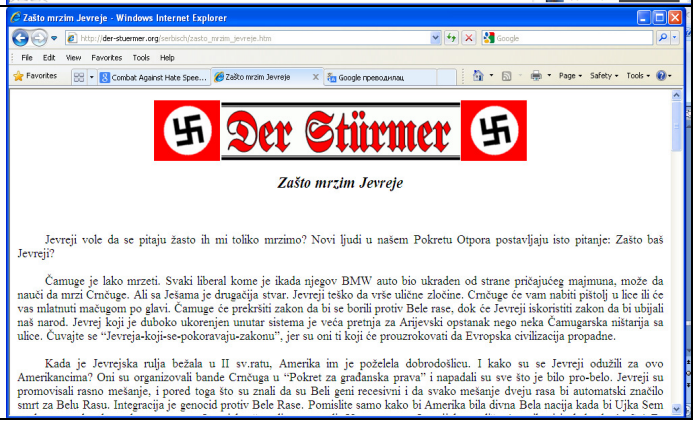
708 INACH, (2014), Headlines May 2014, http://www.inach.net/news.php, приступљено 10.5.2014;

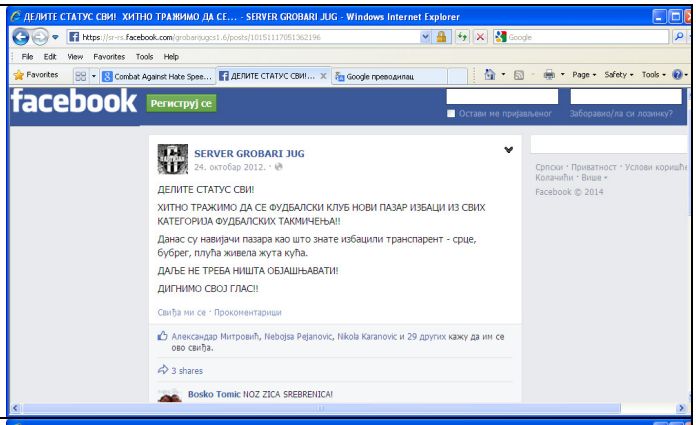
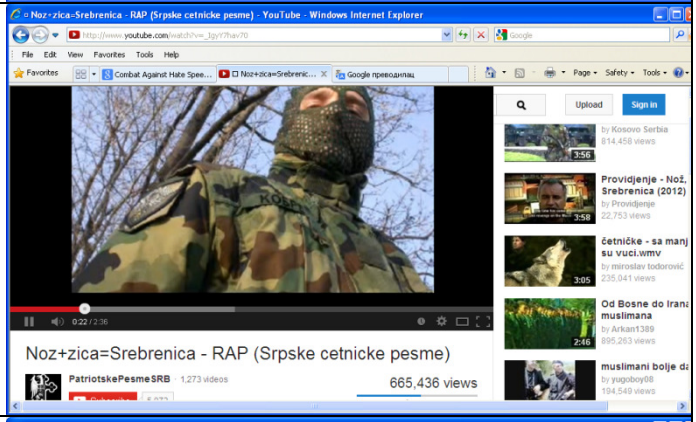
709 *Ben Garrison* је познати цртач који се укључио у акције против говора мржње својим цртежима које објављује преко аустралијског Института, http://ohpi.org.au/ben-garrison-on-trolls/ или на свом сајту, http://grrrgraphics.com/, приступљено 5.4.2014;

710 Harris M. (2014), Europe's rules on freedom of information and hate speech, http://www.indexoncensorship.org/2014/01/eus-commitment-freedom-expression-freedom-information-hate-speech/, приступљено 5.4.2014;

711 Harris M. (2014), op. cit;

712 Бројне примере прикупио је *Media centar*, http://www.mc.rs/govor-mrznje-na-internetu.3542.html, приступљено 5.4.2014;

Српски народни покрет „НАШИ“ - http://nasisrbija.org/	
Радио Митрополије Црногорско-приморске - https://radiosvetigora.wordpress.com/2014/05/03/	
Немачки Лист ***"Der Stürmer"*** који има и српску верзију - http://der-stuermer.org/serbisch/zasto_mrzim_jevreje.htm	

Навијачка група Гробари Југ - https://www.facebook.com/grobarijugcs1.6/posts/10151117051362196?stream_ref=5	
Noz+zica=Srebrenica - RAP (Srpske cetnicke pesme) – YouTube - http://www.youtube.com/watch?v=_IgyY7hav70	
Навијачка група Гробари југ - http://www.youtube.com/watch?v=ppVaTsGDYME	

YouTube је преплављен песмама разних музичких група које шире мржњу (https://www.youtube.com/watch?v=JP3y0XDXkOA) и подстичу коментаре, политичких/ослободилачких група (https://www.youtube.com/watch?v=Vk_1L1LDhJw), навијача

(https://www.youtube.com/watch?v=uVo_JWTuhn0) или постављених знакова/логоа (Anti-antifa Srbija, Ultra Boys и сл.).

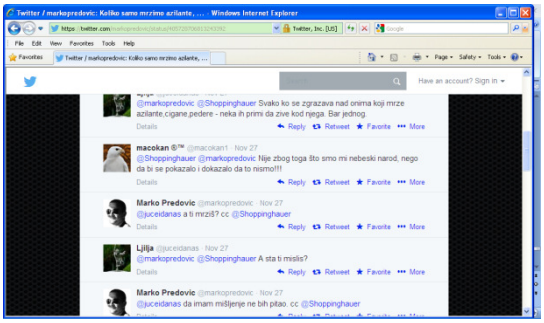
Покретани су разни форуми који имају за циљ „ширење истине“ о неком догађају, појединцу, ситуацији, нацији, групи и слично. На пример: http://forum.novipazar.org/uloga-srpskih-orijentalista-u-opravdavanju-genocida-protiv-muslimana-historija/drustvo-board11/t3486-boa rd12/.

Пред *LGBT* Параду поноса у Београду 2010. године, настала је игрица „Gej protiv navijača”, http://www.extracafe.rs/stuff/akcije_arkade/gej_protiv_navijaca/1-1-0-5859 или http://tracara.com/gej-protiv-navijaca/ коју су често играла и деца.

Настали су и блогови на којима се размењују „искуства и знања“, на неке од њих постављају се текстови као мотиватори и подстрекивачи (http://antiafa-serbia.blogspot.com/). Пример је: http://www.intermagazin.rs/ako-ne-znate-kako-izgleda-najstrasnija-mrznja-prema-srbima-evo-prilike-da-vidite-i-da-procitate/, на коме је постављена „прича“ о одређеној особи и његовој „творевини“ (*Srpska duhovnost*).

Наравно да се друштвене мреже обилно користе за слање порука мржње и cyber мржње (нпр. http://www.alo.rs/vesti/hronika/pocuca-i-ivanovic-uhapseni-zbog-sirenja-mrznje/51497):

„Radomir Počuča saslušan zbog pretnji „Ženama u crnom“
Kako se precizira u saopštenju Tužilaštva, Počuča je priveden zbog sumnje da je izvršio krivično delo ugrožavanja sigurnosti putem svog Fejsbuk profila „Radomir Bata Počuča“, pozivanjem navijača da se obračunaju sa Udruženjem građana „Žene u crnom“.
On je preko svog Fejsbuk profila 25. marta pozvao navijače Crvene zvezde, Partizana, Rada i Vojvodine da „ne troše pesnice između sebe“, već da se udruže i da pretuku „Žene u crnom“, koje su na Trgu Republike u Beogradu obeležile 15 godina od zločina nad albanskim civilima na Kosovu. On je na svom Fejsbuk profilu u nedelju uveče napisao da je pozvan telefonom da sledećeg dana u 8.30 da izjavu istražnom sudiji u Palati „Srbija“.



Једна од група против које је усмерен говор мржње и cyber мржње су мигранти/азиланти. До 2011. године је наводно био добар однос локалног становништва и азиланата смештених у одговарајуће центре[713]. У 2013. и 2014. години у више наврата су организовани протести локалног становништва против азиланата[714]. Све је више новинских чланака усмерених против њих, а ни ситуација на интернету није боља. Појављују се и слични сајтови, блогови, форуми[715].

Све се чешће предузимају правне и остале мере у смањивању утицаја ове појаве. Настају систематске и организоване, једнократне и дугорочне активности, кампање, каква је нпр. YUCOM-a (http://www.yucom.org.rs/rest.php?tip=vestgalerija&idSek=24&idSubSek=-70&id=1&status=drugi), акција Министарства омладине и спорта „Реци НЕ говору мржње на интернету", формиран је сајт „У праву си" (http://upravusi.rs/komunikacije/internet-komunikacije/ponasanje-na-internetu/). Формиран је и Национални комитет за борбу против говора мржње. Али је то, ипак, још увек недовољно и прилично млако и меко (*soft механизми*).

Највећи проблем је и даље изузетно ниска свест о опасностима и размерама cyber мржње, као и о дугорочним невидљивим последицама.

У истраживању које је спроведено у мају 2013. године, испитаницима је постављено једно директно и неколико индиректних питање везаних за говор мржње. Директно питање се односило на реакције које би имали у случају да се са њим сретну. Понуђено је 6 одговора (пријавити администратору, пријавити неком старијем кога познају, пријавити полицији, заборавити на то јер их не занима шта други раде, насмејати се и лајковати ако се слажу са тим и оставити похвални коментар).

Више од половине испитаника (60,6%) би на ову појаву заборавило јер их не занима. Тако су се определили на пасивност, највероватније због потребе да се не замерају, да избегну негативне реакције носилаца оваквог говора или порука, страха од проверавања старијих, администратора, полиције јер су били у контакту са тим садржајима или због велике вероватноће да би се сусрели са честим ставом окружења да „жртва није невина"[716]. Ипак се 19,2% определило да то пријави

713 ECRI Secretariat Directorate General of Human Rights and Legal Affairs Council of Europe, (2011), Извештај ЕКРИ о Србији, http://www.coe.int/t/dghl/monitoring/ecri/country-by-country/serbia/SRB-CbC-IV-2011-021-SRB.pdf, приступљено 5.4.2014,

714 Mladenovac: Protest protiv centra za azilante, (2013), http://balkans.aljazeera.net/vijesti/mladenovac-protest-protiv-centra-za-azilante;

715 https://twitter.com/markopredovic/status/405728706813243392, приступљено 5.4.2014;

716 Findley K.A. (2008), Toward A New Paradigm Of Criminal Justice: How The Innocence Movement Merges Crime Control And Due Process, https://media.law.wisc.edu/m/dfknm/findley_new_paradigm-10-10-08.pdf; Meyer C., (2010), Why Does the Passive Aggressive Play the Victim Role?, http://divorcesupport.about.com/od/abusiverelationships/a/PassiveAggressive_Victim.htm; Wolfe L.

администратору. Забрињава став, иако малог броја испитаника, да би оставили похвални коментар (2,2%). Међутми, беневолентни став има и 7,1% испитаника који би се насмејали и лајковали да се слажу. Исто тако је мали, али и охрабрујући, број испитаника који би то пријавио полицији (3,9%).

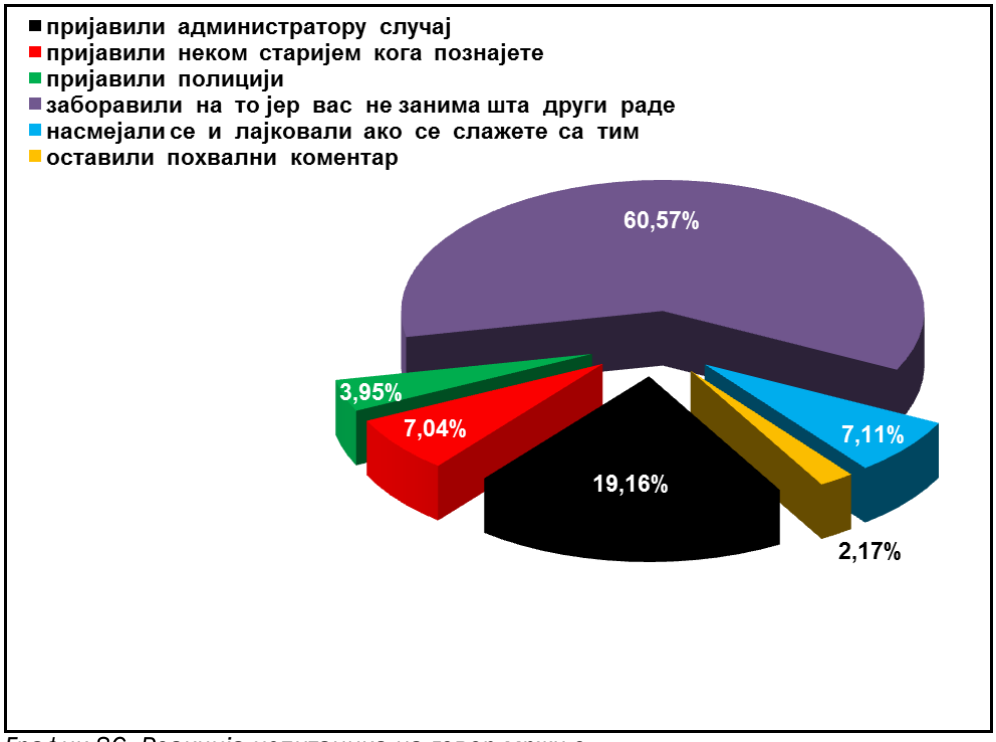


График 86. Реакција испитаника на говор мржње

Највећи проценат испитаника оба пола би заборавио на говор мржње на који су наишли јер их не занима шта други раде[717]: жене 62,8%, а мушкарци 58,3%. Очигледно је да су испитанице много више склоне „забораву“ и комформизму од испитаника. То се може објаснити и страхом од реакције окружења и лошим искуствима са проблемима са којима су се сретали након реаговања и укључивања трећих лица. Као и мушкарци, њихова следећа најзаступљенија активност је пријављивање администратору (18,5%:19,7%), што показује и дозу спремности на реаговање, али и избор најблаже и најједноставније опције. Најмање су се обе групе испитаника определиле да би оставили похвални коментар[718] (жене 1,1%,

(2012), Eight reasons why victim-blaming needs to stop: Writers, activists, and survivors speak out, http://www.womenundersiegeproject.org/blog/entry/eight-reasons-why-victim-blaming-needs-to-stop-writers-activists-and-surviv, приступљено 5.4.2014;

717 Radwan F. (2010), I wish i was attractive, http://www.2knowmyself.com/I_wish_i_was_attractive, приступљено 5.4.2014;

718 Vanstone A. (2014), Should hate speech be allowed?, http://www.abc.net.au/radionational/programs/ counterpoint/should-hate-speech-be-allowed3f/4816546, приступљено 5.4.2014;

мушкарци 3,3%), али и тај мали број забрињава јер је могуће да припадају категорији људи који воле да плаше[719] или да поруке мржње не доживљавају као стварне и третирају их као и „крими приче“[720] или да сматрају да су тако „важнији“.

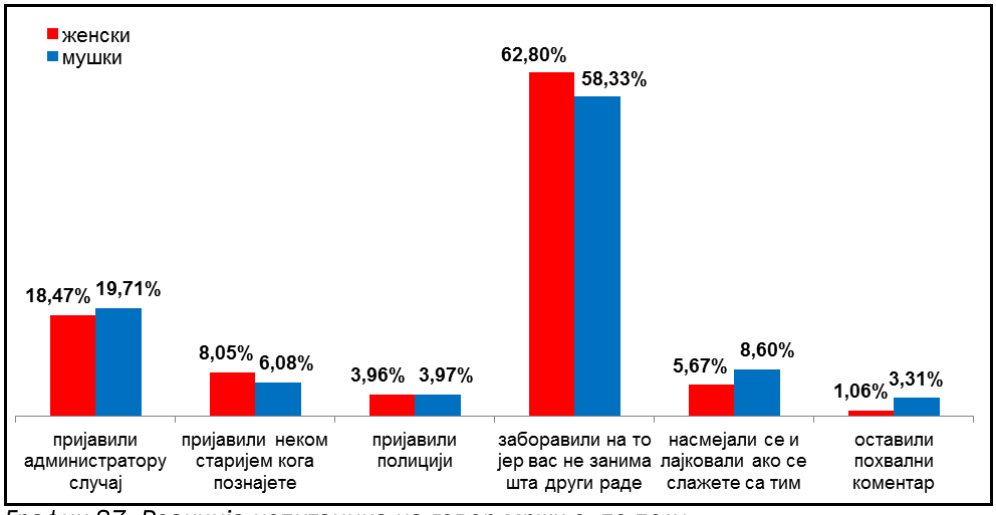


График 87. Реакција испитаника на говор мржње, по полу

Посматрано по годинама старости испитаника највећи проценат свих старосних група се определио за заборав и пасивност. То је најкарактеристичније за групу старију од 45 година (69,8%), а најмање за оне који су млађи од 18 година (54%). Најмлађи највише од свих група би говор мржње пријавили старијима (17,1%), што је потпуно нормална и очекивана реакција. У много мањем проценту би пријавили полицији (4,9%), што би урадили и они преко 45 година (4,8%). Старији од 45 година не би уопште остављали позитивне коментаре, док су најмлађи управо одговорили супротно, али су се они од свих група највише смејали и „лајковали“ такве садржаје. Највише би пријавили администратору испитаници између 30 и 45 година (27,6%). Интересантно је да су све старосне групе резервисане у пријављивању полицији.

719 Damjanović A. Damjanović A. Pantović M. Barišić J. (2011), Zašto volimo da se plašimo? – Psihofiziologija horor filma, http://www.psihijatrijakcs.org/klinika_psihijatrija/pdf_engrami/zasto-volimo-da-se-plasimo-psihofiziologija-horor-filma.pdf, приступљено 5.4.2014;

720 Montaldo C. (2011), Why Do Women Like True Crime Books? Why Are Women Drawn to the Gruesome Details?, http://crime.about.com/od/women/a/women_books.htm; Tyler T., (2001), Is the Internet Changing Social Life? More Things Change, The more Stay The Same, www.researchgate.net/...Social.../e0b49521e1b3a6787a.pdf, приступљено 5.4.2014;

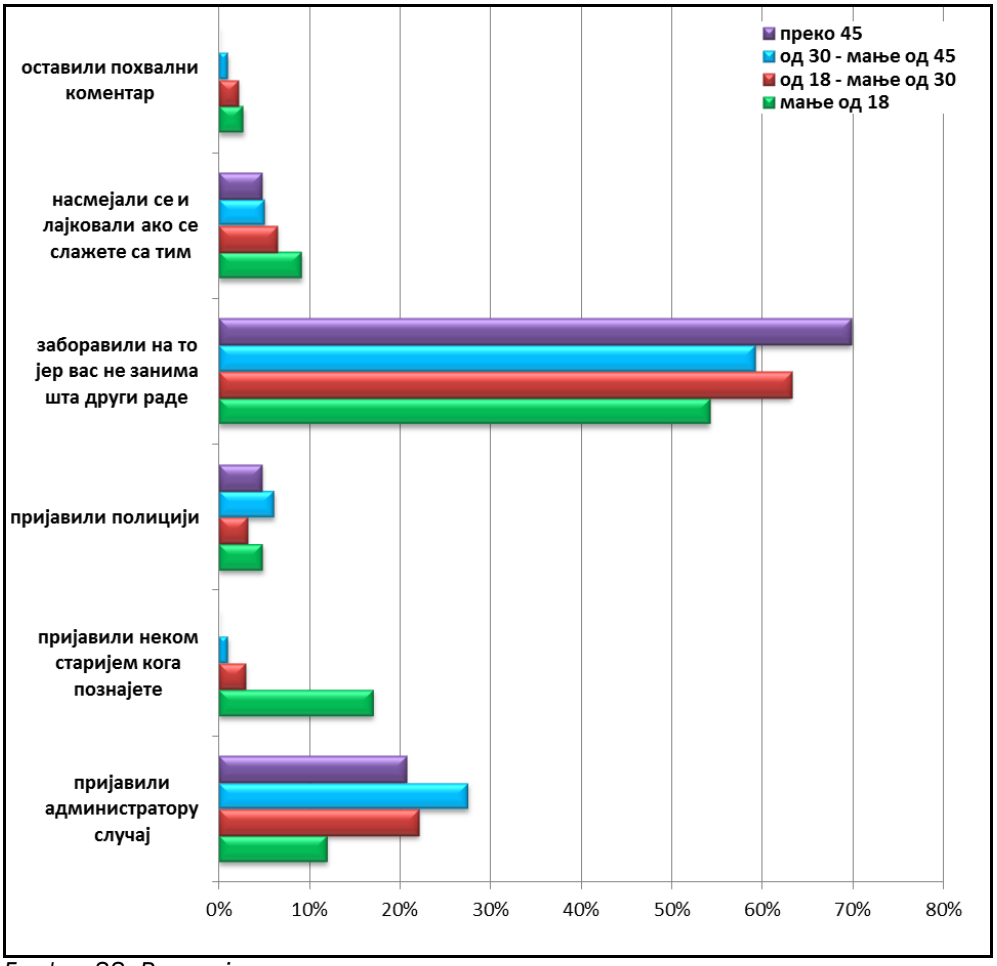


График 88. Реакција испитаника на говор мржње, по годинама старости

Анализа одговора испитаника по величини места у којима живе показује да би испитаници процентуално из свих места најмање оставили похвални коментар, с тим што се у овој малој групи „истичу“ они из места до 5000 становника (3,6%). Забораву би прибегли највише становници места између 20.000 и 100.000 становника (66,9%), а најмање између 5000 и 20.000 (58,1%). Испитаници из градова већих од 500.000 становника, после пасивности и заборава, највише су се определили за пријаву администратору (21,5%). Пријавили би полицији највише испитаници из места до 5000 (6,4%), вероватно јер се познају са полицајцима[721], а најмање између 100.000 и 500.000 становника (2,7%).

721 Weisheit R.A. Wells L.E. Falcone D.N. (1995), Crime and Policing in Rural and Small-Town America: An Overview of the Issues, https://www.ncjrs.gov/txtfiles/crimepol.txt, приступљено 5.4.2014;

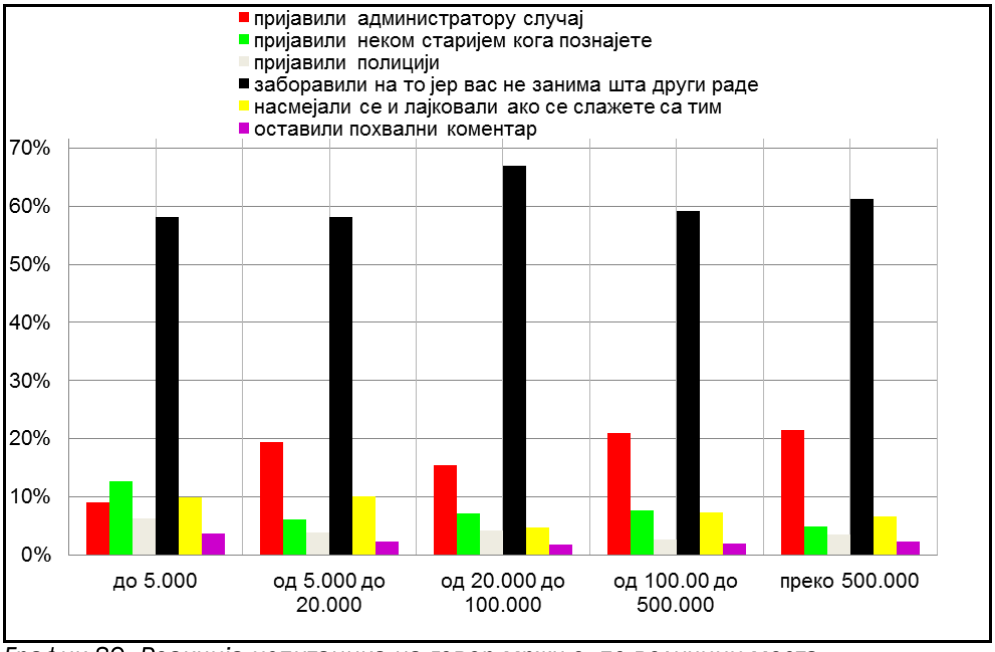


График 89. Реакција испитаника на говор мржње, по величини места пребивалишта

Посматрајући заједно по полу и годинама старости највише мушкараца преко 45 година је одговорило да би заборавило јер их не занима шта други раде. Испитаници преко 45 година оба пола не би оставили похвалне коментаре за поруке које носе cyber мржњу. Припаднице „лепшег“ пола између 30 и 45 година, такође, нису бирале овај понуђени одговор. Без обзира што је најмање изабрани одговор,мушки део испитаника се у незанемарљивом проценту за њега определио: до 18 година (3,8%) и између 18 и 30 (3,4%). Не треба занемарити да овим групацијама припадају и навијачи познати по свом екстремном понашању (Taurunum boys 1987, Фирма, Гробари југ, Делије север)[722], као и подмладак осталих нетолерантних и „национално свесних“ група.

722 Navijacke grupe Srbije, http://navijaci.wordpress.com/, приступљено 5.4.2014;

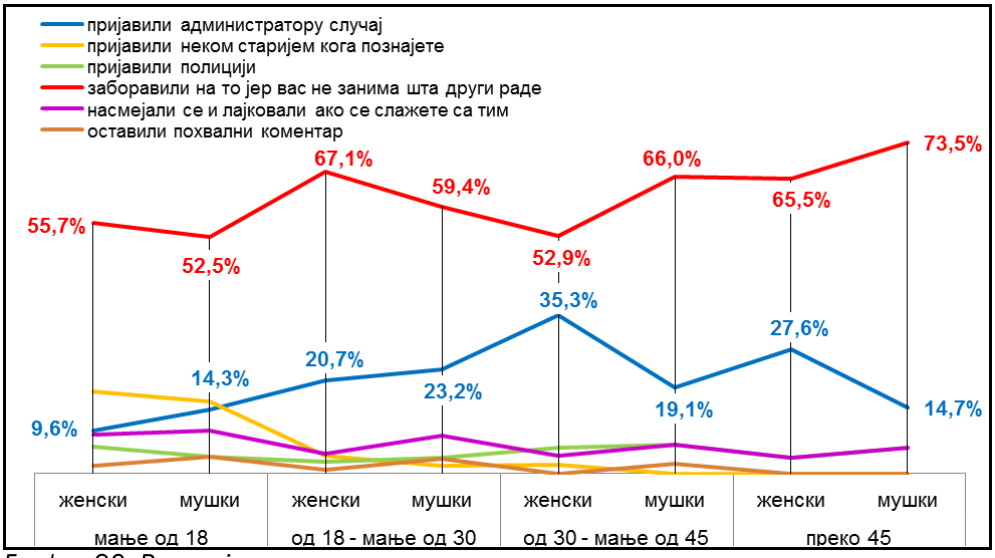


График 90. Реакција испитаника на говор мржње, по полу и годинама старости

Анализа одговора које су дали испитаници различитих полова и из места различите величине, указује да су се жене, из места величине између 20.000 и 100.000 становника (71,4%), највише определиле за одговор да би заборавиле јер их то не занима. Можда би ситуација била другачија да су оне имале податке да су жене мета, циљ, говора мржње. Ово је доминантан одговор и за мушкарце из таквих места. Преко 11,5% мушкараца из места до 20.000 становника лајкују говор мржње, а жене из ових места су мање екстремне (око 8,7%).

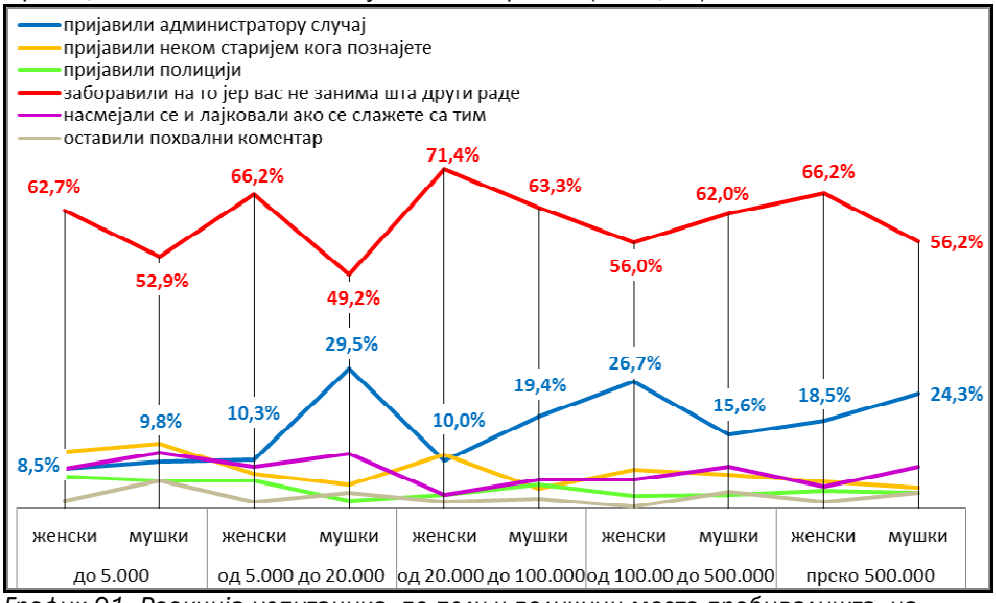


График 91. Реакција испитаника, по полу и величини места пребивалишта, на говор мржње

Упоређивањем одговора које су дале групе испитаника различите старости који потичу из места различите величине, види се да поред уобичајеног највећег броја одговора везаних за заборав и незаинтересованост или најмањег броја остављања похвалних коментара, определили за опцију пријављивања говора мржње администратору и то највише из места између 5000 и 20.000 становника старости између 30 и 45 година (50%). Три четвртине испитаника старих преко 45 година, из градова већих од 500.000 становника, највише су склони забораву. Млађи од 18 година, поред заборава, највише су се усмерили на пријаву старијима ако су из места између 100.000 и 500.000 становника (22%), односно из места између 20.000 и 100.000 становника (18%).

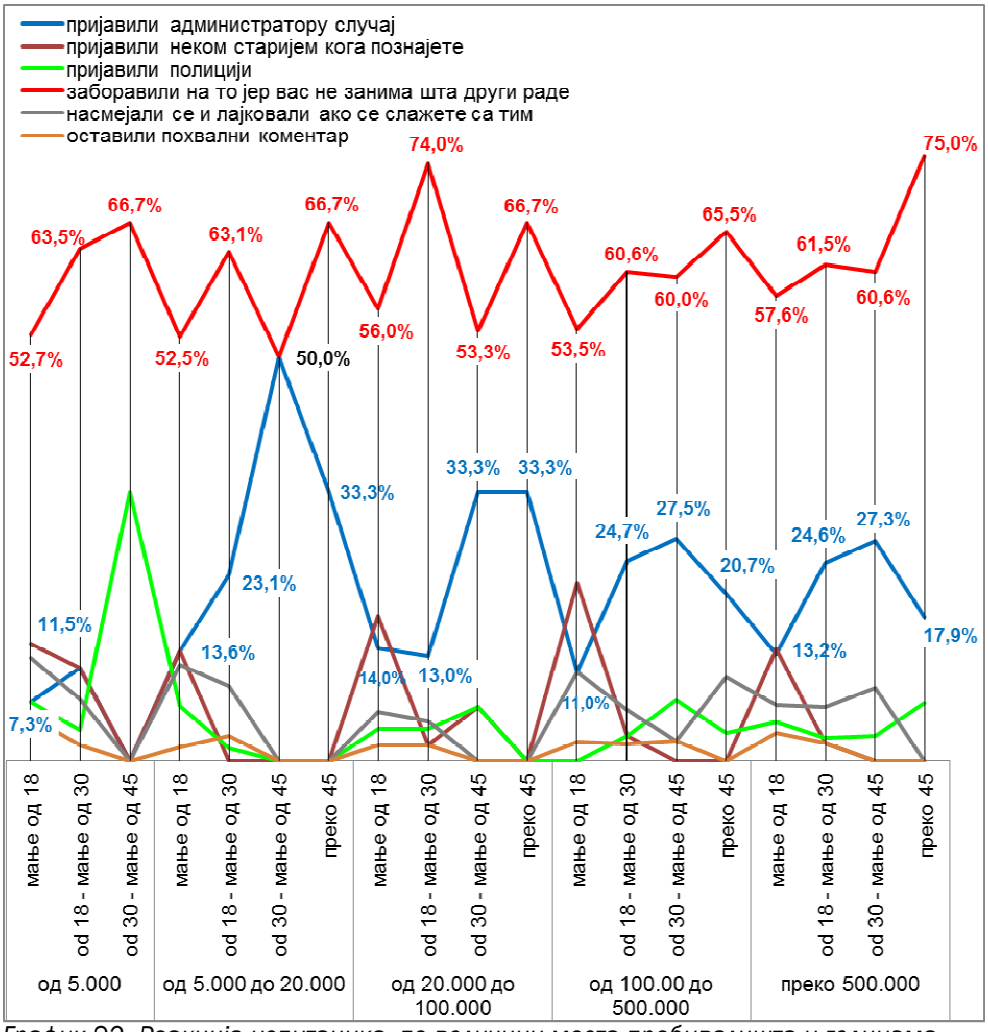


График 92. Реакција испитаника, по величини места пребивалишта и годинама старости, на говор мржње

Значи, кад је у питању cyber мржња испитаници из Србије:

- све групе (по полу, старости, местима пребивалишта) би у највећем броју заборавиле, јер их то не занима;
- све групе би изузетно у малом броју пријавиле полицији;
- млади до 18 година би пре пријавили старијима од осталих група, али би и оставили похвалне коментаре;
- жене су се, иако више склоне забораву и пасивности, у преко 3% определиле за остављање похвалних коментара или лајковање, односно, насмејале би се говору мржње, и то највише старости до 18 година и из места до 20.000 становника;
- старији од 45 година су и „најмудрији“ не би оставили похвалне коментаре нити би се насмејали и лајковали, највише би их пријавило полицији и то из места до 5000 становника;
- становници места преко 500.000 становника су веома пасивни и мање од осталих би пријавили полицији, поготово ако су у питању испитаници млађи од 18 година.

Ипак, изузетно је велики број свих категорија који уопште не би реговали, односно заборавили би да су ишта видели и то зато што их то не интересује. Таква количина летаргије у односу на овакве проблеме и туђе несреће могуће је да су последица огромног незнања, неразумевања или неосетљивости[723].

723 Indifference to the Suffering of Others Occupying the moral and ethical high ground through doublespeak, (2013), http://www.laetusinpraesens.org/docs10s/indiff.php; Landau R., (2014), We must not be indifferent to others suffering, http://www.thejc.com/comment-and-debate/comment/117790/we-must-not-be-indifferent-others-suffering, приступљено 5.4.2014;

ЛИТЕРАТУРА

1. 12 cybercimes a second: Beware rise in mobile app fraud, Russian anti-hacking czar warns, (2014), http://rt.com/news/cybercrime-victims-number-grow-427/
2. 2013 Cloud Computing Outlook – Cloud Computing Wave 5, https://451research.com/report-long?icid=2831
3. 2013 Cyber Attacks Statistics, http://hackmageddon.com/2013-cyber-attacks-statistics
4. 2013 Cyber Threat Landscape Review, (2014), http://www.sunsoft*onlin*e.com/wp/?p=2606
5. 2014 Best Cloud Computing Services Comparisons and Review, (2014), http://cloud-services-review. toptenreviews.com/
6. Aaron G., Rasmussen R., (2014), Global Phishing Survey 2H2013: Uni fying the Global Response To Cybercr ime Trends and Domain Name Use, http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf
7. ACMA, (2012), Communications report 2011. – 12 series Report 3 – Smarthphones and tablets Take –up and use in Australia, Summarz report, http://www.acma.gov.au/webwr/_assets/main/lib310665/report-3-smartphones_tablets-summary.pdf
8. ACPO Managers Guide Good Practice and Advice Guide for Managers of e-Crime Investigation, (2008), http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf
9. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, (2003), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
10. Adeniran I.A., (2008), The Internet and Emergence of Yahooboys sub-Culture in Nigeria, International Journal of Cyber Criminology,Vol 2 (2): 368–381, http://www.cybercrimejournal.com/adebusuyiijccdec2008.htm
11. AFP, (2012), Hacking victim talks about perils of digital age, http://www.hindustantimes.com/technology/gadgets-updates/hacking-victim-talks-about-perils-of-digital-age/article1-911989.aspx
12. Alienation, http://psychology.jrank.org/pages/22/Alienation.html
13. Alper J.S., (1995), Biological influences on criminal behaviour: how good is the evidence, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2548687/pdf/bmj00578-0006.pdf;
14. Alshalan A., (2005), Cyber-Crime Fear and Victimization: An Analysis of A national Survay, http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf
15. Amosun P.A, O Ige O.I., (2013), Impact Of An Action Cyber Crime Prevention Programme On In-School Aged Children's Attitude To Crime Prevention Concepts In Civic Education And Social Studies, Proceedings-st Annual International Interdisciplinary Conference, AIIC 2013, 24-26 April, Azores, Portugal, http://eujournal.org/index.php/esj/article/viewFile/1454/1463
16. Analytics, Cloud Computing Challenge Flat Growth in Forrester's Tech Market Outlook for 2012, (2012), http://socialmediatoday.com/wwwshirazdattacom/421657/analytics-cloud-computing-challenge-flat-growth-forrester-s-tech-market-out
17. Anđelić B. (1999), Ostajemo na internetu, Svet kompjutera, 6/1999., http://www.sk.rs/1999/06/skak01.html
18. Angeles S., (2013), 8 Reasons to Fear Cloud Computing, http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html
19. Anti-Defamation League, (2011), Extremism in Florida: The Dark Side of the Sunshine State, http://www.adl.org/assets/pdf/combating-hate/ExtremismFloridaINSIDE.pdf
20. Anti-NATO-War Site of the Group Neue Einheit, (1999), http://www.neue-einheit.com/english/anti-nato-war.htm
21. Antwi-Boasiako J., (2012), Six teenagers engage in mysterious Sakawa deal, http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=260823
22. APWG, (2013), Phishing Activity Trends Report, 1st Quarter 2013, http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf
23. APWG, (2014), Phishing Activity Trends Report, 3rd Quarter 2013. Unyfing of Global Response to Cybercrime, https://www.google.rs/search?hl=sr&q=,+Phishing+Activity+Trends+Report,+3rd+Quarter+2013.+U

nifying+of+Global+Response+to+Cybercrime&gbv=2&sa=X&as_q=&nfpr=&spell=1&ei=eV9oU5LfEcGGONOwgIAL&ved=0CBwQvwU
24. Arseneau C., The History of Cyberbullying, http://www.ehow.com/about_6643612_history-cyberbullying.html
25. ASCL Certified Cyber Crime Investigator
26. Aseef N., Davis P., Mittal M., Sedky K., Tolba A., (2005), White Paper: Cyber-Criminal Activity and Analysis. http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf
27. Attitudes to Crime and Punishment: A New Zealand Study, http://www.rethinking.org.nz/assets/Newsletter_PDF/Truth_in_Justice/V2/Auckland_Uni_Attitudes_crime_punishment.pdf
28. Attitudes to punishment: findings from the British Crime Survey, http://www.icpr.org.uk/media/10372/Attitudes%20to%20punishment,%20hors179.pdf
29. Attracting more young women into STEM (Science and Technology) in Ireland, http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAAFKXTX&men=BAAFKZBY&fmn=BAAFLAFT
30. Aune N., (2009), Cyberbullying, http://www2.uwstout.edu/content/lib/thesis/2009/2009aunen.pdf
31. Australian Institute of Criminology, (1999), 9 Types of Cyber Crime, http://www.aic.gov.au/crime_types/cybercrime/definitions.html
32. Australian Social Trends, (2013), Characteristics of higher education students, http://www.abs.gov.au
33. Axelrod R., Rumen I., (2013), Timing of cyber conflict, http://www.pnas.org/content/early/2014/01/08/1322638111
34. Bailey J., (2011), The Increasing Sophistication of Cybercriminals: Techonomy's "Insecurity" Panel, http://www.forbes.com/sites/techonomy/2011/11/15/the-increasing-sophistication-of-cybercriminals-techonomys-insecurity-panel/
35. Barnett C., (2000), The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data, http://www.fbi.gov/stats-services/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf
36. Beating cybercrime, Security Program Management from the board's perspective, (2013), http://www.ey.com/Publication/vwLUAssets/Beating_cybercrime:_Security_Program_Management_from_the_Board%E2%80%99s_perspective/$FILE/EY-Beating-Cybercrime.pdf
37. Becker G.S., Crime and Punishment: An Economic Approach, http://www.nber.org/chapters/c3625.pdf
38. Bednar M.P., Katos V., Hennell C., (2009), On the Complexity of Collaborative Cyber Crime Investigations, Digital Evidence and Electronic Signature Law Review, Vol 6, *journals.sas.ac.uk/deeslr/article/download/1894/1831*
39. Bejatović S., Đurđić V., Škulić M., Ilić G., Kiurski J., Matić M., Lazić R., Nenadić S., Trninić V., (2012), Primena načela oportuniteta u praksi, izazovi i preporuke, Udruženja javnih tužilaca i zamenika javnih tužilaca Srbije, http://www.partners-serbia.org/wp-content/uploads/2013/06/primena.nacela.oportuniteta-publikacija1.pdf
40. Bernik I., (2013), Cybercrime and Cyber Warfare, Wiley, FOCUS Series
41. Bernik I., Dobovšek B., Markelj B., (2013), To fear or not to fear on cybercrime, Innovative Issues and Approaches in Social Sciences, Vol. 6, No. 3., http://www.iiass.com/pdf/IIASS-2013-no3-art01.pdf
42. *Bernik I., Prislan K.,* (2012), *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem,* Fakulteta za varnostne vede, Ljubljana
43. Black Hat White Hat and Gray Hat Hackers Definition, http://ethical-hacking-course.blogspot.com/2012/01/ethical-hacking-is-considered-as-craft.html
44. Brennan S., (2012), Victimization of older Canadians, 2009, http://www.statcan.gc.ca/pub/85-002-x/2012001/article/11627-eng.pdf
45. Brenner S.W., Clarke L., (2010), Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. 43:, http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/Brenner-_Final_1.pdf
46. Brenner W.S., (2002), Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina Journal Of Law & Technology Volume 4, Issue 1.
47. Brenner W.S., (2004), Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law & Technology Association, Vol. 9, No. 13 http://www.vjolt.net

48. British Institute of Human Rights for Council of Europe, (2012), Young People Combating Hate Speech On-line, Mapping study on projects against hate speech *online*, www.coe.int/.../2012_Mapping_projects_against_Hate_Speech.pdf
49. Broadhurst R., Grabosky P., Alazab M., Bouhours B., Chon S., Da C., (2013), Crime in Cyberspace: Offenders and the Role of Organized Crime Groups, http://ssrn.com/abstract=2211842
50. Brown D., (2014), Is This the Year of the Hybrid Cloud?, http://www.hybridcloudforum.com/45/year-hybrid-cloud
51. Brunton-Smith I., Hopkins K., (2013), The factors associated with proven re-offending following release from prison: findings from Waves 1 to 3 of SPCR, Results from the Surveying Prisoner Crime Reduction (SPCR) longitudinal cohort study of prisoners), http://socialwelfare.bl.uk/subject-areas/services-client-groups/adult-offenders/ministryofjustice/157543re-offending-release-waves-1-3-spcr-findings.pdf
52. BSA Global cloud computing scorecard, http://cloudscorecard.bsa.org/2012/
53. Bubanja B. (1999), Iza kulisa, http://www.sk.rs/1999/07/skin01.html
54. Budka P. (2011), From Cyber to Digital Anthropology to an Anthropology of the Contemporary?, http://www.media-anthropology.net/file/budka_ contemporary.pdf
55. Burgard A., Schlembach C., (2013),Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet, International Journal of Cyber Criminology (IJCC), July – December 2013, Vol 7 (2): 112–124, http://www.cybercrimejournal.com/burgardschlembachijcc2013 vol7issue2.pdf
56. Buss M.D., (2012), The Evolutionary Psychology of Crime, Journal of Theoretical and Philosophical criminology Commentary, Special edition, January, 2012, Vol. 1(1):90-98, http://homepage.psy.utexas.edu/HomePage/Group/BussLAB/pdffiles/Evolutionary-psychology-and-crime.pdf
57. Byrne N., (2008), Camouflage attacks now standard for cyber-criminals, http://www.siliconrepublic.com/enterprise/item/9839-camouflage-attacks-now-stan
58. Cardenas A.A., Radosavac S., Grossklags J., Chuang J., Hoofnagle C., (2009), An Economic Map of Cybercrime, http://chess.eecs.berkeley.edu/pubs/772/cardenas_2009.pdf;
59. Carnahan P., Roberts D., Shay Z., Yeary J., (2005), The motivation behind computer viruses, http://vxheaven.org/lib/pdf/The%20motivation%20behind%20computer%20viruses.pdf
60. Centre for International Crime Prevention Office for Drug Control and Crime Prevention United Nations Interregional Crime and Justice Research Institute, (1999), Global studies on organized crime, http://www.uncjin.org/CICP/gsoc_e.pdf
61. Cevidalli A., (2010), Leveraging The Multi-Disciplinary Approach to Countering Organised Crime, http://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-06.pdf; Europol, Socta 2013 EU Serious and Organised Crime, Threat Assessment, https://www.europol.europa.eu/sites/default/files/ publications/socta2013.pdf
62. Cevidalli A., Austenf J., (2010), The Challenge of Combating *Online* Organised Crime – A Multi-Disciplinary Perspective, http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Cevidalli_2010.pdf
63. Chabinsky R.S., (2010), The Cyber Threat: Who's Doing What to Whom?, Cyber Division Federal Bureau of Investigation http://www.fbi.gov/ news/speeches/the-cyber-threat-whos-doing-what-to-whom
64. Chadee D., (1999), Fear of Crime, Safety and Community Integration: Another Fear-Safety Paradox? https://www.jiscmail.ac.uk/.../filearea.cgi
65. Chawki M., (2005), A Critical Look at the Regulation of Cybercrime A Comparative Analysis with Suggestions for Legal Policy, http://www.droit-tic.com/pdf/chawki4.pdf
66. Chensney-Lind M., (1986), Women i Crime, The female offenders, http://www.jstor.org/discover/10.2307/3174358?uid=3738928&uid=2129&uid=2&uid=70&uid=4&sid=21103473239181
67. Cherry K., (2014), Attitudes How Attitudes Form, Change and Shape Our Behavior, http://psychology.about.com/od/socialpsychology/a/attitudes.htm; Schwarz N., Bohner G., (2001), The Construction of Attitudes, http://sitemaker.umich.edu/norbert.schwarz/files/schwarzz___bohner_attitude-construction-ms.pdf
68. Chiea R., Hackers Profiling: Who Are the Attackers?, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=302:hackers-profiling-who-are-the-attackers&catid=50:issue-7&Itemid=187

69. Chik B.W., Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore, www2.law.ed.ac.uk/ahrc/complaw/docs/chik.doc
70. Chiu Y.D., Wang S.C., Chung T.T., (2010), Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach, Academy Publisher, Journal of software, vol. 5, no. 12, December 2010, pp. 1349–1354, www.*ojs.academypublisher.com*
71. Chon S., Broadhurst R., Routine Activity Theory and Cybercrime: What about Offender Resources, http://ssrn.com/abstract=2379201
72. Cloud Computing Penetration into Enterprise IT Gaining Momentum WaveLength Market Analytics & Winn Technology Group Report Says Early Cloud Users and Planners Estimate 30% of IT will be Cloud-based by 2015, (2011), http://www.businesswire.com/news/home/20110517005132/en/Cloud-Computing-Penetration-Enterprise-Gaining-Momentum
73. Cloud Services Users Will Hit 625 Million in 2013: IHS, http://slashdot.org/topic/cloud/cloud-services-users-will-hit-625-million-in-2013-ihs/
74. CoE, (2001), Convention on Cybercrime, Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
75. Cohen S., (2002), Folk Devils and Moral Panics: The Creation of the Mods and Rockers, 3rd Edition, London, Routledge
76. Coldwell R.A., (1990), Computer Crime: A Social Perspective, Ed.: Essays on Computer Law, Melbourne, Longman Chechire Pty. Lim.
77. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, (2012) Unleashing the Potential of Cloud Computing in Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
78. Conference report, (2013), European conference on cyberbullying, http://deletecyberbullying.files.wordpress.com/2013/09/euconference-cyberbullying-28-may-madrid-conference-final-report1.pdf
79. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, (1950), amended by its Protocol No. 14 (CETS No. 194), (2010), http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
80. Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185& CL=ENG
81. Council of Europe, (1997), Committee of ministers, Recommendation no. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech", http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1997)020&expmem_EN.asp
82. Council of Europe, (2001), Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
83. Council of Europe, (2011), Internet Governance - Developing the future together, http://www.un.org/en/sc/ctc/specialmeetings/ 2011/docs/coe/coe-hInf_2011_4.pdf
84. Council of the European Union, (2011), Joint Investigation Teams Manual, https://www.europol.europa.eu/sites/default/files/st15790-re01.en11.pdf
85. Crerar D., (2011), No Hiding Place in Cyberspace: Electronic Discovery from Non-Parties 2011 Updated Version, http://www.blg.com/en/newsandpublications/documents/DAC_Article_-_No_Hiding_ Place_in_ Cyberspace_JAN2011.pdf
86. Criminal Code on Computer Crime, (2001), http://www.cybercrimelaw.net/Belgium.html
87. *Criminol J.,* (2010), Functional Fear and Public Insecurities About Crime, British Journal of Criminology**,** 50 (1): 1-22;
88. Cyber bullying trends force parents to keep up, (2013), http://www.stuff.co.nz/dominion-post/news/9251149/Cyber-bullying-trends-force-parents-to-keep-up
89. Cyber crime is Europe's 'big challenge', (2012), http://www.dw.de/cyber-crime-is-europes-big-challenge/a-15988087
90. Cyber Crime Offenders of Younger Age Group Rising: National Crime Records Bureau, (2013), http://www.jagranjosh.com/current-affairs/cyber-crime-offenders-of-younger-age-group-rising-national-crime-records-bureau-1375079356-1
91. Cyber risk assessment, http://www.baesystemsdetica.com/resources/cyber-risk-assessment/

92. Cybercrime on social networks continues to climb, (2011) http://www.net-security.org/secworld.php?id=11464
93. Cybercrime, (2013), http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
94. Daly J., (2013), 13 Cloud Computing Stats for CIOs, http://www.statetechmagazine.com/article/2013/09/13-cloud-computing-stats-cios
95. Damjanović A., Damjanović A., Pantović M., Barišić J., (2011), Zašto volimo da se plašimo? – Psihofiziologija horor filma, http://www.psihijatrijakcs.org/klinika_psihijatrija/pdf_engrami/zasto-volimo-da-se-plasimo-psihofiziologija-horor-filma.pdf
96. Danish national project for attracting more girls to technical high-schools, (2012), http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAACAYPX&men=BAAFKZBY&smen=BAAFLAIR&fmn=BAAFLAFT
97. Data Security Concil of India, (2011), Cyber crime Investigation Manuel, http://uppolice.up.nic.in/All%20Rules/ Cyber%20crime/4-Cyber_Crime_Investigation_Manual.pdf
98. Daugherty A., (2013), Women know less about politics than men, study finds (that goes for Canada, too), http://www.theglobeandmail.com/life/the-hot-button/women-know-less-about-politics-than-men-study-finds-that-goes-for-canada-too/article12947354/
99. Dedić G., (2003), Kvalitet života vojnika za vreme služenja vojnog roka, Vojnosanitetski pregled, br. 3, str. 305-314
100. Denning E.D., Baugh E. W., (1999), Hiding Crimes in Cyberspace, *Information, Communication and Society*, Vol. 2, No 3, http://lotstoread.tripod.com/faqs/hiding.html
101. Detica, (2012), Organised Crime in the Digital Age: The Real Picture, Executive Summary of BAE Systems Detica and the John Grieve Centre for Policing and Community Safety 'Organized Crime in the Digital Age' research report, http://www.baesystemsdetica.com/uploads/resources/ORGANISED_ CRIME _IN _THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf
102. Digital Agenda for Europe, (2013), Women in ICThttp://ec.europa.eu/digital-agenda/en/women-ict
103. Dingarac D., (1999), Internetom protiv bombi, Ratovi se danas vode na razne načine. Internet je jedno od oružja koje i mi posedujemo, Svet kompjutera, 4/1999., http://www.sk.rs/1999/04/skak01.html
104. Dingarac D., (1999), Na Mreži, na položaju, Dok razaranja naše zemlje traju, Internet je ostao jedino oružje koje građani mogu da upotrebe protiv agresora, Svet kompjutera, 5/1999., http://www.sk.rs/1999/05/skak01.html
105. Dingarac D., Stančević T., (1989), Srpski hakeri „Crna ruka", Svet kompjutera, 11/1998., http://www.sk.rs/1998/11/skin03.html
106. Ditch the Label, (2013), The annual cyberbullying survey, http://www.ditchthelabel.org/annual-cyber-bullying-survey-cyber-bullying-statistics
107. Donegan R., (2012), Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis, http://www.elon.edu/docs/e-web/academics/communications/research/vol3no1/04DoneganEJSpring12.pdf
108. Doyle C., (2013), Cybersecurity: Cyber Crime Protection Security Act (S. 2111, 112th Congress) - A Legal Analysis, http://www.fas.org/sgp/crs/misc/R42403.pdf
109. Drakulic M., Drakulic R., (1999), Balkan Hackers War in Cyberspace, BILETA, CYBERSPACE 1999: Crime, Criminal Justice and the Internet", http://www.bileta.ac.uk/content/files/conference%20papers/1999/Balkan%20Hackers%20War%20in%20Cyberspace.pdf
110. Drakulic M., Drakulic R.,(2000), Privacy in the Yugoslav Cyberspace -Problems and Protection, 15th BILETA Conference: Electronic Datasets and access to legal information, http://www.bileta.ac.uk/content/files/conference%20papers/2000/Privacy%20in%20the%20Yugoslav%20Cyberspace%20-%20Problems%20and%20Protection.pdf
111. Drakulić M., (1996), Osnovi Kompjuterskog prava, Beograd, DOPIS, str.12
112. Drakulić M., Drakulić R., (1996), Hakerska etika u kontekstu profesionalne etike informatičara, Zbornik radova: II naučni skup, Tehnologija, razvoj i kultura, Herceg Novi, 1996. str. 136–153
113. Drakulić M., Drakulić R., (2005), Cyber kriminal, www.bos.org.yu/cepit/drustvo/sk/cyberkriminal.pht
114. Drakulić M., Drakulić R., (2010), Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnom evropskom pravu, Telekomunikacije, br. 6/2010, http://www.telekomunikacije.rs/arhiva_brojeva/sesti_broj/prof_dr_mirjana_drakulic,_mr_ratimir_drakulic:_evropska_perspektiva_regulisanja_internet_usluga:_izazov_tradicionalnom_evropskom_pravu.344.html

115. Drakulić M., Drakulić R., (2010), Regulacija interneta, studija, RATEL, Beograd
116. Drakulić, M., Drakulić, R., (1999), Deca i zloupotreba interneta, Beograd, Jugoslovenski komitet pravnika za ljudska prava
117. Duhaime J.C., Europol issues organized crime threat assessment focusing on cybercrime, hacking, money laundering and drugs, http://www.duhaimelaw.com/2013/03/21/europol-issues-organized-crime-threat-assessment-focusing-on-cybercrime-hacking-money-laundering-and-drugs/
118. Dunlap C.J., (2008), Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors, http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1032&context=nlr
119. Đorđević D., (2006), Religije i veroispovesti nacionalnih manjina u Srbiji, Sociologija, Vol. XLVII (2005), N° 3, str. 193 - 212-. http://www.doiserbia.nb.rs/img/doi/0038-0318/2005/0038-03180503193D.pdf
120. Đurić-Lulić A., (2003), Mogućnosti krivično-pravne zaštite od kompjuterskog kriminaliteta po pozitivnom zakonodavstvu SRJ, www.netizen.co.yu/toni/2ojt/index:php?strana=kompjuteri
121. ECRI General Policy Recommendation No. 7 on national legislation to combat racism and racial discrimination, (2003), http://www.coe.int/t/dghl/monitoing/ecri/activities/gpr/en/recommendation_n7/ecri03-8%20recommendation%20nr%207.pdf
122. ECRI Secretariat Directorate General of Human Rights and Legal Affairs Council of Europe, (2011), Извештај ЕКРИ о Србији, http://www.coe.int/t/dghl/monitoring/ecri/country-by-country/serbia/SRB-CbC-IV-2011-021-SRB.pdf
123. Edgington S., (2014), Pediatrics, answered, http://www.sharecare.com/health/parenting-teens/what-is-sextortion
124. ELSA International *Online* Hate Speech Competition, (2012), *Online* Hate Speech: Hate or Crime?, Legal issues in the virtual world - Who is responsible for *online* hate speech and what legislation exists that can be applied to react, counter or punish forms of hate speech *online*?, www.elsa.org/.../*Online*_Hate_Speech_Essay_Competition_runner_up.pdf
125. EMC&RSA (The Security Division of EMC), (2014), 2013 a Year in Review, January 2014, www.emc.com/rsa
126. ENISA, (2011), New report: Cyber bullying & *online* grooming: 18 protective recommendations against key risks, http://www.enisa.europa.eu
127. Erickson L.M., (1973), Delinquency in a Birth Cohort: A New Direction in Criminological Research, Journal of Criminal Law and Criminology, Volume 64 | Issue 3, pp. 362 – 367., http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5866&context=jclc
128. Esquibel E.J., Laurenzano A.M., Xiao J.J., Zuvich T., (2005), Cyber Criminal Activity: Methods and Motivations
129. EU Skills Panorama Analytical Highlight, (2012), Information and Communications Technologies (ICT) sector, http://euskillspanorama.cedefop.europa.eu/docs/AnalyticalHighlights/ICT_Sector_en.pdf
130. Eurobarometer Special Surveys 404, Cyber security, report, Fieldwork: May - June 2013, Publication: November 2013, http://ec.europa.eu/public_opinion/index_en.htm
131. European Commission, (2000), Recommendation No. 6 on Combating the Dissemination of Racist, Xenophobic and Antisemitic material via the Internet
132. European Commission, (2012), Commission Staff Working Document, Exploiting the employment potential of ICTs Accompanying the document Communication From The Commission To The European Parliament, The Council, The European Social And Economic Committee And The Committee Of The Regions, Towards a job-rich recovery, ec.europa.eu/social/BlobServlet?docId=7628&langId=en
133. European Commission, (2012), Communication on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF
134. European Commission, (2013), Special Eurobarometer 404, Cyber Security, Report, Fieldwork: May - June 2013, Publication: November 2013, http://ec.europa.eu/public_opinion/index_en.htm
135. European Concil, (2003), Declaration on freedom of communication on the Internet
136. European Crime Prevention Network, (2004), A Review of Scientifically Evaluated Good Practices For Reducing Feelings of in Security or Fear of Crime in the EU Member States, http://www.eucpn.org/pubdocs/review_reducing_feelings_insecurities_fear_crime_en.pdf
137. Europol, (2013), Strategy & Prevention, https://www.europol.europa.eu/ec3/strategy

138. Facebook users in the world, Facebook Usage and Facebook Growth Statistics By World Geographic Regions, http://www.internetworldstats.com/facebook.htm
139. Fadia A., (2005), The Ethical Hacking Guide to Corporate Security, http://www.centroatl.pt/titulos/tecnologias/imagens/e-book-ca-corporate-security-excerpt.pdf
140. Fafinski S., Dutton W.H., Margetts H., (2010), Mapping and Measuring Cybercrime, OII Forum Discussion Paper No 18, http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf
141. Fairlie W.R., Kalil A., (2014), The Effects of Computers on Cyberbullying and Social Participation among Schoolchildren: Evidence from a Field Experiment, http://www.iza.org/conference_files/riskonomics2014/fairlie_r1726.pdf
142. FBI, (2012), Uniform Crime Reporting Program, Hate Crime Statistics, 2012, http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2012/topic-pages/victims/victims_final.pdf
143. FBI, (2013), Operation Cross Country Recovering Victims of Child Sex Trafficking, http://www.fbi.gov/news/stories/2013/july/operation-cross-country-recovering-victims-of-child-sex-trafficking
144. FBI, (2014), Cyber's Most Wanted, http://www.fbi.gov/wanted/cyber
145. FBI, Wanted by FBI, http://www.fbi.gov/wanted/dt/donna-joan-borup/view
146. Ferraro K., (1995), Fear of Crime: Interpreting Victimization Risk, New York, SUNY Press
147. Filshtinskiy S., (2013), Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air?, Communications of the ACM, Vol. 56 No. 6, pp. 28-30
148. Findley K.A., (2008), Toward A New Paradigm Of Criminal Justice: How The Innocence Movement Merges Crime Control And Due Process, https://media.law.wisc.edu/m/dfknm/findley_new_paradigm-10-10-08.pdf
149. Finklea K.M., Theohary C.A., (2013), Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, Congressional Research Service, http://www.fas.org/sgp/crs/misc/R42547.pdf
150. Finnie T., Peteet T., Jarvis J., ed., (2010), The Future Challenges of Cybercrime: Volume 5 Proceedings of the Futures Working Group, http://futuresworkinggroup.cos.ucf.edu/docs/Volume%205/index.php
151. Fishbein D., (1966), Biological Perspectives In Criminology, http://criminology.fsu.edu/crimtheory/fishbein90.htm
152. Floreencio D., Herley C., (2011), Sex, Lies and Cybercrime Surveys, http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf
153. Fötinger S.C., Ziegler W., Understanding a hacker's mind – A psychological insight into the hijacking of identities, a White Paper by the Danube-University Krems, Austria, http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf
154. Fox A.K., Nobles R.M., Piquero R.A., (2009), Gender, crime victimization and fear of crime, Security Journal, vol. 22, 1, pp. 24/39
155. Fu X., Ling Z., Yu W., Luo J., (2010), Cyber Crime Scene Investigations (C2SI) through Cloud Computing, http://www.cs.uml.edu/~xinwenfu/paper/SPCC10_Fu.pdf
156. Gabrić Molnar I., (2007), Karakteristike ljudskog resursa u regionu (Demografske promene i migracije u Vojvodini i susednim regionima), http://gabritymolnariren.com/demografske.pdf
157. Gallup/CNN/USA Today Pollhttp (1999), www.pollingreport.com/serb9903.htm
158. Garofalo J., (1981), The Fear of Crime: Causes and Consequences, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6243&context=jclc
159. Gartner Special Report Examines How Businesses Must Meet Consumers' Cloud Expectations in Order to Win Customers, http://www.gartner.com/newsroom/id/1947315
160. Gender Balance and Gender Perspectives in Research and Innovation, (2014), http://www.womenandtechnology.eu/digitalcity/projects/w4ict/boxedNewsEvent.jsp?dom=AAABECDQ&prt=BAAFLAFR&firt=AAAFBTEG&men=BAAFKZBY&smen=BAAFKZBY&fmn=BAAFLAFT
161. Gender equality and empowerment of women through ICT, (2005), http://www.un.org/womenwatch/daw/public/w2000-09.05-ict-e.pdf
162. Gercke M., (2009), An introduction to cybercrime, http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf.
163. Getoš A.M., Giebel S., (2012), Strah od kriminala među studentima pravnog fakulteta u Splitu, Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012., str. 533.- 552.
164. Ghernaouti-Hélie S., (2004), Increase trust and confidence in information and communication technologies by a multidisciplinary approach, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.198.3785&rep=rep1&type=pdf

165. Ghosh S., Turrini E., editors, (2010), Cybercrimes: A Multidisciplinary Analysis, http://f3.tiera.ru/2/Cs_Computer%20science/Ghosh%20S.,%20Turrini%20E.%20(eds.)%20Cybercrimes..%20A%20multidisciplinary%20analysis%20(Springer,%202010)(ISBN%203642135463)(0)(435s)_Cs_.pdf
166. Ghosh S., Turrini E., editors, (2010), op. cit.
167. Give and Take Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime, (2012), www.enisa.europa.eu
168. Goethals G.F.,Carugati A., Leclercq A., (2009), Differences in e-commerce behavior between neighboring countries: the case of France and Belgium, ACM, Vol. 40, Iss. 4.
169. Goggin G.P.C., Cullen T.F., (1999), The Effects of Prison Sentences on Recidivism, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ffcts-prsn-sntncs-rcdvsm/index-eng.aspx
170. Goh Guan Gan G., Nya Ling T., Choon Yih G., Cyril Eze U., (2008), Phishing: A Growing Challenge for Internet Banking Providers in Malaysia, Communications of the IBIMA, Volume 5, pp. 133 – 142., http://www.ibimapublishing.com/journals/CIBIMA/volume5/v5n17.pdf
171. Gomes S., Machado H., (2011), Media's made criminality: the construction of moral panic over gypsies and immigrants, http://www.inter-disciplinary.net/wp-content/uploads/2011/02/gomesppaper.pdf
172. Goodman M D., (1997), Why the police don't care about computer crime, Harvard Journal of Law & Technology Volume 10, Number 3., 468 - 469. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech 465.pdf
173. Goodwin V., Davis B., (2011), Crime families: Gender and the intergenerational transfer of criminal tendencies Trends & Issues in Crime and Criminal Justice no.414, Australian Institute of Criminology http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi414.html
174. Gordon S., Ford R., (2006), On the definition and classification of cybercrime, Journal in Computer Virology, August 2006, Volume 2, Issue 1, pp 13-20, http://link.springer.com/article/10.1007%2Fs11416-006-0015-z#page-1
175. Gottfredson G., & Hirschi T., (1990), A general theory of crime. Stanford, CA: Stanford University Press, http://www.mltei.org/cqn/Adolescent%20Development/Resources/Gender,%20Race,%20Ethnicity%20&%20SES/Gottfredson&%20Hirshi,%20A%20general%20theory%20of%20crime.pdf
176. Grabosky P., Computer Crime: A Criminological Overview, http://www.aic.gov.au/media_library/conferences/other/grabosky_peter/2000-04-vienna.pdf
177. Grabosky P., Stohl M., (2003), Cyberterrorism; http://www.alrc.gov.au/reform-journal
178. Gráinne Kirwan; Power A., (2012), The Psychology of Cyber Crime: Concepts and Principles, http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf
179. Gray E, Jackson J., Farrall S., (2009), In Search of the Fear of Crime: Using Interdisciplinary Insights to Improve the Conceptualisation and Measurement of Everyday Insecurities,
180. Gray P., (2005), Beware the crime lords of the internet, http://www.smh.com.au/news/Next/Beware-the-crime-lords-of-the-internet/2005/05/30/1117305534401.html
181. GRID Report: Q1 2014, http://www.fosigrid.org/files/fosigrid-q1-2014-report.pdf
182. Group/IB, (2012), State and Trends of the Russian digital crime market 2011, http://www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf
183. Grupa 484, (2010), Odliv mozgova iz Srbije - problemi i moguća rešenja, http://wbc-inco.net/object/document/7352/attach/2010majGrupa484OdlivmozgovaFinal.pdf
184. Gu L., (2013), Beyond *Online* Gaming Cybercrime: Revisiting the Chinese Underground Market, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-*online*-gaming-cybercrime.pdf
185. Gunarto H., (2003), Ethical Issues in Cyberspace and IT Society, http://www.apu.ac.jp/~gunarto/it1.pdf
186. H. R. 1966, A BILL To amend title 18, United States Code, with respect to cyberbullying, (2009), http://www.gpo.gov/fdsys/pkg/BILLS-111hr1966ih/pdf/BILLS-111hr1966ih.pdf
187. Hackers Write Computer Viruses (2009), http://gizmodo.com/5827405/why-hackers-write-computer-viruses
188. Håkansson A., Berglund M., (2012), Risk factors for criminal recidivism – a prospective follow-up study in prisoners with substance abuse, http://www.biomedcentral.com/1471-244X/12/111
189. Hale C., (2002), Cybercrime: Facts & Figures Concerning this Global Dilemma, Crime&Justice, September, Vol. 18 – Issue. 65

190. Hargeaves C., Prince D., (2013), Understuding Cyber Criminals and Measuring Thair Future Activities, Developing Cyber crime Research, http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_ cyber_criminals_and_measuring_their_activity.pdf
191. Hargreaves G., Prince D., (2011), Understanding Cyber Criminals and Measering Thair Future Activitiy, Developing Cyber crime Research, http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring _their_activity.pdf
192. Harley B., (2010), A Global Convention on Cybercrime?, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/
193. Harper, D., (2008), *Online etymology dictionary,* http://www.etym*online*.com/index.php?allowed_in_frame =0&search=bully&searchmode=none
194. Harris M., (2014), Europe's rules on freedom of information and hate speech, http://www.indexoncensorship.org/2014/01/eus-commitment-freedom-expression-freedom-information-hate-speech/
195. Here's Where Teens Are Going Instead Of Facebook, http://www.forbes.com/sites/parmyolson/2013/11/12/heres-where-teens-are-going-instead-of-facebook/
196. Hilvert J., (2010), Cybercrime response a win for self-regulation, http://www.itnews.com.au/News/239813, cybercrime-response-a-win-for-self-regulation.aspx
197. Himanen P., (2001), The hacker Ethic and the Spirit of Information Age, http://code.google.com/p/hfg-resources/downloads/detail?name=The.Hacker.Ethic.pdf
198. Hinduja S., (2007), Computer Crime Investigations in the United States:Leveraging Knowledge from the Past to Address the Future, International Journal of Cyber Criminology, Vol 1 Issue 1., http://www.cybercrimejournal.com/sameer.pdf
199. Hinduja S., Patchin W.J., (2014), State Cyberbullying Laws, A Brief Review of State Cyberbullying Laws and Policies, http://www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf
200. Hinduja S., Patchin W.J., (2010), Cyberbullying, Identification, Prevention and Response, http://www.mbfxc.com/uploads/4/1/8/4/4184069/hinduja_and_patchin.pdf
201. HM Government, (2013), Serious and Organised Crime Strategy, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf
202. Holt T.J., (2011), Cybercrime and Criminological Theory: Fundamental Readings on Hacking, Piracy, Theft, and Harassment, University Readers, San Diego;
203. Hough M., Roberts J., (1998), Attitudes to punishment: findings from the British Crime Survey, http://www.icpr.org.uk/media/10372/Attitudes%20to%20punishment,%20hors179.pdf
204. Human Rights Council, (2009), Twelfth session, Agenda item 3, Promotion And Protection Of All Human Rights, Civil, Political, Economic, Social And Cultural Rights, Including The Right To Development, Resolution adopted by the Human Rights Council, 12/16; Freedom of opinion and expression, http://www.globalgovernancewatch.org/docLib/20091216_US-Egypt_Compromise-1.pdf
205. Human Rights Council, (2012), Twentieth session, Agenda item 3, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, https://geneva.usmission.gov/2012/07/05/internet-resolution/
206. ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE and ISACA Belgium, (2013), Belgian Cyber Security Guide, Protect Your Information, https://www.b-ccentre.be/wp-content/uploads/2013/11/BCSG.pdf
207. Icove D., Seger K. VonStorch W., (1995), Computer Crime, http://oreilly.com/catalog/crime/chapter/cri_02.html
208. Ignjatović Đ., (2011), Pojam i etiologija nasilničkog kriminaliteta, CRIMEN (II) 2/2011, str 179–211, http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen_002-2011_02.Ignjatovic.pdf
209. INACH, (2014), Headlines May 2014, http://www.inach.net/news.php
210. India Ministry Of Law, Justice And Company Affairs, (2000), The Informtion Technology Act, http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf
211. Indifference to the Suffering of Others Occupying the moral and ethical high ground through doublespeak, (2013), http://www.laetusinpraesens.org/docs10s/indiff.php

212. Internet Crime Complaint Center, (2012), 2012 Internet Crime Report, http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf
213. Internet Statistics, http://www.statisticbrain.com/internet-statistics/
214. Internet World Stats, http://www.internetworldstats.com/stats4.htm
215. Internet World Stats, http://www.internetworldstats.com/stats9.htm
216. Internet World Stats, www.internetworldstats.com/facebook.htm
217. ISECOM, Open Methodologies, http://www.isecom.org/
218. ISM Projected To Cost U.S. Cloud Computing Industry $35B, http://www.forbes.com/sites/louiscolumbus/2013/08/08/prism-projected-to-cost-u-s-cloud-computing-industry-35b/
219. ITU, (2012), Understanding cybercrime: Phenomena, challenges and legal response, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
220. ITU, Percentage of Individuals using the Internet, www.itu.int/en/
221. Jackson J., (2006), Introducing Fear of Crime to Risk Research, Risk Analysis, Vol. 26, No. 1, pp. 253–264
222. Jackson J., Farrall S., Gadd D., (2004),Filtering Fear?, On the Use of Filter and Frequency Questions in Crime Surveys, http://www.lse.ac.uk/socialPolicy/Researchcentresandgroups/mannheim/JonJackson/FilteringFear.pdf
223. Jackson J., Gousetl I., (2013), Fear of Crime, http://www.academia.edu/1815559/Fear_of_Crime_An_Entry_to_the_Encyclopedia_of_Theoretical_Criminology
224. Jaishankar K., (2008), Cyber Hate: Antisocial networking in the Internet, International Journal of Cyber Criminology, Vol 2 (2): 16–20, http://www.cybercrimejournal.com/editorialijccjuly2008.pdf
225. Jaishankar K., (2008). Space Transition Theory of cyber crimes. In Schmallager F., Pittaro M. (Eds.), Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall
226. Jarrett H.M., Bailie W.M., (2009), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
227. Jaser J., (2010), Smart Phones: The Next Cyber Crime Frontier, http://www.cocc.com/smart-phones-cyber-crime.html
228. Jerković R., Borba protiv visokotehnološkog kriminaliteta u Srbiji, Telekomunikacije, http://www.telekomunikacije.rs/arhiva_brojeva/treci_broj/ranko_jerkovic:_borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html
229. Johnson R.D., Post G.D., (1996), Law and Borders - The Rise of Law in Cyberspace, Stanford Law Review, Vol. 48, pp. 1367, http://ssrn.com/abstract=535
230. Kaspersky Lab, (2013), Global Corporate IT Security Risks: 2013, http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf
231. Keeney M., Cappelli D., Kowalski E. Moore A., Shimeall T., (2005), Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, http://www.secretservice.gov/ntac/its_report_050516.pdf
232. Khadam N., (2012), Insight to Cybercrime, http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf
233. Kirwan G., Power A., (2011), The Psychology of Cyber Crime: Concepts and Principles, IGI Global
234. Klee M., (2014), The new era of organized cybercrime, http://www.dailydot.com/crime/ organized-crime- cybercrime-obsolete/
235. Klinteberg B., Almquist Y., Beijer U., Rydelius A.P., (2011), Family psychosocial characteristics influencing criminal behaviour and mortality - possible mediating factors: a longitudinal study of male and female subjects in the Stockholm Birth Cohort, http://www.biomedcentral.com/1471-2458/11/756
236. Knight A., (2014), Where are the female hackers?, http://www.smh.com.au/small-business/franchising/where-are-the-female-hackers-20140228-33ogc.html
237. Kolarić D., (2013), Nova koncepcija krivičnih dela terorizma u Krivičnom zakoniku Republike Srbije, CRIMEN (IV) 1/2013, str. 49–71., http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen_001-2013/Broj%201-2013%20-%2004%20Dragana%20Kolaric.pdf
238. Kovačič M., (2008), Kiberkriminal, http://matej.owca.info/predavanja/Kibernetski_kriminal_Kovacic.pdf

239. Krinsky C., (2010), Introduction: The Moral Panic Concept, http://www.ashgate.com/pdf/SamplePages/Ashgate-Research-Companion-to-Moral-Panics-Intro.pdf
240. Kropotkin P., (1927), Prisons and Their Moral Influence on Prisoners, http://dwardmac.pitzer.edu/anarchist_archives/kropotkin/revpamphlets/prisonsmoral.html
241. LaBarge R., McGuireT., (2012), Cloud Penetration Testing, http://arxiv.org/ftp/arxiv/papers/1301/1301.1912.pdf
242. Ladbury A., (2013), Fears over cybercrime rising among EU consumers, http://www.commercialriskeurope.com/cre/2832/239/Fears-over-cybercrime-rising-among-EU-consumers
243. Landau R., (2014), We must not be indifferent to others suffering, http://www.thejc.com/comment-and-debate/comment/117790/we-must-not-be-indifferent-others-suffering
244. Lardinois F., Report: Cloud Storage Services Now Have Over 375M Users, Could Reach 500M By Year-End, http://techcrunch.com/2012/10/15/report-cloud-storage-services-now-have-over-375m-users-could-reach-500m-by-year-end/
245. Lee M., (2001), The Genesis of `Fear of Crime', Theoretical Criminology November 2001 vol. 5 no. 4, 467-485;
246. Legal and Ethical Aspects, http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-23.pdf
247. Leonard C., (2013), New Phishing Research: 5 Most Dangerous Email Subjects, Top 10 Hosting Countries, https://community.websense.com/blogs/websense-insights/archive/2013/12/10/new-phishing-research-5-most-dangerous-email-subjects-top-10-hosting-countries.aspx
248. Li X., (2008), The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited Through Typical Cases Prosecuted, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034529
249. Libin A., Libin E., (2005), Cyber-anthropology: a new study on human and technological co-evolution. Stud Health Technol Inform. 118:146-55;
250. Lickiewicz J., (2011), Cyber crime psychology – proposal ofan offender psychological profil, Problems of Forensic Sciences 2011, vol. LXXXVII, 239–252, http://www.forensicscience.pl/component/option,com_jbook/task,view/Itemid,2/catid,72/id,664/lang,en/
251. Lipson H., (2002), Trackin and Tracing Cyber/Attacks: Technical Challenges and Global policy Issues, http://www.dtic.mil/dtic/tr/fulltext/u2/a408853.pdf
252. Lohmann R., (2014), Psychology, answered on behalf of Top 10 Social HealthMakers, http://www.sharecare.com/health/parenting-teens/what-is-sextortion
253. Lu C.C., Jen Y.W., Chang W., Shihchieh C., (2006), Cybercrime& Cybercriminal: An Overview of the Taiwan Experience, Journal of Computers, vol. 1, no. 6
254. Ljubičić S., Stephenson P., Murrill R., Laličić L., (2013), Tehnički dokument Procena sadašnjeg stanja u pogledu statistike o korupciji i privrednom kriminalu i preporuke za poboljšanja u merenju napretka u upravljanju predmetima i njihovom praćenju, http://www.coe.org.rs/REPOSITORY/2930_1_tp2_2013_pacs_assessment_statistics_and_track_record_serb.pdf
255. March 2013 Cyber Attacks Statistics, http://hackmageddon.com/2013-cyber-attacks-statistics/#July
256. Mass S., (1982), The Dilemma of the Intimidated Witness in Federal Organized Crime Prosecutions: Choosing Among the Fear of Reprisals, the Contempt Powers of the Court, and the Witness Protection Program, Fordham Law Review. Volume 50 | Issue 4, pp. 582 – 610, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4556&context=flr
257. Mastronardi E., (2014), Charlotte's Law - Tougher Cyber Bullying Legislation, https://www.change.org/en-AU/petitions/malcolm-turnbull-charlotte-s-law-tougher-cyber-bullying-legislation
258. McAfee A., (2012), Modeling the Cost of Cloud vs. On-Premise Computing, http://policybythenumbers.blogspot.com/2012/10/modeling-costs-of-cloud-vs-on-premise.html
259. McGonagle T., (2013), The Council of Europe against *online* hate speech: Conundrums and challenges, http://www.ivir.nl/publications/mcgonagle/Expert_paper_hate_speech.pdf
260. McGuire M., (2012), Organised Crime in the Digital Age, London: John Grieve Centre for Policing and Security, https://www.baesystemsdetica.com/news/organised-crime-in-the-digital-age/
261. McGuire M., (2013), Cyber crime: A review of the evidence Research Report 75, Chapter 1: Cyber-dependent crimes,

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/ horr75-chap1.pdf
262. McGuire M., (2013), Cyber crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
263. McGuire M., Dowling S., (2013), Cyber crime: A review of the evidence, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf
264. McGuire M., (2013), Cyber crime: A review of the evidence Research Report 75, Chapter 3: Cyber-enabled crimes - sexual offending against children, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf
265. McQuade C.S. III, (2009), Encyclopedia of Cybercrime, London, Greenwood Press
266. Media centar, http://www.mc.rs/govor-mrznje-na-internetu.3542.html
267. Meyer C., (2010), Why Does the Passive Aggressive Play the Victim Role?, http://divorcesupport.about.com/od/abusiverelationships/a/PassiveAggressive_Victim.htm
268. Miladinović D., (2007), Institut pomilovanja u svetlu restorativne pravde, Temida, Maj 2007, str 37-45, http://www.doiserbia.nb.rs/img/doi/1450-6637/2007/1450-66370701037M.pdf
269. Miller M., (2002), Teenagers and Internet Safety, http://www.giac.org/paper/gsec/2081/teenagers-internet-safety/103566
270. Millward S., (2012), China's Forgotten 3rd Twitter Clone Hits 260 Million Users, http://www.techinasia.com/netease-weibo-260-million-users-numbers/
271. Milošević M., (2007), Aktuelni problemi suzbijanja kompjuterskog kriminala, Nauka, bezbednost, policija, 2007, vol. 12, br. 1, str. 57-74.
272. Ministry of Justice, (2014), Proven Re-offending Statistics Quarterly Bulletin July 2010 to June 2011, England and Wales, https://www.gov.uk/.../proven-reoffending-statistics-april-2011-march-2012
273. Mizrach S., Is there a Hacker Ethic for 90s Hackers?, http://www2.fiu.edu/~mizrachs/hackethic.html
274. Mobile Social Networking Audience Grew 44 Percent Over Past Year in EU5, (2011), http://www.comscore.com/Insights/Press_Releases/2011/11/Mobile_Social_Networking_Audience_Grew_44_Percent_Over_Past_Year_in_EU5
275. Mohamud A., (2012), Facebook: Around the World in 800 Days, http://www.comscore.com/Insights/Blog/Facebook_Around_the_World_in_800_Days
276. Montaldo C., (2011), Why Do Women Like True Crime Books? Why Are Women Drawn to the Gruesome Details?, http://crime.about.com/od/women/a/women_books.htm
277. Moore H.M., Trojanowicz C.R., (1988), Policing and the Fear of Crime, U.S. Department of Justice National Institute of Justice, Perspectives of Policing, no.3, pp.1-8
278. Morag N., (2013), Keyboard Criminals: How Cybercrime Has Grown Up and Diversified, http://www.coloradotech.edu/resources/blogs/october-2013/keyboard-criminals
279. Morcroft G., (2014), Markets/Finance Cyber Criminals Are Getting More Sophisticated, So Watch Out For These New Scams In 2014, http://www.ibtimes.com/cyber-criminals-are-getting-more-sophisticated-so-watch-out-these-new-scams-2014-1472504
280. Morcroft G.,(2014), Cyber Criminals Are Getting More Sophisticated, So Watch Out For These New Scams In 2014, http://www.ibtimes.com/cyber-criminals-are-getting-more-sophisticated-so-watch-out-these-new-scams-2014-1472504
281. Mukherjee W., (2007), Women taking to cyber crime in large nos, http://articles.economictimes.indiatimes.com/2007-06-23/news/28434010_1_cyber-crime-women-employees-mukund-pawar
282. Murphie A., Wilkins M., Measuring the effectiveness of prison sentences in England and Wales, http://www.justice.gouv.fr/art_pix/MurphieWilkins.pdf
283. Mussington D., (2007.), The Profileration Chalanges of Cyberspace, http://www.yorku.ca/yciss/publications/CyberspacePart2.pdf
284. Mwaita P., Owo M., (2013), Workshop Report on Effective Cybercrime Legislation in Eastern Africa Dar Es Salaam, Tanzania, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf

285. Namestnikov Y., (2012), The geography of cybercrime: Western Europe and North America, http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America?print_mode=1
286. Ndubueze N.P., Igbo M.U.E, Okoye O.U., (2013), Cyber Crime Victimization among Internet active Nigerians: An Analysis of Socio-Demographic Correlates, International Journal of Criminal Justice Sciences, Vol. 8 (2): 225–234, http://www.sascv.org/ijcjs/pdfs/philipetalijcjs2013vol8issue2.pdf
287. Ngafeeson M., (2010), Cybercrime Classification: A Motivational Model, http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf
288. Ngo T.F., Paternoster R., (2011), Cybercrime Victimization: An Examination of Individual and Situational Level Factors, International Journal of Cyber Criminology, Vol 5 Issue 1 January - July 2011, http://www.cybercrimejournal.com/ngo2011ijcc.pdf
289. Niveau G., (2010), Cyber-pedocriminality: Characteristics of a sample of internet child pornography offenders, http://www.drlynepiche.com/uploads/photos/pedo%20and%20internet.pdf
290. North A., (2007), Three In Ten Young People Victims Of Hacking, But Many Don't Care, http://jezebel.com/5847775/three-in-ten-young-people-victims-of-hacking-but-many-dont-care
291. Norton Cybercrime Report, (2012)&(2013), go.symantec.com/norton-report-2013
292. Nuccitelli M., (2012), iPredator-A Global Internet Predator Theorymoreby, http://www.academia.edu/1169441/iPredator-A_Global_Internet_Predator_Theory
293. Nykodym N., Taylor R., Vilela J., (2005), Criminal profiling and insider cyber crime. Computer Law and Security Report, 21:408–14
294. O'Leary M., (2009), Improving Mathematical Approaches to Geographic Profiling, http://pages.towson.edu/moleary/docs/Profiling/Report.pdf.
295. O'Connor T., (2014), Modus Operandi of Hacking, Mega Links in Criminal Justice. http://www.drtomoconnor.com/3100/3100lect04.htm
296. Ohm P., (2008), The Myth of the Superuser: Fear, Risk, and Harm *Online*, UC Davos Law Review, Vol. 41, No. 4, pp. 1327–1402, http://hein*online*.org/HOL/LandingPage?handle=hein.journals/davlr41&div= 36&id=&page=
297. Olson P., (2013), Teenagers say goodbye to Facebook and hello to messenger apps, http://www.theguardian.com/technology/2013/nov/10/teenagers-messenger-apps-facebook-exodus
298. OSCE, (2004), Decision No. 607 Combating Anti-Semitism
299. Overcoming the Fear of Cloud Computing, (2013), http://www.csc.com/cloud/publications/96289/96297-overcoming_the_fear_of_cloud_computing
300. Parker B.D., (1989), Computer Crime Criminal Justice Resource Manual, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf;
301. Parr M., Dagley J., Pogrund A., MacDonell L., (2012), Bullying: A Report from the Huntington Beach Human Relations Task Force, http://www.surfcity-hb.org/government/boards_commissions/pdf-files/2800-May-2012-Bullying-Report.pdf
302. Paulin J., Searle W., Knaggs T., (2003), Attitudes to Crime and Punishment: A New Zealand Study, http://www.rethinking.org.nz/assets/Newsletter_PDF/Truth_in_Justice/V2/Auckland_Uni_Attitudes_crime_punishment.pdf
303. Payne J., (2007), Recidivism in Australia: findings and future research, Australian Institute of Criminology, http://www.aic.gov.au
304. Pelemiš D., (1999), Prvi hakerski rat, http://www.sk.rs/1999/09/skin01.html
305. Percentage of global internet attack traffic during 3rd quarter 2013, by originating country, (2013), http://www.statista.com/statistics/276425/internet-attack-traffic-by-originating-country/
306. Perritt H.H., (1998), The Internet as a Threat to Sovereignty? Thoughts on the InternetsRole in Strengthening National and Global Governance, IT Chicago-Kent, College of Law, Illinois Institute of Technology, http://works.bepress.com/cgi/viewcontent.cgi?article=1030&context=henry_perritt
307. Personal Cloud Adoption: Steady March Towards One Billion Users by 2016, http://blog.tmcnet.com/thinking-out-cloud/2012/09/personal-cloud-adoption-steady-march-towards-one-billion-users-by-2016.html
308. Petee A.T., Corzine J., Corzine H.L., Clifford J., Weaver G., (2006), Defining "Cyber-Crime": Issues In Determining The Nature And Scope Of Computer-Related Offenses**,** http://futuresworkinggroup.cos.ucf.edu/docs/Volume%205/PeteeV5.pdf
309. Petrović N., Drakulić M., Vujin V., Drakulić R., Jeremić V., (2011), Climate changes and green information technologies, Management, no 59/2011, pp. 35–45.

310. Petrović S., (2012), Dilema: kiber ili sajber, Strani pravni život 2/2012., str 368 – 377, http://www.itvestak.org.rs/library/DILEMA%20KIBER%20ILI%20SAJBER.pdf
311. Petrović S.R. (2006), O neophodnosti nacionalne strategije zaštite kiber-prostora, Nauka, bezbednost, policija, vol. 11, br. 2, str. 3-28
312. Pfitzmann A., KöhntoppM., (2001), Striking a Balance between Cyber-Crime Prevention and Privacy, http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=40&ved=0CFkQFjAJOB4&url=http%3A%2F%2Fdud.inf.tu-dresden.de%2Fliteratur%2FStriking%2520a%2520Balance%2520betwee. doc &ei=fFb_UqSlNoWqyAPv5oCwBw&usg=AFQjCNEGx5ZI7nmzJUlVPZtPwbr8qg0Mng
313. Philippines, Analysis of the Cybercrime Prevention Act, (2012), http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final_.pdf
314. Pickett P., Cyber Threat Analyst - Career Profile, http://jobsearchtech.about.com/od/careertypes/p/Cyber_Threat_Analyst.htm
315. Poonia A.S., Dangayach G.S., Dr. Bhardwaj A., (2011), Technical management issues for resolving the cyber crime, 3rd International Conference on Information and Financial Engineering, IPEDR vol.12, http://www.ipedr.com/vol12/24-C026.pdf
316. Porteous H., Valiquet D., *(2011),* Cybersecurity and Cybercrime: Dealing with a Complex Threat, http://www.parl.gc.ca/content/lop/ researchpublications/cei-06-e.htm
317. Position Statement: Building the Gender Balance in the ICT Profession, (2013), http://www.cepis.org/index.jsp?n=1142&p=827
318. Powers S., (2013), The Threat of Cyberterrorism to Critical Infrastructure, http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/
319. Prasad K., (2012), Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act
320. Prasanna A., Cyber Crimes: Law And Practice, http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
321. Pritikin H.M., (2009), Is prison increasing crime?, Wisconsin Law Review, 1/5/2009, pp. 1050–1108, http://hosted.law.wisc.edu/lawreview/issues/2008_6/1_-_pritikin.pdf
322. Prlja D., Reljanović M., (2009), Visokotehnološki kriminal – uporedna iskustva, Strani pravni život, br. 3/2009.,str. 161 - 184;
323. Probation & Welfare Service, Assessing the Risk of Re-offending, http://www.probation.ie/pws/websitepublishing.nsf/attachmentsbytitle/Assessing+Risk+of+Re-offending/$file/Assessing+Risk+of+Re-offending.pdf
324. Putnam M.S., (2005), Cyber Ethics in a Real World, http://www.character-ethics.org/articles/cyberethics.htm
325. Radwan F., (2010), I wish i was attractive, http://www.2knowmyself.com/I_wish_i_was_attractive
326. Raine A., (2002), The Biological Basis of Crime, http://cooley.libarts.wsu.edu/soc3611/soc%20361%20summer% 202008/biologicalbasiscrime.pdf
327. Ramsland K., Women Who Kill: Part One, http://www.crimelibrary.com/notorious_murders/women/women1/1.html
328. Reljanović M., (2007), Visokotehnološki kriminal - pojam, regulativa, iskustva, Strani pravni život, br. 3, str. 75-98
329. Report – analysis "levels of cyber hate in Bulgaria, (2012), nohate.ext.coe.int/.../2012%20-%20REPORT%20-%20ANALYSIS%20„LEVELS%20OF%20CYBER%20HATE%...
330. Republic of the Philippines, (2012), An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes, http://www.gov.ph/2012/09/12/republic-act-no-10175/
331. Republic of the Philippines, (2013), An Act Requiring All Elementary And Secondary Schools To Adopt Policies To Prevent And Address The Acts Of Bullying In Their Institutions, http://www.gov.ph/2013/09/12/republic-act-no-10627/
332. Republika Srbija, Ministarstvo unutrašnjih poslova, (2009), Polazni okvir Nacionalne stretegije prevencije kriminala, http://www.bezbednost.org/upload/document/polazni_okvir_nacionalne_strategije.pdf
333. Republika Srpska vlada gender centar – centar za jednakost i ravnopravnost polova, (2013), Žene i informaciono-komunikacione tehnologije Dostupnost i mogućnosti u Republici Srpskoj, http://www.vladars.net/sr-SP-Cyrl/Vlada/centri/gendercentarrs/media/vijesti/Documents/216ene_i_IKT_FINAL).pdf

334. RESOLUTION 70, (Rev. Guadalajara 2010), Gender mainstreaming in ITU and promotion of gender equality and the empowerment of women through information and communication technologies, http://www.itu.int/ITU-D/sis/Gender/Documents/Resolution_70_2010.pdf
335. Ritter N., (2013), Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise, NIJ Journal / issue no. 271, February 2013, https://www.ncjrs.gov/pdffiles1/nij/240696.pdf
336. Robert W., Mikko S., (2009) Overcoming the insider: reducing employee crime through Situational Crime Prevention. Communications of the ACM, 52 (9)
337. Roberts L.D. Indermaur D., (2012), Are Neighbourhood Incivilities Associated with Fear of Crime?, ed. Australia: Identity, Fear and Governance in the 21st Century, http://press.anu.edu.au/apps/bookworm/view/Australia%3A+Identity%2C+Fear+and+Governance+in+the+21st+Century/10171/cover.html
338. Rosin H., (2014), When Men Are Raped, http://www.slate.com/articles/double_x/doublex/2014/04/male_rape_in_america_a_new_study_reveals_that_men_are_sexually_assaulted.html
339. Rossmo K., (2000), Place, space, and police investigations: hunting serial violent criminals, http://www.popcenter.org/library/crimeprevention/volume_04/10-Rossmo.pdf
340. Russian cyber crime market more organized, lucrative, (2012), SC Magazine, http://www.scmagazine.com/russian-cyber-crime-market-more-organized-lucrative/article/238100/
341. Rutherford A., (2014), 4,766 crimes against the elderly, but 96% of cases remain unsolved, Shocking statistics spark call for tougher sentences, http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/4766-crimes-against-the-elderly-but-96-of-cases-remain-unsolved-30063796.html
342. Ruyver B., Vermeulen G., Beken T., (2013), Strategies of the EU and the US in Combating Transnational Organized Crime, http://books.google.rs/books?id=094gPcnKQAwC&pg=PA208&lpg=PA208&dq=cyber+transnational+organized+crime+cooperation&source=bl&ots=ohum9m2gbt&sig=oMmUy6MzJJxW6JTS3yKkx1lcNIo&hl=sr&sa=X&ei=fDVGU6LNNobIsgapi4H4Bw&ved=0CFYQ6AEwCQ#v=onepage&q=cyber%20transnational%20organized%20crime%20cooperation&f=false
343. Safety & Security Guide, http://cybercrime.org.za/definition;
344. Saini H., Rao Y.S., Panda T.C., (2012), Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209, www.ijera.com, Vol. 2, Issue 2, pp.202-20;
345. Salimi E., (2013), Cyber Criminology: investigating the characteristics of internet crimes and criminals, International Journal of Law in the New Century, November 2013, Vol. 1(1), www.lawjournal.ir
346. Sands L., (1998), Moral Panics, http://www.aber.ac.uk/media/Students/lcs9603.html
347. Saran C., (2012), Fear of cyber crime stops EU citizens doing business on the web, http://www.computerweekly.com/news/2240159331/European-citizens-afraid-of-*online*-crime
348. Scarborough K.B., Like-Haislip Z.T., Novak J.K., Lucas L.W., Alarid F.L., (2010), Assessing the relationship between individual characteristics, neighborhood context, and fear of crime, Journal of Criminal Justice, no. 38, pp. 819–826
349. Schneier B., (2014), Cyberwar: Myth or Reality?, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=315:cyberwar-myth-or-reality&catid=50:issue-7&Itemid=187
350. Secretary General of the Council of Europe, (2008), Internet - a critical resource for all, http://www.coe.int/t/informationsociety/documents/SG-Inf(2008)14_en.pdf
351. Sembok T.M.T., (2003), Ethics Of Information Communication Technology (ICT), http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF
352. Senate of the United States, S. 2111 (112th): Cyber Crime Protection Security Act, https://www.govtrack.us/congress/bills/112/ s2111/text
353. Serrano A.S., (2006), Internet Regulation: A Hard-Law Proposal, www.JeanMonnetProgram.org
354. Serrano A.S., Internet Regulation and the Role of International Law, http://www.mpil.de/shared/data/pdf/pdfmpunyb/06_antoniov.pdf
355. Shackelford J.S., (2009.), From nuclear war to net war: analogizing cyber attacks in international law, http://www.grocjusz.edu.pl/Materials/_archiwum/archiwum2009/pd_sem_2611_B.pdf

356. Shaw D.E., (2006), The role of behavioral research and profiling in malicious cyber insider investigations, hftp://163.13.200.222/Prof_Liang/%BC%C6%A6%EC%C5%B2%C3%D1/Volume%203%20(2006)/Issue%201/Pages%2020-31.pdf
357. Sheng S., Holbrook M., Kumaraguru P., Cranor L., Downs J., (2010), Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interve, http://lorrie.cranor.org/pubs/pap1162-sheng.pdf
358. Shinder L.D., Tittel E., (2002), Cybercrime Scene of the Computer Forensics Handbook, Rockland, Syngress Publishing, Inc.
359. Siderman M.L., (2013), Pathways to Cyber Bullying from Bystander to Participant: Secondary School Students' Perspectives, http://www.cybersmile.org/resources/155/Pathways-to-Cyber-Bullying-from-Bystander-to-Participant_-Seconda.pdf
360. Sieber U., (1998), Legal Aspects of Computer-Related Crime in Information Society – comcrime study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf
361. Simion R., (2010), Cybercrime and its challenges between reality and fiction. Where do we actually stand?, http://www.vittimologia.it/rivista/articolo_simion_2009-03_2010-01.pdf
362. Simon Wiesenthal Center, (2009), Facebook, Youtube+: How Social Media Outlets Impact Digital Terrorism and Hate, http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=lsKWLbPJLnF&b=4441467&ct=7131713
363. Singapore to legislate against cyber bullies, (2014), http://www.out-law.com/articles/2014/march/singapore-to-legislate-against-cyber-bullies/
364. Sinrod J.E., Reilly P.W., (2000), Cyber-crimes: a practical approach то тне application of federal computer crime laws, www.sinrodlaw.com/cybercrime.doc
365. Sjouwerman S., (2014), FBI: The 10 Criminal Cyber Crime Professions, http://community.spiceworks.com/topic/440511-fbi-the-10-criminal-cyber-crime-professions
366. Small P.E., (2012), Defense in Depth: An Impractical Strategy for a Cyber World, SANS Institute, http://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world- 33896
367. Smith K., Lader D., Hoare J., Lau I., (2012), Hate crime, cyber security and the experience of crime among children: Findings from the 2010/11 British Crime Survey, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116463/hosb0612.pdf
368. Social Networking Statistics, http://www.statisticbrain.com/social-networking-statistics/
369. Social, Digital & Mobile Around The World, (2014), http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014
370. Sofaer D.A., Goodman E.S., (2000), Proposal for an International Convention on Cyber Crime and Terrorism, A CISAC Report, http://fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a/
371. Sofaer D.A., Goodman E.S., Cuéllar F.M., Drozdova A.E., Elliott D.D., Grove D.G., Lukasik J.S., Putnam L.T., Wilson D.G., (2000), A Proposal for an International Convention on Cyber Crime and Terrorism, http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf
372. Sollfrank C., (1999), Women Hackers, http://www.obn.org/hackers/text1.htm;
373. Solomon J., (2010), Hate speech infiltrates social-networking sites, report says, http://edition.cnn.com/2010/TECH/03/15/hate.speech.social.networks/
374. Sprondel J.T., Breyer T., Wehrle M., (2011), Cyberanthropology - Being Human on the Internet, 1st Berlin Symposium on Internet and Society: Exploring the Digital Future, Berlin, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1943399
375. Srivastava A., (2014), 2 Billion Smartphone Users By 2015 : 83% of Internet Usage From Mobiles [Study], http://www.dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017/#ixzz2rcbChM tk
376. Srpski školarac na internetu-zabrinajvajuće brojke!, (2013), http://bezbedannet.wordpress.com/2013/05/22/srpski-skolarac-na-internetu-zabrinajvajuce-brojke/
377. Standing Senate Committee on Human Rights, (2012), Cyberbullying Hurts: Respect for Rights in the Digital Age, http://www.parl.gc.ca/Content/SEN/Committee/411/ridr/rep/rep09dec12-e.pdf

378. Statham H., (2012), The experiences of gay young people in Britain's schools in 2012, http://www.stonewall.org.uk/documents/school_report_2012(2).pdf
379. Statistic Brain, (2014), Social Networking Statistics, http://www.statisticbrain.com/social-networking-statistics/
380. Statistics on bullying, (2013), http://www.nspcc.org.uk/Inform/resourcesforprofessionals/bullying/bullying_statistics_wda85732.html
381. Steele H., (2010), 25% Recidivism Rate – Really? http://innocentjustice.org/2010/25-recidivism-rate-%E2%80%93-really/
382. Stewart B.E., (2008), School Structural Characteristics, Student Effort, Peer Associations, and Parental Involvement, The Influence of School- and Individual-Level Factors on Academic Achievement, http://olms.cte.jhu.edu/olms/data/resource/3890/School%20Structural%20Characteristics.pdf
383. Stiennon R., (2012), UP and to the RIGHT: Strategy and Tactics of Analyst Influence: A complete guide to analyst influence, IT-Harvest Press, Birmingham
384. Stojičević D., (1998), Želite li američki pasoš?, Svet kompjutera, 12/1998., http://www.sk.rs/1998/12/skin06.html
385. Stojičević D., (2003), Nullum crimen nulla poena sine lege, Svet kompjutera, br. 3/2003
386. Stojičević D., (2003), Sve sudije da sude po zakoniku, Svet kompjutera, br. 5/2003, http://www.sk.rs/2003/05/skin05.html
387. Strategija sajber bezbjednosti Crne Gore 2013–2017, http://www.gsv.gov.me/biblioteka/strategije?query =sajber%20bezbjednost&sortDirection=desc
388. Stuart H., (2003), On the Effectiveness of Prison as Punishment, http://www.is.wayne.edu/StuartHenry/Effectiveness_of_Punishment.htm
389. Study surveyed a random sample of 4441 youth between the ages of 10 and 18 from a large school district, Summary of our cyberbullying research from 2004-2010, (2010), http://www.cyberbullying.us/research.php
390. Sukhai B.N., (2004), Hacking And Cybercrime, http://jjc*online*.net/PAD_750/Readings/Class8/Hacking_And_Cybercrime.pdf; Australian High TechCrime Centre Hacking Motives, (2005/2006), http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb 006.pdf
391. Sukhai B.N.,(2005), Hacking And Cybercrime, http://jjc*online*.net/PAD_750/Readings/Class8/Hacking_ And_Cybercrime.pdf
392. Sumo3000, (2012), Top 20 Countries Found to Have the Most Cybercrime, http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
393. *Svete U., Kolak A., Varnostna relevantnost kibernetskega prostora v obdobju web 2.0,* http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/vojaski_izzivi/ svi_13_3.pdf
394. Symantec, (2013), Internet security Threat Report 2013: Trends, Volume 18, Published, April 2013, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_ 21291018.en-us.pdf
395. Škrtic D., (2009), Implementacija odredbi Konvencije o kibernetickom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo, http://www.fvv.uni-mb.si/dv2009/Zbornik/clanki/skrtic.pdf
396. Škulić M., (2010), Starosna granica sposobnosti za snošenje krivice u krivičnopravnom smislu, http://www.ius.bg.ac.rs/crimenjournal/articles/Crimen%20002-2010%20_%203%20Skulic.pdf
397. Šugman K., (2006), Slovenija i njezino približavanje eu na području policijske i sudske suradnje**,** www.hrcak.srce.hr/file/130332
398. Taipale K.A., (2009), Unit 01: Overview, What is Cybercrime?, http://www.information-retrieval.info/cybercrime/index01.html
399. Tanilir M.N., Tahirović M., (2013), Međunarodna bezbjednost i sajber opasnosti**,** Monet, Institut za strateške studije i projekcije (ISSP), Edicija Bezbjednost, Volume 4, стр. 8 – 26, http://issp.me/wp-content/uploads/2012/10/monet34se.pdf
400. Teachman J., (2008), Military service and the life course: An assessment of what we know, http://www.ncfr.org/ncfr-report/focus/military-families/military-service-life-course-assessment
401. Team Cymru, (2006), Cybercrime—An Epidemic Can we protect ourselves from the hazards of an *online* world, http://queue.acm.org/detail.cfm?id=1180190

402. The Belgian Cybercrime Centre of Excellence for Training, Research and Education, (2012), Cybercrime: modern crime, modern methods, http://www.kuleuven.be/english/news/cybercrime.html
403. The Commission on Crime Prevention and Criminal Justice Resolution 22/7 Strengthening international cooperation to combat cybercrime, (2013), http://www.unodc.org/documents/commissions/CCPCJ_session22/Resolutionsweb/Resolution_22.7.pdf
404. The Computer Crime Act, (1997), http://cyberlawforyou.blogspot.com/2012/09/cyber-crime-laws-in-malaysia.html
405. The Current State of Cybercrime 2013, An Inside Look at the Changing Threat Landscape, (2013), http://www.emc.com/collate
406. The cyber-crime professions, (2011), http://cybercrime.pandasecurity.com/blackmarket/cybercrime_professions.php
407. The geography of cybercrime: Western Europe and North America, (2013), http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America
408. The Hoover Institution,The Consortium for Research on Information Security and Policy (CRISP), The Center for International Security and Cooperation (CISAC), (2000), Stanford University: A Proposal for an International Convention on Cyber Crime and Terrorism http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm
409. The Internet Crime Complaint Center (IC3), (2012), 2012 Internet Crime Report, http://www.ic3.gov/media/ annualreport/2012_IC3Report.pdf
410. The Nizkor Project, (2012), The Skinhead International: Canada, http://www.nizkor.org/hweb/orgs/american/adl/skinhead-international/skins-canada.html
411. The Pew Center on the States, (2011), State of Recidivism, The Revolving Door of America's Prisons, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/sentencing_and_corrections/State_Recidivism_Revolving_Door_America_Prisons%20.pdf
412. The World in 2013 ICT Facts and Figures, (2013), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf
413. Thomas D., Loader B., (2000), Cybercrime: law enforcement, security and surveillance at the information age, London, Routledge;
414. Tiku N., (2012), Paul Graham Says Women "Haven't Been Hacking For the Past 10 Years", http://valleywag.gawker.com/paul-graham-says-women-havent-been-hacking-for-the-pa-1490581236
415. Tiwari A., (2014), Operating System Usage Trend September – December 2013: Smartphone Operating Systems Are Driving Growth!, http://www.dazeinfo.com/2014/01/24/operating-system-usage-trend-2013-smartphone-growth/
416. Tompsett C.B., Marshall M.A., Semmens C.N., (2005), Cyberprofiling: Offender Profiling and Geographic Profiling of Crime on the Internet, http://www2.hull.ac.uk/science/pdf/CyberProfilingIEEE.pdf
417. Tropina T., (2014), Cyber Crime and Organized Crime, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=305:cyber-crime-and-organized-crime&catid=50:issue-7&Itemid=187
418. Tulloch M., (1998), Quantitative Review, едиција Fear of Crime, volume 1, www.ncavac.gov.au
419. Turvey E.B., (2011), Modus operandi, Motive and Technology, in edition, Digital Evidence and Computer Crime, Forensics Science, Computers and Internet, Amsterdam, Elsevir
420. Tyler T., (2001), Is the Internet Changing Social Life? More Things Change, The more Stay The Same, www.researchgate.net/...Social.../e0b49521e1b3a6787a.pdf
421. U.S. Attorney's Office, Central District of California, (2013), Glendale Man Who Admitted Hacking into Hundreds of Computers in Sextortion Case Sentenced to Five Years in Federal Prison, http://www.fbi.gov/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison
422. U.S. Attorney's Office, Public Affairs Specialist Laura Eimiller, (2013), Temecula Student Arrested in Sextortion Case Involving Multiple Victims, http://www.fbi.gov/losangeles/press-releases/2013/temecula-student-arrested-in-sextortion-case-involving-multiple-victims
423. UK Government, (2012), Governments are Prime Targets for Cybercrime, White Paper, http://secunia.com/?action=fetch&filename=governments-are-prime-targets-for-cybercrime.pdf

424. UN Economic and Social Council Commission on Crime Prevention and Criminal Justice, (2013), International cooperation in combating transnational organized crime and corruption Report of the Secretary-General, http://www.coe.int/t/dghl/standardsetting/CDPC/PC-GR-COT/ECN.15_2013_4.pdf
425. UNICEF Canada, (2012), Bullying And Cyberbullying: Two Sides of the Same Coin, Brief submitted by UNICEF Canada to the Standing Senate Committee on Human Rights, http://www.unicef.ca/sites/default/files/imce_uploads/TAKE%20ACTION/ADVOCATE/DOCS/cyberbullying_submission_to_senate_committee.pdf
426. UNICRI, Cybercrime and Organized Crime, http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/organized_crime/
427. UNICRI, International Crime Victims Survey, http://www.unicri.it/services/library_documentation/publications/icvs/
428. United Nations Convention against Transnational Organized Crime and the Protocols Thereto, (2000), http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf;
429. United Nations Office on Drugs and Crime, (2010), The globalization of crime a transnational organized crime threat assessment, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_ 2010_low_res.pdf
430. United Nations Office on Drugs and Crime, (2013), Comprehensive Study on Cybercrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf;
431. United Nations, (1969), International Convention on the Elimination of All Forms of Racial Discrimination, General Assembly resolution 2106 (XX) of 21 December 1965, entry into force 4 January 1969, in accordance with Article 19, http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/218/69/IMG/NR021869.pdf?OpenElement
432. United Nations, (1981), Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, Report of Committee II, Workshop on crimes related to the computer network & Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, http://www.uncjin.org/Documents/10thcongress/10cDocumentation/10cdocumentation.html
433. United Nations, (2009), 2009 Unlearning Intolerance Seminar Cyber Hate: Danger in Cyber Space, http://www.un.int/wcm/content/site/ui/
434. United Nations, (2010), Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime on its fifth session, http://www.unodc.org/documents/treaties/organized_crime/COP5/CTOC_COP_2010_17/CTOC_COP_2010_17_E.pdf
435. United Nations, (2010), Twelfth United Nations Congress on Crime Prevention and Criminal Justice Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, http://www.unodc.org/documents/crime-congress/ 12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf
436. United Nations, (2014), UN Action to Counter Terrorism, International Legal Instruments. http://www.un.org/terrorism/
437. United States Action Yahoo Group, (2000), List of Active US Hate Groups as of 2000, (Alphabetical List of Groups by USA State), (research from Southern Law Poverty Center Intelligence Report), http://www.unitedstatesaction.com/list-us-hate-groups.htm
438. UNODC, (2013), Comporehensive Study on Computercrime, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
439. Van Blarcum C.D. (2005), Internet Hate Speech: The European Framework and the Emerging American Haven, http://law.wlu.edu/deptimages/Law%20Review/62-2VanBlarcum.pdf
440. Vanstone A., (2014), Should hate speech be allowed?, http://www.abc.net.au/radionational/programs/counterpoint/should-hate-speech-be-allowed3f/4816546
441. Veenstra S., Stol W., Leukfeldt R., (2013), High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands, International Journal of Cyber

Criminology, Vol 7 Issue 1 January - June 2013., 2013 International Journal of Cyber Criminology. January – June 2013, Vol 7 (1)
442. Vestbi R.Dž., (2004), Međunarodni vodič za borbu protiv kompjuterskog kriminala, Američka advokatska komora, Komitet za zaštitu privatnosti i borbu protiv kompjuterskog kriminala, Odeljenje za naučno i tehnološko pravo, Beograd
443. Vijayashankar H., (2013), Modus Operandi of a Phishing Fraud, http://www.naavi.org/wp/?p=1072;
444. Vogel J., (2007), Towards a Global Convention against Cybercrime, First World Conference of Penal Law. Penal Law IN THE XXIst century. Guadalajara (Mexico), 18-23 November 2007, http://www.penal.org/IMG/Guadalajara-Vogel.pdf
445. Vojković G., Štambuk-Sunjić M., (2006), Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split.
446. Vukotić M., Đolović A., Koprivica I., (2011), Analiza podataka centara za socijalni rad o slučajevima seksualnog zlostavljanja i zloupotrebe dece u AP Vojvodini za period 2006-2010. godina, http://www.pzsz.gov.rs/multimedia/dodaci/ Pandorina_kutija_2011.pdf
447. Vuković H., (2012), Kibernetska sigurnsot i sustev borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, www.*hrcak.srce.hr/file/ /148443*
448. Walker B.M., (2010), FBI's Chabinsky: Cybercrime is a profession, http://www.fiercegovernmentit.com/story/chabinsky-cybercrime-should-be-top-priority-all-agencies-not-just-fbi/2010-03-24
449. Walker R., (2013), Four tips for mitigating risk of cyber crime, Data loss doesn't just happen, http://www.sas.com/knowledge-exchange/risk/fraud-financial-crimes/four-tips-for-mitigating-risk-of-cyber-crime
450. Wall D.S., (2005), The Internet as a Conduit for Criminals', in Pattavina A. (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage
451. Wall D.S., (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press
452. Wall D.S., (2008/11), Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime (revised Feb. 2011)', Information, Communication & Society (11): 861–884., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155
453. Wall D.S., (2008a), Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime, Information, Communication & Society, Vol. 11, No. 6, pp. 861-884, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155
454. Wall D.S., (2008b), Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime, International Review of Law, Computers & Technology, 22:1-2, 45-63, http://dx.doi.org/10.1080/13600860801924907
455. Warren E., (2011), Legal, Ethical and Professional Issues in Information Security, http://www.cengage.com/resource_uploads/downloads/1111138214_259148.pdf
456. Wattanajantra A., (2011), Cloud security will turn cyber criminals professional, http://www.theinquirer.net/inquirer/news/2079931/cloud-security-cyber-criminals-professional
457. Weisheit R.A., Wells L.E., Falcone D.N., (1995), Crime and Policing in Rural and Small-Town America: An Overview of the Issues, https://www.ncjrs.gov/txtfiles/crimepol.txt
458. Weston P., (2002), Sabotage, WVP, http://www.stpubtraining.com/images/Documents/SABOTAGE.pdf;
459. Williams C.J., (2010), Court tightens definition of cyber-bullying, Appellate panel rules 2 to 1 that hostile comments left on a Harvard-Westlake School student's website aren't protected by the 1st Amendment, http://articles.latimes.com/2010/mar/18/local/la-me-cyber-speech18-2010mar18
460. Wilson C., (2008), Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, http://www.dtic.mil/dtic/tr/fulltext/u2/a477642.pdf
461. Wilson J., Kelling G., (1982), Broken windows: Atlantic Monthly, no.211, 29–38
462. Wolak J., Finkelhor D., Mitchell J.K., Ybarra L. M., (2008), *Online* "Predators" and Their Victims, Myths, Realities, and Implications for Prevention and Treatment, American Psychologist, Vol. 63, No. 2, 111–128, pp. 111 - 128., http://www.apa.org/pubs/journals/releases/amp-632111.pdf
463. Wolfe L., (2012), Eight reasons why victim-blaming needs to stop: Writers, activists, and survivors speak out, http://www.womenundersiegeproject.org/blog/entry/eight-reasons-why-victim-blaming-needs-to-stop-writers-activists-and-surviv
464. Wolfgang E.M., Figlio M.R., Sellin T., (1972), Delinquency in a Birth Cohort, University of Chicago Press, Chicago

465. Woollaston V., (2014), Formula for the perfect HACK: Scientists create mathematical model to understand how cybercriminals know when to strike, http://www.my-rss.co.uk/feeditem.php?feed=0&word=&search=&item=252610;
466. World: Europe Nato to strike Yugoslavia (1999), http://news.bbc.co.uk/2/hi/ europe/302265.stm
467. Worth D., (2013), Lack of women in ICT sector costs Europe €9bn a year, http://www.v3.co.uk/v3-uk/news/2298528/lack-of-women-in-ict-sector-costs-europe-eur9bn-a-year
468. Wynne T., (2008), An Investigation into the Fear of Crime: Is there a Link between the Fear of Crime and the Likelihood of Victimisation?, http://www. internetjournalofcriminology.com/Wynne%20-%20Fear%20of%20Crime.pdf
469. Yang Z., (2011), A Survey of Cybercrime, http://www1.cse.wustl.edu/~jain/cse571-11/ftp/crime.pdf
470. Yar M., (2005), The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory, Journal of Contemporary Criminal Justice November, pp. 407-427., http://wenku.baidu.com/view/7855fafe700abb68a982fb5f.html
471. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Službeni glasnik RS, br. 61/2005;
472. Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, (2002), http://narodne-novine.nn.hr/clanci/medunarodni/327873.html
473. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS, br. 19/2009.
474. Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih /MKKKDP/Ur.l. RS-MP, št. 17/2004. http://www.uradni-list.si/1/objava.jsp?urlmpid=200468
475. Ziegler J.C., Muneaux M., (2007), Orthographic facilitation and phonological inhibition in spoken word recognition: A developmental study, http://gsite.univ-provence.fr/gsite/Local/lpc/dir/ziegler/article/ Ziegler_Muneaux_PBR_07.pdf
476. Аутономна Покрајина Војводина, http://www.vojvodina.gov.rs/sr,
477. Бановић Б., (2003), Компјутерски криминалитет и заштита личности, Безбедност 1/2003, стр. 16 – 43
478. Влада Републике Србије, (2012), Стопа незапослености, http://www.srbija.gov.rs/vesti/vest.php?id=182379
479. Водинелић В., (1990), Методика откривања, разјашњавања и доказивања рачунарског криминалитета, Приручник 4/90, МУП Хрватске
480. Вулетић Д., (2011), Одбрана и претње у сајбер простору, http://www.isi.mod.gov.rs/pdf/publikacije/1328179353_Odbrana%20od%20pretnji%20u%20sajber%20prostoru%20-%20za%20sajt.pdf
481. Ђурић С., Поповић-Ћитић Б., (2013), Страх од криминала, родне разлике у перцепцији ризика, Социолошки преглед, vol. XLVII (2013), no. 4, стр. 537–554
482. Закон о војсци, Службени гласник РС, бр. 116/07 и 28/09
483. Закон о изменама и допунама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр. 42 /02, 27/03, 39 /03, 67 /03, 29/04, 45/05, 72/09, 32/13
484. Закон о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013
485. Закон о одговорности правних лица за кривична дела, Сужбени. гласник РС, бр. 97/2008
486. Закон о полицији, Службени гласник РС, бр. 101/2005, 63/2009
487. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013)
488. Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, Службени гласник РС, број 19/09.
489. Закон о потврђивању Европске конвенције о сузбијању тероризма, Службеном листу СРЈ – „Међународни уговори", бр. 10/2001.
490. Закон о спречавању прања новца и финансирању тероризма, Службени гласник РС, бр, 20/2009, 72/2009, 91/2010.
491. Законик о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013.

492. Ивановић З., Бановић Б., (2010), Мобилне социјалне мреже – нови ризик високотехнолошког криминала, у: Злоупотреба информационих технологија и заштита – зборник радова ЗИТЕХ 10., *www.singipedia.com/attachment.php? attachmentid*
493. Игњатовић Ђ., (1991), Појмовно одређење компјутерског криминалитета, Анали Правног факултета у Београду, бр.1-3/91
494. Јовашевић Д., (2002), Институт саучесништва у кривичном праву, Право – теорија и пракса, вол. 19, бр. 11, стр. 14-26.
495. Конвенција за компјутерски криминал, Република Македонија, Група на држави за борба против корупцијата, http://old.soros.org.mk/dokumenti/Makedonija&Greko.pdf
496. Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013
497. Крушчић М., (1986), Искуства ГСУП-а Београд у откривању нових појавних облика кривичних дела из области привредног криминалитета у пословним банкама, Безбедност, бр. 2/86
498. Митровић М. Д., Трајковић С.М., (2011), Може ли виртуелни лик да буде субјект права?, http://anali.ius.bg.ac.rs/A2011-2/Anali%202011-2%20str.%20028-042.pdf
499. Младеновић Д., (2013), Међународни аспект сајбер ратовања, Београд, Одбрана
500. МУП Републике Србије, (2014), Информатор о раду Министарства унутрашњих послова Републике Србије, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/informator
501. Настић Д., (2012), Профил сајбер криминалаца у Србији, мастер рад, Београд, ФОН
502. Odluka o ratifikaciji Konvencije o kibernetičkom kriminalu, http://www.fup.gov.ba/wp-content/uploads/ 2012/01/Konvencija-o-cyber-kriminalu-Budimpesta.pdf
503. Попадић Д., (2009), Насиље у школи, Институт за психологију, УНИЦЕФ; www.unicef.rs/files/nasilje-u-skolama-za-web.pdf
504. Правилник о Протоколу поступања у установи у одговору на насиље, злостављање и занемаривање, Службени гласник РС, бр. 30/2010, http://www.paragraf.rs/propisi/pravilnik_o_protokolu_postupanja_u_ustanovi.html
505. Пројекције становништва Републике Србије, 2011–2041., http://webrzs.stat.gov.rs/WebSite/public/PublicationView.aspx?pKey=41&pLevel=1&pubType=2&pubKey=2208
506. Путник Н., (2009), Сајбер простор и безбедносни изазови, Београд, Универзитет у Београду, Факултет за безбедност
507. Раденковић Б., (2009), Интернет, два пута међу Србима, http://www.politika.rs/rubrike/Drustvo/Internet-dva-puta-medju-Srbima.sr.html
508. Ратификувана во Советот на европа на 15 септември 2004. година (Објавена во „Службен весник на РМ" бр. 41/2004)
509. Република Србија, Републички завод за статистику, (2013), Демографска статистика 2012, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=164
510. Република Србија, Републички завод за статистику, (2013), Пунолетни учиниоци кривичних дела у Републици Србији, 2012. – Пријаве, оптужења и осуде, http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/24/91/SB_576_Punoletni_uciniociKD2012.pdf
511. Република Србија, Републички завод за статистику, (2014), Актуелни показатељи Република Србија, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2#fusnota
512. Урошевић В., Уљанов С., Вуковић Р., (2010), Полиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије
513. Цветковић С., (2009), Прилог проучавању амнестија и аболиција политичких осуђеника у Југославији 1944–1980., Архив, часопис Архива Југославије, 1–2, 2009., стр. 120–132, www.arhivyu.gov.rs/index.php?download
514. Шкулић М., (1997), Компјутерски криминалитет: Да ли смо беспомоћни пред овом опасношћу, Југословенски часопис за правну информатику, Компјутери и право, Вол. 5, број 2, Београд, стр. 43-61

др Владимир Урошевић, Министарство унутрашњих послова РС,
УКП СБПОК, Одељење за борбу против ВТК
научни сарадник Института за упоредно право

доц. др Звонимир Ивановић, КПУ КПА
Криминалистичко–полицијски универзитет
Криминалистичко–полицијска академија

КРИВИЧНОПРАВНИ АСПЕКТИ CYBER КРИМИНАЛА

Садржај

Графици

Табеле

1. УВОД

Иако је Србија ратификовала одређене конвенције Савета Европе, не постоји потпуно адекватна законско-техничка конструкција која покрива целокупну проблематику високотехнолошког криминала (ВТК), а у вези са ИКТ. Као што се може закључити из прегледа правних аката који се односе на питање ВТК, постоје многи секундарни правни акти који регулишу материју одговарајући у малим детаљима. Ова ситуација, ипак, није одговарајућа у погледу обавеза појединих министарстава и владиних агенција, који су дужни да спроводе све прописе у овој области и старају се о њиховој примени. Да би то потпуније приказали и објаснили можемо указати на правни партикуларитет српског правног система који додатно доприноси стварању проблема за све оне у обавези да спроводе и примењују правне норме.

Поред утицаја препорука и конвенција из ОЕБС-а у правном систему Србије није била покривена област високотехнолошког криминала и ИКТ све до ступања на снагу Кривичног законика РС (2006), а као израз обавезе потписивања и ратификовања (истина тек 2009) ЦЕТС-а 185. Иако је Државна заједница Србије и Црне Горе потписала Конвенцију о високотехнолошком криминалу Савета Европе (ЦЕТС 185) 2005. године, законодавство Републике Србије не покрива област високотехнолошког криминала до следеће 2006. године, када је само делимично покривена Кривичним закоником (КЗ, ступио на снагу 1.1.2006. године, објављен у Службеном гласнику РС бр. 85/2005, 88/2005, 107/2005) у складу са обавезама које се односе на Конвенцију. Од тог тренутка се правни систем Републике Србије модификовао врло често, од којих су неке измене биле веома темељне. Томе је, такође, допринела улога радне групе у оквиру хармонизације у примени прописа ЦЕТС 185 и 189[724], као део Cybercrime@IPA SEE пројекта[725].

1.1 Организациони и процедурални аспекти

Године 2008. Министарство унутрашњих послова (МУП) је основало у оквиру Службе за борбу против организованог криминала (СБПОК) Посебно одељење за борбу против високотехнолошког криминала, као форму испуњења законских обавеза. Ово одељење се састоји од два одсека - Одсека за борбу против електронског криминала и Одсека за сузбијање криминала против интелектуалне својине (кршење ауторских права и фалсификовање). Ова јединица се сматра српском јединицом за борбу против високотехнолошког (cybercrime) криминала (ХТЦУ). Одељење у СБПОК-у има надлежност у поступању и примени мера и радњи у оквирима предистражног поступка за кривична дела из области високотехнолошког криминала, а према Закону о организацији и надлежности државних органа у борби против ВТК и у случајевима где се рачунари и рачунарске мреже појављују као средство извршења кривичних дела. МУП је овлашћен и дужан да спроводи мере и

724 Uljanov, S. Urošević, V. Ivanović, Z. Visokotehnološki kriminal iz ugla međunarodne saradnje kriminalističke policije, str.530-541. Zbornik radova Konferencije Internacionalne asocijacije kriminalista, Međunarodna i nacionalna saradnja i koordinacija u suprostavljanju kriminalitetu, na Kelebiji, Banjaluka 2010. Vol. 3. Br.1;

725http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_reports_en.asp последњи пут приступљено 17.2.2014.год;

радње у склопу предистражног поступка (под вођством јавног тужиоца) за кривична дела која се односе на дистрибуцију одређеног, илегалног, садржаја на интернету и кривична дела који укључују повреде права интелектуалне својине. Ова надлежност је утврђена законом о организацији и надлежности државних органа у борби против високотехнолошког криминала Службени гласник РС бр. 61/2005 и 104/09. Јединица за борбу против високотехнолошког криминала је надлежна за спровођење предистражног поступка у вези кривичних дела против рачунарских система, мрежа и као и свих кривичних дела која укључују технологију. Прикупљање и анализу трагова у електронском облику као и дигиталну форензику не спроводи ХТЦУ већ је поверена посебном одсеку у оквиру Министарства унутрашњих послова, служби за специјалне истражне мере (ССИМ).

Сарадња ХТЦУ са специјалистима из других земаља је организована путем директне комуникације официр - официр, као и кроз разне међународне полицијске организације, као што су Европол, СЕЛЕК, Интерпол И24/7 мреже[726] и путем И24/7 сталне контакт-тачке успостављене ЦЕТС 185[727].

У оквиру јавног тужилаштва, у надлежност вишег јавног тужиоца уведена је 2005. године законом (први пут је представљен 25.7.2005.), који даје посебну надлежност у случајевима кривичних дела ВТК и уједно одређује шта спада у ову област. Тужилац према начину доношења, обиму обухватности, техници и архитектури овог законског прописа има статус тужиоца (канцеларије) посебне надлежности, а у исто време тим законом утврђена је судска надлежност (тада Окружног) Вишег суда у Београду посебног већа тог суда.

Изменама Кривичног законика (КЗ) у августу (31.) 2009. године законски систем Србије је више усклађен са ЦЕТС-ом 185 и 189, али не у потпуности.

2. ПРОМЕНЕ У ЈУРИСДИКЦИЈАМА

Промена Закона о организацији и надлежности државних органа у борби против високотехнолошког криминала, од 11.12.2009.године, наводи се у члану бр. 3. Овај закон примењује се ради откривања, кривичног гоњења и суђења за:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником;
2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара;
3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2 став 1 овог закона.

726 Đukanović, D. Ivanović, Z. Uljanov, S: Oblici međunarodne policijske saradnje u uslovima tranzicije na zapadnom Balkanu Serbian law in transition: changes and challenges, Belgrade Institute of comparative law;

727 Yrošević, V. Ivanović, Z. Yljanov, S. Mač u www – u: Izazovi VTK, Beograd: Eternal mix, 2012;

Описане промене су ишле ка томе да се повећа број појединачних копија заштићеног материјала (нови закон је ажуриран бројно на 2000 са 500 примерака и износ материјалне штете нанете на 1000000 са 850000 динара). Јурисдикција је додатно проширена у трећем ставу овог члана допуњавањем надлежности над другим кривичним делима.

2.1 Измене - у организационом смислу

Према новим изменама посебно тужилаштво надлежно за ВТК остаје (Посебно одељење за борбу против високотехнолошког криминала), као такво, али се налази у оквиру Вишег јавног тужилаштва у Београду, што је представљало облик умањења надлежности. Републички јавни тужилац именује специјалног тужиоца за ВТК, из реда јавних тужилаца и заменика јавних тужилаца, који испуњавају услов за избор за заменика вишег јавног тужиоца, додатно условљено писменом сагласношћу лица које се поставља.

Одељење Вишег суда у Београду има стварну и месну надлежност, а не Веће, као што је било предвиђено пре измена. У пракси не постоје сталне судије опредељене ка том одељењу, они се постављају од стране председника Вишег суда кроз распоред рада. Тренутно у оквиру Вишег јавног тужилаштва у Београду ради Посебно одељење за борбу против високотехнолошког криминала, надлежно за целу територију Републике Србије, у оквиру којих делују два поступајућа заменика вишег тужиоца и одређени број тужилачких сарадника.

Поред описаног, надлежности органа у овој областии и имају Сектор за нормативне послове и међународну сарадњу у оквиру свог Одељења за узајамну правну помоћ и у оквиру МУП-а, Управа за међународну оперативну полицијску сарадњу - Национални централни биро Интерпола Београд. Наравно да у том смислу од великог значаја јесте и потписани оперативни споразум са ЕУРОПОЛ- ом.

2.2 Криминални новчани токови

У смислу законских одредби на располагању да следе кривичне новчане токове и да тражи, заплени и конфискује приходе, закон о одузимању имовине учинилаца кривичних дела садржи опште одредбе и могуће је спровођење финансијске истраге и конфискације имовине, без обзира на то како је до кривичног дела дошло. Према новом концепту довољно је да се докаже да имовине има, а терет доказивања о начинима стицања је на субјеку који је осумњичен за прање новца и финансирање тероризма. Ако је дело извршено на интернету и испуњава ове опште одредбе, финансијска истрага ће бити спроведена и поступак ће се даље одвијати својим током. Овакви поступци финансијских истрага ће бити иницирани онда када тужилац изда налог за такве истраге, а оне ће бити спроведене од стране Јединица за финансијске истраге МУП- у. У исте ће бити укључена и Управа за спречавање прања новца Министарства финансија. Улоге тих

институција одговорних за питања финансијских истрага и праћење токова новца су следеће[728]:

- Министарство финансија - Управа за спречавање прања новца поступци откривања и пријављивања дела из надлежности;
- Министарство унутрашњих послова - Финансијске истраге спроведене од стране јединице за финансијске истраге (ФОС);
- Министарство правде - тужилаштво, судски поступци и одузета имовина управљање.

Поменута Министарства су институционално одговорна за праћење токова новца стеченог кроз злочиначке подухвате и за откривање, одузимање и конфискацију имовине стечене криминалом, без обзира на то да ли је кривично дело из области ВТК или не. Следеће специфичне активности у овим случајевима спроводе:

- Управа за спречавање прања новца прикупља и анализира податке о сумњивим трансакцијама;
- Јединица за финансијске истраге спроводи истраге са циљем да идентификују и пронађу средства добијена кроз криминалне активности;
- Одељење за организовани криминал води финансијски претkривични поступак у циљу идентификовања починилаца злочина у области сајбер криминала, као и других злочина који се изводе употребом рачунара и рачунарских мрежа.

Пре покретања кривичног поступка полицајци спроводе, тзв. потражне активности или радње, али предузимају и (доказне) истражне радње, како би се открили учиниоци кривичних дела и у циљу спречавања њиховог бекства или скривања и у циљу проналажења, фиксирање и обезбеђивања предмета и трагова и других доказа кривичног дела, као и прикупљања обавештења корисних за вођење кривичног поступка[729]. У овом случају, надлежност за предузимање радњи и примену овлашћења имају полиција, јавни тужилац и суд у случајевима прописаним законом.

Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (Маријин закон) прописује посебне мере за учиниоце сексуалног злостављања почињеног над малолетником, утврђене овим законом и регулишу вођење посебне евиденције о лицима осуђеним за ове злочине.

728 Лајић, О. Лукић, Т. Ивановић, З. Специфичности финансијске истраге у Србији, Тематски Зборник радова међународног значаја, Академија за Криминалистичко-полицијска академија, Београд 2011 Међународна научна конференција "Арчибалд Рајс дана" пп 369 – 381;

729 Ивановић, З. Жарковић, М. научни приступ у изградњи тимова за одузимање дигиталних доказа, стр 399-413 у тематском зборнику међународног значаја, Академија криминалистике и полицијских студија, 2013, ур . Горан Милошевић;

2.3 Национално законодавство и високотехнолошки криминал

2.3.1 Закони

Иако смо ратификовали одређени број односних конвенција према овој материји, Србија није у потпуности адекватно правно-технички регулисала материју у вези са ВТК, а тиче се ИКТ. Оваква ситуација, ипак, није таква да иде на руку органима који су надлежни за њену примену, а и правни партикуларитет овде ствара велике проблеме за органе гоњења специјализоване за ВТК.

Законодавство у Србији и поред уплива препорука и конвенција ОЕБС-а (OSCE) крајем 20. века, па до 2006. године, није третирало област ИКТ у мери у којој је требало. Наиме, иако је Државна заједница Србије и Црне Горе (ДЗ СЦГ) још од 2005. године потписница Конвенције о Високотехнолошком криминалу (Counsel of Europe Cybercrime Convention – CETS 185), тек је крајем те године дошло до доношења Кривичног законика (ступио на снагу 1.1.2006) који, тада, само делом уважава одредбе ЦЕТС-а 185. Од тада у нашем законодавству биће доста измена, од којих ће неке и темељно изменити ову структуру.

2.3.2 Организациони и процедурални аспекти

Кривични законик Републике Србије у глави XXVII под називом „Кривична дела против безбедности рачунарских података“ прописао је даље у тексту приказана кривична дела.

2008. године је у МУП-у и СБПОК-у формирано Одељење за борбу против високотехнолошког криминала. Ово Одељење састоји се од два одсека: Одсек за сузбијање криминалитета у области интелектуалне својине и Одсек за сузбијање електронског криминала.

Онда у Окружном, а сада у Вишем јавном тужилаштву у Београду, основано је Посебно тужилаштво за високотехнолошки криминал, а у Окружном (сада Вишем) суду поступајући судија и двојица истражних судија

Законом о изменама и допунама Кривичног законика од 31.8.2009. године, објављеном у Службеном гласнику Републике Србије број 72/09, све је делимично усклађен са Конвенцијама 185 и 189.

2.3.3 Измене у надлежности

Законом о изменама и допунама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је објављен у Службеном гласнику Републике Србије број 104/09 дана 11.12.2009. године, наводи се да се Закон примењује ради откривања, кривичног гоњења и суђења за:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником;
2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже

и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара;

3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2 став 1 овог закона.

Изменом се ишло ка повећању броја примерака ауторских дела (новим изменама је број примерака ауторских дела прелази 2000, а према старом закону је био 500, такође има измена и у материјалној штети која је, по новом преко 1.000.000 динара, а била је 850.000 динара). Додат је и трећи став, чиме је надлежност проширена и на друга наведена кривична дела.

2.3.4 Измене – у организационом смислу

Према новим изменама Посебно тужилаштво за високотехнолошки криминал остаје као такво, али се налази у оквиру Вишег јавног тужилаштва у Београду. Републички јавни тужилац поставља посебног тужиоца за ВТК из реда јавних тужилаца и заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља.

Стварно и месно надлежно је Одељење Вишег суда у Београду, а не веће, како је до сада било. Тренутно, у оквиру Вишег јавног тужилаштва у Београду функционише Одељење за високотехнолошки криминал Вишег јавног тужилаштва у Београду, надлежно за читаву територије Републике Србије, у оквиру кога се налазе два поступајућа заменика вишег тужилаштва.

Поред описаних органа, надлежност у овој материји имају и Сектор за нормативне послове и међународну сарадњу, а у оквиру њега Одељење за међународну правну помоћ и, такође, у оквиру МУП-а РС, Управе за међународну оперативну полицијску сарадњу - Национални централни биро ИНТЕРПОЛ –а Београд. Ова управа обавља: послове који се односе на поступање по замолницама домаћих и страних судова и других надлежних домаћих и страних државних органа, уступање и преузимање кривичног гоњења окривљених лица, расписивање међународних потерница и екстрадицију окривљених и осуђених лица, извршење страних кривичних пресуда – трансфер осуђених лица, праћење послова европских интеграција у области међународне правне помоћи, међународне колизионе норме у овој области, примену законског и уговорног реципроцитета, признање и извршење страних судских и арбитражних одлука, поступање у предметима међународне отмице деце, давање мишљења правосудним и другим органима у вези са важењем и применом међународних уговора, као и појединих института међународне правне помоћи, обавештења о прописима, сачињавање информације и извештаја из области међународне правне помоћи, припрему и закључивање међународних уговора из међународне правне помоћи, сарадњу са УНМИК-ом, оверу исправа за употребу у иностранству и друге послове из делокруга Одељења.

2.4 Поступање

Поступање се спроводи:

- **пре покретања кривичног поступка** – приликом предузимања тзв. потражних радњи или одређених (доказних) истражних, у циљу откривања кривичних дела и учинилаца, спречавање бекства и сакривања учинилаца, и проналажење, фиксирање и обезбеђење предмета и трагова као доказа о кривичним делима, као и прикупљање обавештења од користи за вођење кривичног поступка. У овом случају поступају полиција, јавни тужилац, као и суд у законом прописаним случајевима;
- **у току кривичног поступка**, када поступају по налозима и наредбама руководећих органа у поступку (судија за претходни поступак, судско веће, судија појединац) – полиција, али и самостално у процесном положају тужиоца, јавни тужилац и овлашћени тужилац.

Кривично правне карактеристике

У ВТК у Србији спадају према Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала:

- кривична дела против безбедности рачунарских података;
- против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику (уз додатне услове 2000 примерака и 1.000.000 динара);
- кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала.

Правни партикуларитет се у Србији приказује и у оквиру одређених, системских закона где се налазе постојећа кривична дела и материја од значаја за поступање органа у области ВТК.

У Министарству унутрашњих послова извршење задатака обезбеђено је јединственом организацијом на територији Републике Србије. У седишту Министарства унутрашњих послова, у оквиру Управе криминалистичке полиције од 2006. године, први пут је уведена посебна организациона јединица – Одсек за превенцију и сузбијање малолетничке делинквенције у чијој надлежности је, поред осталог, праћење и анализа стања у области кривично-правне заштите малолетних лица, пружање стручне помоћи у примени полицијских овлашћења према малолетницима, организација и унапређење функционисања рада прописивањем јединствених стандарда и процедура, као и перманентно стручно усавршавање полицијских службеника, распоређених у 27 подручних јединица – полицијских управа, са 109 полицијских станица – јединица надлежних за територију једне општине.

Пословима превенције и сузбијања кривичних дела, када се као оштећени појављују малолетна лица, баве се одељења и одсеци, тј. специјализовани полицијски службеници у оквиру организационих јединица МУП-а Републике Србије (за сада њих 1752 су стекли одговарајуће сертификате у складу са чланом 165

Закона о малолетним учиниоцима кривичних дела и кривично-правној заштити малолетних лица, издате од стране Правосудног центра за обуку и стручно усавршавње, данас Правосудне академије). У случајевима вршења кривичних дела на штету малолетних лица путем интернета бави се Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Републике Србије. Одсек за сузбијање електронског криминала, који се налази у Одељењу за борбу против високотехнолошког криминала, ради на сузбијању кривичних дела против безбедности рачунарских података као и кривичних дела: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ), навођење малолетног лица на присуствовање полним радњама (чл. 185а КЗ) и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б КЗ).

С циљем обезбеђивања несметане и што ефикасније међуресорске сарадње, у складу са Националним планом акције за децу, као и са основним принципима и смерницама из Општег протокола за превенцију и заштиту деце од злостављања и занемаривања, министар унутрашњих послова донео је октобра 2006. године Посебни протокол о поступању полицијских службеника у заштити малолетних лица од злостављања и занемаривања. Посебним протоколом уређују се процедуре при поступању полицијских службеника Министарства унутрашњих послова Републике Србије према малолетним лицима. Овај протокол намењен је свим организационим јединицама Министарства унутрашњих послова Републике Србије и обавезујући је за све полицијске службенике.

2.5 Правосуђе

У кривичном поступку ради, посебне заштите малолетних лица као оштећених, изричито је предвиђена посебна специјализација тужилаца и судија. О стицању посебних знања и стручном усавршавању судија и тужилаца који раде у области права детета и кривично-правне заштите малолетних лица, стара се Правосудна академија, у сарадњи са релевантним министарствима, надлежним за правосуђе, социјалну политику, унутрашње послове и Адвокатском комором Републике Србије. О обављеним проверама знања и стручном усавршавању Правосудна академија издаје одређене сертификате.

У случајевима када се суди пунолетним учиниоцима, постоји 27 таксативно набројаних кривичних дела, међу којима је и кривично дело приказивање, прибављање и поседовње порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ), односно у свим оним случајевима када то процени специјализовани јавни тужилац (тужилац који је стекао посебна знања из области права детета и кривично-правне заштите малолетних лица), а оштећени је малолетно лице, примењују се посебне законске одредбе о његовој заштити. Истрагу, такође, спроводи специјализовани истражни судија, а малолетно лице као оштећени мора имати пуномоћника од првог саслушања окривљеног из реда специјализиваних адвоката.

У складу са Законом о уређењу судова, Законом о јавном тужилаштву и Законом о седиштима и подручјима судова и јавних тужилаштава, првостепена

надлежност у кривичним поступцима, када се малолетно лице појављује као оштећено, од 1. јануара 2010. године, подељена је између 34 основна (основни суд у првом степену суди за кривична дела за које је као главна казна предвиђена новчана казна или казна затвора до десет година и десет година ако за поједина од њих није надлежан други суд) и 26 виших судова (суде за кривична дела за које је као главна казна предвиђена казна затвора преко десет година – виши суд у првом степену увек поступа у кривичним поступцима према малолетницима), односно основних и виших тужилаштава. Апелациони судови (у Београду, Новом Саду, Крагујевцу и Нишу) одлучују о жалбама на одлуке виших судова и на одлуке основних судова у кривичном поступку, ако за одлучивање о жалби није надлежан виши суд.

Законом о изменама и допунама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (из децембра 2009. године) предвиђена је надлежност Посебног одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, за кривично гоњење учинилаца кривичних дела против полне слободе, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала. У Посебном одељењу за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду процесуирање ове врсте кривичних дела обављају 3 заменика јавног тужиоца - руководилац одељења и два његова заменика, који поседују сертификате за рад са малолетним лицима оштећенима.

У јуну 2009. година, министарка правде донела је Посебни протокол о поступању правосудних органа у заштити малолетних лица од злостављања и занемаривања. Као специфични циљеви доношења овог Правилника одређени су: 1) допринос успостављању ефикасне и јединствене процедуре, која ће осигурати постојање брзог и координираног поступка који штити малолетна лица од даље виктимизације и обезбеђује им одговарајућу помоћ и 2) допринос остваривању ефикаснијег протока информација између организационих јединица министарства надлежног за правосуђе и правосудних и других државних органа и служби, укључених у процес заштите малолетних лица.

2.5.1 Закон о ауторским и сродним правима

Овај закон из децембра 2009. године, у оквиру поглавља о заштити ауторских и сродних права, у члану 208 дефинише да, и поред случајева предвиђених одредбом члана 204, повреду права представља и:

1) искоришћавање било ког предмета заштите уз употребу неовлашћено умножених примерака тог предмета заштите, односно на основу неовлашћене емисије;
2) држање у комерцијалне сврхе примерака ауторског дела или предмета сродног права, ако држалац зна или има основа да зна да је реч о неовлашћено произведеном примерку;
3) производња, увоз, стављање у промет, продаја, давање у закуп, рекламирање у циљу продаје или давања у закуп или држање у комерцијалне сврхе уређаја који су превасходно конструисани, произведени или прилагођени да омогуће или олакшају заобилажење било

које технолошке мере, и који немају другу значајнију сврху осим наведене;
4) заобилажење било које технолошке мере или пружање или рекламирање услуге којом се то омогућава или олакшава;
5) уклањање или измена електронске информације о правима, или стављање у промет, увоз, емитовање или на други начин јавно саопштавање ауторског дела или предмета сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена, а да при том учинилац зна или има основа да зна да тиме подстиче, омогућава, олакшава или прикрива повреду ауторског права или сродног права.

Израз „технолошке мере" означава сваку технологију, уређај или део који је конструисан да током своје наменске употребе онемогући или ограничи радње у вези са ауторским делом или другим предметом заштите, за које носилац ауторског или сродног права није дао сагласност.

Израз „информација о правима" означава сваку информацију која потиче од носиоца права и која идентификује ауторско дело или предмет сродноправне заштите, аутора, односно носиоца права, или информацију о условима коришћења дела или предмета сродноправне заштите, или било који број или шифру која представља такву информацију.

Казненим одредбама предвиђени су и привредни преступи, па се тако у члану 215 предвиђа - да ће се казнити за привредни преступ новчаном казном у износу од 100.000 до 3.000.000 динара привредно друштво или друго правно лице које:

1) неовлашћено објави, забележи, умножи или јавно саопшти на било који начин, у целини или делимично, ауторско дело, интерпретацију, фонограм, видеограм, емисију или базу података, или стави у промет или да у закуп или у комерцијалне сврхе држи неовлашћено умножене или неовлашћено стављене у промет примерке ауторског дела, интерпретације, фонограма, видеограма, емисије или базе података (чл. 16, 20, 21,22, 25, 26, 27, 28, 29, 116, 126, 131, 136 и 140);
2) у циљу прибављања имовинске користи за себе или другог противправно стави у промет или да у закуп примерке из става 1 овог члана, за које зна да су неовлашћено објављени, забележени или умножени (чл. 16, 20, 21, 22, 25, 26, 27, 28, 29, 116, 126, 131, 136 и 140);
3) произведе, увезе, стави у промет, прода, да у закуп, рекламира у циљу продаје или давања у закуп или држи у комерцијалне сврхе уређаје који су превасходно конструисани, произведени или прилагођени да омогуће или олакшају заобилажење било које технолошке мере, или који немају другу значајнију сврху осим наведене (члан 208 став 1 тачка 3);
4) заобилази било коју технолошку меру или пружа или рекламира услуге којима се то омогућава или олакшава (члан 208 став 1 тачка 4);
5) уклони или измени електронску информацију о правима, или стави у промет, увезе, емитује или на други начин јавно саопшти ауторско дело или предмет сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена и при том зна или има

основа да зна да тиме подстиче, омогућује, олакшава или прикрива повреду ауторског права или сродног права (члан 208 став 1 тачка 5);
6) обавља послове колективног остваривања ауторског, односно сродних права без дозволе надлежног органа (члан 160 став 4).

За радње из става 1 овог члана казниће се за привредни преступ новчаном казном у износу од 50 хиљада до 200 хиљада динара и одговорно лице у привредном друштву или другом правном лицу.

Предмети извршења привредних преступа и предмети који су били употребљени за извршење привредног преступа биће одузети, а предмети извршења привредних преступа биће и уништени. Пресуда којом је учиниоцу изречена казна за привредни преступ јавно се објављује. Кажњавање предузетника је предвиђено чланом 216 за радње из члана 21 став 1 тачка 1, 2, 3, 4, 5 и 7 овог закона казниће се за прекршај предузетник новчаном казном у износу од 50 хиљада до 500 хиљада. За радњу из члана 215 став 1 тачка 6 овог закона казниће се за прекршај физичко лице новчаном казном у износу од 10 хиљада до 50 хиљада динара.

Предмети извршења прекршаја и предмети који су били употребљени за извршење прекршаја из ст. 1 и 2 овог члана биће одузети, а предмети извршења прекршаја биће и уништени.

Такође и у члану 217 предвиђа се:

Казниће се за прекршај новчаном казном у износу од 100 хиљада до милион динара привредно друштво или друго правно лице које:
1) без навођења имена аутора или интерпретатора или под другим именом у целини или делимично објави, изведе, представи, пренесе извођење или представљање или емитује туђе ауторско дело или искористи туђу интерпретацију (чл. 15 и 114 став 1 тачка 2);
2) без дозволе аутора измени или преради туђе ауторско дело или туђу снимљену интерпретацију (чл. 17, 31 и 114 став 1 тачка 3);
3) приликом уношења у евиденцију и депоновања код надлежног органа, ауторског дела или предмета заштите сродног права да неистинити или прикрије прави податак о свом ауторском делу или предмету заштите сродног права (члан 202 став 4);

За радње из става 1 овог члана, казниће се за прекршај новчаном казном у износу од 10 хиљада до 50 хиљада динара и одговорно лице у привредном друштву или другом правном лицу. За радње из става 1 овог члана, казниће се предузетник новчаном казном у износу од 10 хиљада до 200 хиљада динара. За радње из става 1 тачка 4 и 5 овог члана, казниће се и физичко лице новчаном казном у износу од 10 хиљада до 50 хиљада динара. Новчаном казном у износу од 10 хиљада до 50 хиљада динара казниће се за прекршај физичко лице које у року од 30 дана од дана продаје примерка оригинала дела, односно рукописа не обавести аутора дела о имену и адреси купца и не плати износ од 3% од продајне цене (члан 35 став 1 и члан 36 став 2). Значајно је напоменути да овлашћења у смислу гоњења прекршаја има надлежна инспекција и одговарајући надлежни прекршајни суд, док у погледу привредних преступа поступају надлежни јавни тужилац и надлежни суд.

2.5.2 Закон о електронским комуникацијама

Поред приказаног закона о ауторским и сродним правима, од ширег значаја у области ВТК је и Закон о електронским комуникацијама. Он је усвојен 2010. године и чланом 150 је укинут, до тада важећи, Закон о телекомуникацијама. Од значаја за овај текст су одредбе Закона којима се уређују: услови и начин за обављање делатности у области електронских комуникација; надлежности државних органа у области електронских комуникација; заштита права корисника и претплатника; безбедност и интегритет електронских комуникационих мрежа и услуга; тајност електронских комуникација, законито пресретање и задржавање података; надзор над применом овог закона; мере за поступање супротно одредбама овог закона, као и друга питања од значаја за функционисање и развој електронских комуникација у Републици Србији (чл. 1). Затим и одредба (чл. 4) којом се прописује „значење појединих појмова“ као што су електронска порука (тач. 11), интернет (тач. 15), јавна комуникациона мрежа (тач. 18), комуникација (тач. 23) приступ (тач. 38). Овим законом се дефинишу и случајеви и услови за обраду података о саобраћају електронским комуникацијама (члан 122). Оператор јавних комуникационих мрежа или оператор јавно доступних електронских комуникационих услуга, који обрађује и чува податке о саобраћају претплатника и корисника, дужан је да те податке обрише или учини непрепознатљивим лице на које се ти подаци односе, када подаци о саобраћају више нису неопходни за пренос комуникације, са изузетком:

1) података који су неопходни ради израде рачуна за услуге или међуповезивање, а који се могу обрађивати до истека законом предвиђеног рока за рекламације или наплату потраживања;
2) података које оператор користи ради оглашавања и продаје услуга, уз претходни пристанак лица на које се подаци односе, као и ради пружања услуга са додатом вредношћу, у мери и времену неопходном за те сврхе;
3) података који се задржавају у складу са одредбама овог закона.

Оператор је дужан да, пре отпочињања обраде података о саобраћају, као и пре прибављања пристанка из тачке 2, обавести претплатника или корисника о врстама података који ће бити обрађивани, као и о трајању обраде. Лице које је дало пристанак за обраду података има право опозива датог пристанка у било ком тренутку. Обраду података о саобраћају смеју да чине само лица која за потребе оператора обављају послове издавања рачуна, управљања мрежним саобраћајем, одговарања на питања корисника, откривања превара, оглашавања и продаје услуга електронских комуникација, као и пружања услуга са додатом вредношћу, у мери неопходној за обављање наведених активности.

Од значаја је и одредба у погледу обраде података о локацији (члан 123). Оператор јавних комуникационих мрежа и јавно доступних електронских комуникационих услуга може обрађивати податке о локацији корисника, који нису подаци о саобраћају, само када се лица на која се ти подаци односе учине непрепознатљивим или уз њихов претходни пристанак ради пружања услуга са додатом вредношћу, у мери и времену потребном за те сврхе. Описано се не односи на податке о локацији који се задржавају у складу са одредбама овог закона. Оператор је дужан да, пре прибављања пристанка, корисника и претплатника обавести о врстама података о локацији који ће бити обрађивани, сврси и трајању

обраде, као и томе да ли ће подаци бити достављани трећим лицима за потребе пружања услуга са додатом вредношћу. И у овом случају, лице које је дало пристанак за обраду има право опозива датог пристанка у било ком тренутку. Оператор је дужан да лицу, које је дало пристанак за обраду података, пружи могућност привременог одбијања обраде података о локацији при сваком повезивању на мрежу или преносу комуникације, на једноставан начин и без накнаде. Обраду података о локацији из овог члана смеју да чине само овлашћена лица оператора, односно овлашћена лица треће стране која пружа услугу са додатом вредношћу, у мери неопходној за пружање услуге са додатом вредношћу. У погледу безбедности и интегритета јавних комуникационих мрежа и услуга, чланом 124 Закон прописује да је оператор дужан да, ради обезбеђивања безбедности и интегритета јавних електронских комуникационих мрежа и услуга, тајности комуникација, као и заштите података о личности, саобраћају и локацији, примени адекватне техничке и организационе мере, примерене постојећим ризицима, а посебно мере за превенцију и минимизацију утицаја безбедносних инцидената по кориснике и међуповезане мреже, као и мере за обезбеђивање континуитета рада јавних комуникационих мрежа и услуга.

Ако оператор пружа услугу користећи електронску комуникациону мрежу, припадајућа средства или услуге другог оператора, дужан је да сарађује са тим оператором у обезбеђивању безбедности и интегритета јавних комуникационих мрежа и услуга. Када постоји посебан ризик повреде безбедности и интегритета јавних комуникационих мрежа и услуга (неовлашћени приступ, значајан губитак података, угрожавање тајности комуникација, безбедности података о личности и друго), оператор је дужан да о том ризику обавести претплатнике и, ако је такав ризик ван опсега мера које је оператор дужан да примени, обавести претплатнике о могућим мерама заштите и трошковима у вези са применом тих мера. Овим путем се уводи обавеза оператера за обавештавање јавности о ризицима по кориснике услуга, одавно постојећа у ЕУ. А што се тиче обавезе објављивања информација о продорима у базе података о личности и свакој другој повреди безбедности и интегритета јавних комуникационих мрежа и услуга, она је прописана чл. 125. Оператор је, дакле, дужан да обавести Агенцију о свакој повреди безбедности и интегритета јавних комуникационих мрежа и услуга, која је значајно утицала на њихов рад, а нарочито о повредама које су имале за последицу нарушавање заштите података о личности или нарушавање приватности претплатника или корисника. Агенција је овлашћена да обавести јавност о повреди безбедности и интегритета или да тражи од оператора да то сам уради, када процени да је објављивање такве информације у јавном интересу.

Главом XVII, под називом Тајност електронских комуникација, законито пресретање и задржавање података прописана је чланом 126 - тајност електронских комуникација. Према том члану, пресретање електронских комуникација којим се открива садржај комуникације није допуштено без пристанка корисника, осим на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Ова одредба не спречава снимање комуникација и са њима повезаних података о саобраћају, које се обавља ради доказивања комерцијалних трансакција или других пословних односа, у којима су обе стране свесне или би морале бити свесне или су изричито упозорене на то да обављена комуникација може да буде снимљена. Коришћење електронских

комуникационих мрежа и услуга ради чувања или приступања подацима похрањеним у терминалској опреми претплатника или корисника, дозвољено је под условом да је претплатнику или кориснику дато јасно и потпуно обавештење о сврси прикупљања и обраде података, у складу са законом којим се уређује заштита података о личности, као и да му је пружена прилика да такву обраду одбије. Последња одредба не спречава техничко чување или приступ подацима, у сврху обезбеђивања комуникације у оквиру електронских комуникационих мрежа или пружања услуга које је претплатник или корисник изричито затражио.

Члан 127 прописује услове за Законито пресретање електронских комуникација. Оператор је дужан да омогући законито пресретање електронских комуникација. Надлежни државни орган који спроводи послове законитог пресретања дужан је да води евиденцију о пресретаним електронским комуникацијама, које нарочито садрже одређење акта који представља правни основ за вршење пресретања, датум и време вршења пресретања, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података. Када надлежни државни орган, који спроводи послове законитог пресретања није у могућности да изврши законито пресретање електронских комуникација без приступа просторијама, електронској комуникационој мрежи, припадајућим средствима или електронској комуникационој опреми оператора, оператор је дужан да о примљеним захтевима за пресретање електронских комуникација води евиденцију, која нарочито садржи идентификацију овлашћеног лица које је вршило пресретање, одређење акта који представља правни основ за вршење пресретања, датум и време пресретања, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података.

Оператор је дужан да, ради остваривања обавезе омогућавања пресретања електронских комуникација, о свом трошку, обезбеди неопходне техничке и организационе услове (уређаје и програмску подршку), као и да доказе о томе достави Агенцији, у складу са одредбама овог закона.

Министарство, по прибављеном мишљењу министарства надлежног за послове правосуђа, министарства надлежног за унутрашње послове, министарства надлежног за послове одбране, Безбедносно-информативне агенције и органа надлежног за заштиту података о личности, ближе прописује захтеве за уређаје и програмску подршку.

Овај закон прописује и обавезу задржавања података чланом 128. Оператор је дужан да задржи податке о електронским комуникацијама из члана 129 став 1 овог закона (у даљем тексту: задржани подаци) за потребе спровођења истраге, откривања кривичних дела и вођења кривичног поступка, у складу са законом којим се уређује кривични поступак, као и за потребе заштите националне и јавне безбедности Републике Србије, у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова.

Оператор је дужан да задржи податке у изворном облику или као податке обрађене током обављања делатности електронских комуникација.

Оператор није дужан да задржи податке које није произвео нити обрадио.

Оператор је дужан да задржане податке чува 12 месеци од дана обављене комуникације.

Оператор је дужан да задржава податке тако да им се без одлагања може приступити, односно да се без одлагања могу доставити на захтев надлежног државног органа.

Надлежни државни орган који остварује приступ, односно коме се достављају задржани подаци, дужан је да води евиденцију о приступу, односно достављању задржаних података, која нарочито садржи: одређење акта који представља правни основ за приступ, односно достављање задржаних података, датум и време приступања, односно достављања задржаних података, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података.

Када надлежни државни орган није у могућности да оствари приступ задржаним подацима без приступа просторијама, електронској комуникационој мрежи, припадајућим средствима или електронској комуникационој опреми оператора, оператор је дужан да о примљеним захтевима за приступ, односно достављању задржаних података, води евиденцију .

У погледу заштите задржаних података чланом 130 је предвиђено да је оператор дужан да, у погледу заштите задржаних података, нарочито обезбеди:

1) да су задржани подаци истог квалитета и подвргнути истим мерама безбедности и заштите као и подаци у електронској комуникационој мрежи оператора;
2) да су задржани подаци заштићени на подесан начин од случајног или недопуштеног уништења, случајног губитка или измене, неовлашћеног или незаконитог чувања, обраде, приступа или откривања, у складу са законом којим се уређује заштита података о личности, односно законом којим се уређује заштита тајних података када се ради о подацима који су сачувани и достављени у складу са чланом 128 став 5 овог закона;
3) да се приступ задржаним подацима на подесан начин ограничи само на овлашћена лица органа који остварују приступ задржаним подацима, у складу са чланом 128 став 5 овог закона;
4) да се задржани подаци униште по истеку рока из члана 128 став 4 овог закона, осим података који су сачувани и достављени у складу са чланом 128 став 5 овог закона.

Оператор је дужан да, ради остваривања обавезе, о свом трошку, обезбеди неопходне техничке и организационе услове, као и да доказе о томе достави Агенцији.

2.5.3 Закон о заштити података о личности

Овим законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података и надзор над извршавањем закона.

Послове заштите података о личности обавља Повереник за информације од јавног значаја и заштиту података о личности, као самосталан државни орган, независан у обављању своје надлежности. Он је успостављен са циљем да, у вези са обрадом података о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода.

Међутим, закон се не примењује на обраду свих података. Одредбе овог закона не примењују се на обраду одређене групе података, осим уколико

„очигледно претежу супротни интереси лица“. То су следеће групе података: подаци доступни свакоме (јавна гласила и публикације, архиве, музеји), породични и лични подаци, који нису доступни трећим лицима, затим, подаци о члановима политичких странака и других облика удруживања, који се обрађују од тих организација, али док траје чланство и података које је лице само објавило о себи, а оно је способно да се само стара о својим интересима.

Сви други подаци који се прикупљају и обрађују у друге сврхе, могу да се обрађују искључиво у историјске, статистичке или научно-истраживачке сврхе, ако не служе доношењу одлука или предузимању мера према одређеном лицу уз обезбеђивање одговарајућих мера заштите.

Закон изричито наводи ситуације у којима обрада података (али не и прикупљање) није дозвољена, и то ако:

1) физичко лице није дало пристанак за обраду или се обрада чини без законског овлашћења;
2) се обрада чини у сврху различиту од оне за коју је одређена, без обзира да ли се врши на основу пристанка или законског овлашћења;
3) сврха обраде није јасно одређена, ако је измењена, недозвољена или је већ остварена;
4) је лице на које се подаци односе, одређено или одредиво и након што се оствари сврха обраде;
5) је начин обраде недозвољен;
6) је податак који се обрађује непотребан или неподесан за остварење сврхе обраде;
7) су број или врста података који се обрађују несразмерни сврси обраде;
8) је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео.

Постоји изричита забрана аутоматске обраде одређене врсте података. Тако, одлука која производи правне последице или погоршава његов положај неког лица, не може бити искључиво заснована на подацима који се обрађују аутоматизовано и који служе оцени неког његовог својства (радне способности, поузданости, кредитне способности и слично), сем када је то законом изричито одређено, односно када се усваја захтев лица у вези са закључењем или испуњењем уговора, уз спровођење одговарајућих мера заштите. У том случају лице мора бити упознато са поступком аутоматизоване обраде и начином доношења одлуке.

Оно што је посебно интересантно је таксативно навођење ситуација када је обрада података допуштена ex lege иако нема пристанка, тзв. „обрада без пристанка“. Обрада без пристанка је дозвољена:

1) да би се остварили или заштитили животно важни интереси лица (живот, здравље и физички интегритет);
2) у циљу извршења законских обавеза или обавеза одређених актом донетим у складу са законом;
3) у другим (под)законским случајевима, ради остварења претежног оправданог интереса лица, руковаоца или корисника.

Обрада податке без пристанка лица од стране органа власти врши се ако је обрада неопходна у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања, откривања, истраге и гоњења за

кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса, а у другим случајевима на основу писменог пристанка лица.

Закон прави разлику између „обраде“' података и „прикупљања“' података. У том смислу он каже да се подаци прикупљају од лица на које се односе, од органа управе који су овлашћени за прикупљање и од другог лица ако:

1) је то предвиђено уговором закљученим са лицем на које се подаци односе;
2) је то прописано законом или другим прописом;
3) је то неопходно с обзиром на природу посла;
4) прикупљање података од самог лица захтева прекомерни утрошак времена и средстава;
5) се прикупљају подаци ради остварења или заштите животно важних интереса лица на које се односе, посебно живота, здравља и физичког интегритета.

Закон уводи посебну категорију података који се зову „нарочито осетљиви подаци“ у коју спадају: подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот. Ови подаци имају посебан законски режим прикупљања и обраде. Ови „нарочито осетљиви подаци'“ су посебно законом заштићени јер се могу обрађивати искључиво на основу слободно датог пристанка лица. Закон их посебно штити јер уводи још један степен заштите када прописује да се законом може забранити обрада ових нарочито осетљивих података, иако је и дат пристанак.

Изузетно, подаци о политичкој припадности, здравственом стању и социјалној помоћи, могу се обрађивати и без пристанка лица, ако је то законом допуштено.

Маријин закон

Уставни основ за доношење Закона о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима садржан је у члану 97 тачка 2 Устава Републике Србије према коме Република Србија, поред осталог, уређује и обезбеђује остваривање и заштиту слобода и права грађана и одговорност и санкције за повреду слобода и права и грађана утврђених Уставом и за повреду закона.

Чланом 37 Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања, коју је потврдила Народна скупштина маја 2010. године, обавезане су државе чланице ове конвенције да ради спречавања и гоњења кривичних дела установљених у складу са овом конвенцијом, предузму све неопходне законодавне или остале мере за прикупљање података који се односе на идентитет и на генетски профил (ДНК) лица која су осуђена за кривична дела установљена у складу са овом конвенцијом.

Поред тога, имајући у виду повећан број кривичних дела против полне слободе која су извршена према малолетним лицима, неопходно је да се поред постојећег система кривичних санкција, које се нису у потпуности показале као делотворне, уведу и посебне мере којима би се отклонили услови који могу бити од утицаја да учиниоци ових кривичних дела убудуће чине та дела.

Законом о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (Маријин закон) прописују се посебне мере које се спроводе према учиниоцима кривичних дела против полне слободе извршених према малолетним лицима одређених овим законом и уређује се вођење посебне евиденције лица осуђених за та кривична дела (члан 1 Службени гласник РС бр. 32/13). Као подручје примене закона чланом 3 се одређује да се он примењује на учиниоце који су према малолетним лицима извршили следећа кривична дела:

1) силовање (члан 178 ст. 3 и 4 Кривичног законика);
2) обљуба над немоћним лицем (члан 179 ст. 2 и 3 Кривичног законика);
3) обљуба са дететом (члан 180 Кривичног законика);
4) обљуба злоупотребом положаја (члан 181 Кривичног законика);
5) недозвољене полне радње (члан 182 Кривичног законика);
6) подвођење и омогућавање вршења полног односа (члан 183 Кривичног законика);
7) посредовање у вршењу проституције (члан 184 став 2 Кривичног законика);
8) приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185 Кривичног законика);
9) навођење малолетног лица на присуствовање полним радњама (члан 185а Кривичног законика);
10) искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б Кривичног законика).

Као сврху овог закона члан 2 одређује онемогућавање учинилаца кривичних дела против полне слободе извршених према малолетним лицима да убудуће чине ова дела.

Маријиним законом прописана је и забрана ублажавања казне и условног отпуста (члан 5) Учиниоцу кривичног дела на које се односи Маријин закон, суд не може ублажити казну применом члана 57 став 1 Кривичног законика. Лице осуђено на казну затвора за кривично дело из Маријиног закона не може се условно отпустити. Као правне последице осуде обавезно наступају следеће правне последице:

1) престанак вршења јавне функције;
2) престанак радног односа, односно престанак вршења позива или занимања које се односи на рад са малолетним лицима;
3) забрана стицања јавних функција;
4) забрана заснивања радног односа, односно обављања позива или занимања које се односи на рад са малолетним лицима.

Правне последице осуде наступају даном правноснажности пресуде. Правне последице осуде из става 1 тач. 3 и 4 трају 20 година. Време проведено на издржавању казне затвора не урачунава се у време трајања правне последице осуде.

Правноснажна пресуда обавезно се доставља и послодавцу осуђеног лица.

Имајући у виду циљ Закона прописан у члану 2, а то је отклањање услова који могу бити од утицаја да учиниоци кривичних дела против полне слободе извршених према малолетном лицу убудуће врше ова дела, чланом 7 Закона предвиђене су посебне мере које се спроводе након издржане казне затвора. Према учиниоцу кривичног дела из члана 3 овог закона, после издржане казне затвора, спроводе се следеће посебне мере:

1) обавезно јављање надлежном органу полиције и Управи за извршење кривичних санкција;
2) забрана посећивања места на којима се окупљају малолетна лица (вртићи, школе и слично);
3) обавезно посећивање професионалних саветовалишта и установа;
4) обавезно обавештавање о промени пребивалишта, боравишта или радног места;
5) обавезно обавештавање о путовању у иностранство.

Мере се спроводе 20 година после извршене казне затвора.

После истека сваке четири године од почетка примене посебних мера из става 1 овог члана, суд који је донео првостепену пресуду, по службеној дужности одлучује о потреби њиховог даљег спровођења.

Захтев за преиспитивање потребе даљег спровођења посебних мера може поднети и лице на које се ове мере односе. Овај захтев може се поднети суду који је донео првостепену пресуду после истека сваке две године од почетка примене посебних мера.

У поступку у коме одлучује о потреби даљег спровођења посебних мера, суд прибавља извештаје органа и организација надлежних за спровођење тих мера.

Прва мера - обавезно јављање надлежном органу полиције и Управе за извршење кривичних санкција детаљније је обрађена чланом 8. Под овом мером подразумева се дужност учиниоца кривичног дела из члана 3 овог закона да се лично јави организационој јединици полиције у месту његовог пребивалишта и организационој јединици Управе за извршење кривичних санкција надлежној за третман и алтернативне санкције, сваког месеца, најкасније до 15. дана у месецу.

Друга мера - забрана посећивања места на којима се окупљају малолетна лица (члан 9). Под мером забране посећивања места на којима се окупљају малолетна лица подразумева се дужност учиниоца кривичног дела из члана 3 овог закона да се уздржава од посећивања места на којима се окупљају малолетна лица, као што су школске зграде, школска дворишта, вртићи, игралишта и слично.

Трећа мера - обавезно посећивање професионалних саветовалишта и установа (члан 10) Под мером обавезног посећивања професионалних саветовалишта и установа подразумева се дужност учиниоца кривичног дела из члана 3 да посећује професионална саветовалишта и установе према програму који му одреди организациона јединица Управе за извршење кривичних санкција надлежна за третман и алтернативне санкције.

Четврта мера - обавезно обавештавање о промени пребивалишта, боравишта или радног места (члан 11). Под мером обавезног обавештавања о промени пребивалишта, боравишта или радног места подразумева се дужност учиниоца кривичног дела из члана 3. овог закона да у року од три дана од дана промене лично обавести надлежну организациону једниницу полиције и

организациону јединицу Управе за извршење кривичних санкција надлежну за третман и алтернативне санкције, о промени пребивалишта, боравишта или радног места.

Пета мера - обавезно обавештавање о путовању у иностранство (члан 12). Под мером обавезног обавештавања о путовању у иностранство подразумева се дужност учиниоца кривичног дела из члана 3. овог закона да се најкасније три дана пре путовања у иностранство лично јави надлежној организационој јединици полиције. Лице из става 1 овог члана је дужно да надлежној организационој јединици полиције пружи податке о држави у коју путује, као и о месту и дужини боравка у иностранству.

Маријин закон уводи и посебну евиденцију за осуђене извршиоце ових дела (члан 13). Посебна евиденција из става 1 овог члана садржи:

1) име и презиме осуђеног;
2) јединствени матични број грађана осуђеног;
3) адресу пребивалишта осуђеног;
4) податке о запослењу осуђеног;
5) податке о особеним знацима осуђеног;
6) ДНК профил осуђеног;
7) податке о кривичном делу и казни на коју је осуђен;
8) податке о правним последицима осуде;
9) податке о спровођењу посебних мера прописаних овим законом.

Посебну евиденцију води Управа за извршење кривичних санкција. Сви државни и други органи, као и правна лица или предузетници су дужни да у року од три дана од дана прибављања података о којима се води посебна евиденција прописана овим законом, те податке доставе овлашћеном лицу Управе за извршење кривичних санкција које води посебну евиденцију. Подаци из посебне евиденције воде се трајно и не могу се брисати. Министар надлежан за послове правосуђа ближе уређује начин вођења посебне евиденције. На овај начин се постиже централизација вођења података из посебне евиденције, чиме се омогућава ефикасније праћење спровођења овог закона и олакшава приступ потребним подацима, органима који су надлежни за сузбијање кривичних дела против полних слобода, како у земљи тако и у иностранству. Подаци из посебне евиденције могу се дати суду, јавном тужиоцу и полицији у вези са кривичним поступком који се води против лица о коме се води посебна евиденција, односно надлежној организационој јединици полиције, као и организационој јединици Управе за извршење кривичних санкција надлежној за третман и алтернативне санкције, када је то потребно за вршење послова из њихове надлежности (члан 15).

Подаци из посебне евиденције могу се, на образложен захтев, дати и државном органу, предузећу, другој организацији или предузетнику, ако још трају правне последице осуде и ако за то постоји оправдани интерес заснован на закону. Државни и други органи, као и правна лица или предузетници који раде са малолетним лицима дужни су да затраже податак да ли је лице које треба да заснује радни однос код њих, односно да обавља послове са малолетним лицима, уписано у посебну евиденцију. Подаци из посебне евиденције могу се дати и иностраним државним органима, у складу са међународним споразумом. На податке садржане у посебној евиденцији, ако одредбама овог закона није другачије прописано, сходно се примењују одредбе закона који уређују заштиту података о личности и

тајност података. Треба истаћи да приступ подацима из посебне евиденције могу остварити и инострани државни органи, у складу са међународним споразумом, што је неопходно ради сузбијања кривичних дела сексуалног злостављања и искоришћавања малолетних лица на међународном плану, а што је прописано у члану 37 тачка 3 Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања.

Прекршаји учиниоца кривичног дела предвиђени су Маријиним законом у члану 16. Казном затвора од 30 до 60 дана казниће се за прекршај учинилац кривичног дела из члана 3 овог закона ако:

1) прекрши правну последицу осуде из члана 6 став 1 овог закона;
2) не испуњава посебне мере из члана 7 став 1 овог закона.

У члану 17 Маријиног закона наведени су и прекршаји правног лица, предузетника и одговорних лица.

Новчаном казном од 500 хиљада динара до 2 милиона динара казниће се за прекршај правно лице ако:

1) не поштује правну последицу осуде из члана 6 став 1 овог закона;
2) не достави податак или не достави податак у прописаном року овлашћеном лицу Управе за извршење кривичних снакција које води посебну евиденцију (члан 14 став 2).
3) не затражи податак из посебне евиденције у складу са чланом 15 став 3 овог закона.

За прекршај из става 1 овог члана казниће се предузетник новчаном казном од 200 хиљада до 500 хиљада динара.

За прекршај из става 1 овог члана казниће се и одговорно лице у правном лицу и државном и другом органу новчаном казном од 100 хиљада до 150 хиљада динара.

Законска решења заснована су на релевантним међународним документима, као што су наведена конвенција, Препорука REC (2001) 16 о заштити деце од сексуалног искоришћавања, Оквирна одлука Савета Европске уније о борби против сексуалног искоришћавања деце и дечје порнографије, као и на пракси Европског суда за људска права у Стразбуру и упоредноправним решењима држава које имају прописе које уређују предметно питање (Велика Британија, Француска, Норвешка и Канада).

2.5.4 Породични закон (Службени гласник РС, бр. 18/2005)

Овај закон установљава обавезу државе да предузме све потребне мере за заштиту детета од занемаривања, од физичког, сексуалног и емоционалног злостављања, те од сваке врсте експлоатације, као и обавезу свих дечјих здравствених и образовних установа, установа социјалне заштите, правосудних и других судских органа, удружења и грађана да обавесте јавног тужиоца или орган старатељства о потреби и разлозима за заштиту права детета. Породични закон, такође, установљава право детета на независно заступање у случајевима колизије интереса детета и законског заступника детета и уводи специјализацију судија за поступање у породичним стварима. Обуку судија спроводи Правосудна академија,

сходно Правилнику о програму и начину стицања посебних знања из области права детета судија који суде у поступцима у вези са породичним односима.

Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица (Службени гласник РС, бр. 85/2005) ради посебне заштите личности малолетних лица као оштећених, односно оштећених који се саслушавају као сведоци у кривичном поступку, изричито предвиђа увођење посебне специјализације свих актера кривичног поступка (судија који председава већем, јавни тужилац, истражни судија, полицијски службеник и пуномоћник оштећеног) у случају када се суди пунолетним учиниоцима за 27 таксативно набројаних кривичних дела (између осталог и за кривично дело: приказивање, прибављање и поседовње порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ), односно у свим оним случајевима када то процени специјализовани јавни тужилац. Такође, закон садржи нова доказна правила која су доживела значајне процесне модификације и то, пре свега, у светлу заштите малолетног оштећеног лица (усвојен 2005, у примени од 1. јануара 2006).

2.6 Организациони аспекти

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је ступио на правну снагу 25.7.2005. године (и уз измене 2009. године објављене у Службеном гласнику Републике Србије број 104-09) по први пут је и у домаћем законодавству дефинисан појам високотехнолошког криминала и то као:

вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.

2.6.1 ЦЕТС 185

Конвенција о сајбер или cyber криминалитету или како га наш законодавац терминолошки одређује, високотехнолошком криминалу донета је још 2001. године. Она пружа платформу за кривично-правне и процесне активности држава потписница. Домаћи процесно-правни оквир за пресретање садржинских података о комуникацијама садржан је у Законику о кривичном поступку (ЗКП). У погледу процесно-правних одредаба имамо систем који задржава шира претходно прописана овлашћења, са тенденцијом проширења њихове примене на новонастале и будуће случајеве. У пракси то значи да је за ефикасно обезбеђење и прикупљање доказа у вези са кривичним делима високотехнолошког криминала потребно тумачење и уподобљавање процесних механизама и радњи које, ни по интенцији креатора законских норми, ни по својој природи и намени, не одговарају конкретној процесној ситуацији у којој се примењују.

Механизам хитне заштите сачуваних рачунарских података предвиђен Конвенцијом (ЦЕТС 185) јесте инструмент који омогућава надлежним органима заштиту рачунарских података како би се обезбедило да не буду избрисани или на други начин компромитовани, пре него што се укаже прилика да буду обезбеђени за потребе кривичног поступка, посебно у погледу података о саобраћају који се

често аутоматски обришу у кратком временском периоду. У домаћим правним оквирима о примени овог механизма могло би се говорити кроз одредбе из чланова 152, 153, 154, 157 и 166, 178 Законика о кривичном поступку, односно о члановима 126, 128, 129 и 130 Закона о електронским комуникацијама (ЗЕК)[730]. У погледу привременог одузимања предмета у питању је чл.147 ЗКП[731].

Ове одредбе пружају могућност испуњења захтева Конвенције, али, ипак, не представљају потпун основ за хитну заштиту сачуваних рачунарских података. Одредба члана 166 односи се на писма, пошиљке и телеграме, који су материјални предмети, па се рачунарски подаци чија је заштита хитно потребна морају тумачити као „друге пошиљке", што је у пракси немогуће. Материјални облици документације захваћени су запленом списа или чл.155. Задржавање података од значаја је у надлежности Закона о електронским комуникацијама, конкретно у члановима 128, 129 и 130. У члану 286, који садржи листу (која није затворена) радњи, на које су у претткривичном поступку овлашћени органи МУП-а док нема прописивања неке од радњи предвиђених конвенцијом. Ово је и разумљиво јер није била интенција доносилаца Конвенције да ове радње обавља полиција већ да се на њих обавежу (у спровођењу, али не иницирању или надзору над спровођењем) пружаоци услуга.

Могућност надзора и снимања телефонских и других комуникација, прописана чланом 166, односи се на комуникације које се одвијају у реалном времену, али не пружа могућност обезбеђења, одређених, у прошлости насталих података, при чему се чак и не може примењивати на сва кривична дела високотехнолошког криминала, већ само на одређена, јер је поље примене ограничено само на кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела. Обавеза заштите целовитости рачунарских података у року не дужем од 90 дана и обавеза чувања тајности оваквог поступка, уопште није прописана нашим процесним законодавством. Ове обавезе су решене подзаконским актима изван процесне материје, што представља својеврсни српски парадокс. ЗЕК се поред описаног односи на ово, а посебно чланови 128 и 129, којима се дефинишу подаци који се имају задржати као и услови везани за овај поступак.

Интенција Конвенције у погледу мере хитне заштите и делимичног откривања података о саобраћају, јесте премошћавање раздвојености наредбе за хитну заштиту података и обавезе предаје таквих података. У домаћем законодавству одредбе већ поменутог члана 152, 155, 157, 158 односно 166, ЗКП-а, односно чланова 128 и 129 ЗЕК-а могле би се идентификовати као одредбе које одговарају овој мери Конвенције.

Лице које држи предмете из члана 147 ст. 1 и 2 ЗКП-а дужно је да органу поступка омогући приступ предметима, пружи обавештења потребна за њихову употребу и да их на захтев органа преда. Пре одузимања предмета орган поступка ће по потреби, у присуству стручног лица, прегледати предмете. (чл.148 ЗКП-а)

Лице које одбије да омогући приступ предметима, да пружи обавештења потребна за њихову употребу или да их преда, јавни тужилац или суд може казнити

730 Ивановић, З. Жарковић, М. Лајић, О. Криминалистичка разматрања дигиталних доказа, Криминалистичко–форензичка обрада места кривичних догађаја, стр.121-141, Тематски зборник радова, Криминалистичко–полицијска академија, 2013;

731 Ivanović, Z. Žarković, M. Scientific approach in building teams for seizure of digital evidence, pp. 399-413 in Thematic proceedings of international significance, Vol I, Academy of criminalistics and police studies, 2013, Ed. Goran Milošević;

новчано до 150.000 динара, а ако и после тога одбије да испуни своју дужност, може га још једном казнити истом казном. На исти начин поступиће се према одговорном лицу у државном органу, војном објекту, предузећу или другом правном лицу.

О жалби против решења којим је изречена новчана казна, одлучује судија за претходни поступак или веће. Жалба не задржава извршење решења.

Од дужности предаје предмета ослобођен је:

1) окривљени;
2) лице из члана 93 тачке 1 и 2 ЗКП-а, осим ако суд другачије не одлучи (члан 93 став 2).

Мера издавања наредбе је предвиђена чл. 16 ЦЕТС 185

Сврха мере издавања наредбе јесте да се надлежни органи једне државе овласте да лицима на својој територији или даваоцима услуга нареде да предају одређене податке које поседују или над којима имају државину (фактичку власт), односно да предају податке о претплатнику у вези са услугама које тај давалац услуга поседује или над којима има државину. Неспорна је чињеница да сва национална законодавства познају мере претресања и заплене у поступку обезбеђивања доказа, али код рачунарских података традиционалне мере могу створити низ компликација. Као што то исправно примећује Радуловић: „сасвим је извесна ситуација да се рачунарски подаци, који могу бити доказ у кривичном поступку налазе на серверу, што би значило да је применом традиционалне методе заплене потребно запленити цео сервер“. Мера хитне заштите и делимичног откривања података о саобраћају представљају значајан конкретизовани инструмент усмерен ка тачно одређеним рачунарским подацима и лицима која их поседују или контролишу. Домаће процесно право познаје само већ поменути члан 166 Законика о кривичном поступку који не одговара описаној сврси ове мере, јер је његова примена сведена на надзор комуникације која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки. Члан 155 прописује да ће се привремено одузети списи који могу послужити као доказ, пописати и запечатити и да њихов садржај не сазнају неовлашћена лица. Члан 170 прописује обавезу достављања материјала прикупљених применом одредбе о тајном надзору судији за претходни поступак и поступак у вези истих уколико се примењују, односно, не примењују као доказ у кривичном поступку. Посебно је значајна обавеза органа који је спровео радњу да поред описаног и дâ оцену о сврсисходности и резултатима примене мере надзора.

Привремено одузимање предмета регулисано је чл. 147 ЗКП-а. У предмете који се одузимају уврштени су и спадају и уређаји за аутоматску обраду података и уређаји и опрема на којој се чувају или се могу чувати електронски записи. Мера претраживања и заплене сачуваних рачунарских података надовезује се на привремено одузимање предмета и као разлог прописивања одредбама Конвенције може се разумети околност да национална законодавства често не покривају процедуре претресања и заплене у погледу података већ само, као што је речено, у погледу предмета. Мера предвиђена Конвенцијом која се односи на прикупљање података о саобраћају у реалном времену није регулисана у нашем Законику о кривичном поступку, она је регулисана ванпроцесним законодавством конкретно ЗЕК-ом. Ова мера омогућава надлежним органима да у реалном

времену прикупљају и снимају податке о саобраћају одређених комуникација пренетих преко рачунарског система. Оцењено је да је потребна управо оваква мера Конвенције јер пружа могућност надлежним органима да наложе прикупљање података о интернет саобраћају у реалном времену. Код нас се ова врста мере може довести у питање посредним тумачењем иницијатива за оцену уставности и законитости Заштитника грађана и Повереника за информације од јавног значаја и заштиту података о личнпости (чл.128 ЗЕК и Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији (Службени гласник РС, број 88/09), члан 13 став 1 у вези са чланом 12 став 1 тачка 6 и члан 16 став 2)

Мера пресретања података из садржаја надовезује се на претходну меру и такође даје могућност надлежним органима за поступање у реалном времену. Реч је о члану 166 ЗКП-а. По правилу, за меру коју ОУН одређују као претрага претресање и одузимање у окружењу аутоматизованих информационих система неопходна је наредба суда за претресање стана и осталих просторија или евентуално испуњење законом прописаних услова (ЗКП из чл. 158) како би се ушло у просторије у којима се рачунар налази (такође, сам рачунар се може изједначити са затвореним простором). „Претресање наређује суд писаном наредбом. Захтев за претресање и писана наредба, када су у питању кривична дела високотехнолошког криминала, треба да садрже следеће битне елементе:

- доказе, за које се очекује да ће бити прибављени путем претреса (носачи података, физичке јединице, врста података) треба разликовати по томе да ли је реч о средствима извршења или предметима прибављеним извршењем кривичног дела;
- техничке услове претреса. Рачунарски подаци су рањиви и не може се унапред предвидети са каквом техником осумњичени располаже и да ли постоје препреке код презервације и заштите доказа, нити која ће врста стручњака бити потребна да би се подаци заштитили од уништења. Стога, овај део мора бити унапред анализиран од стране органа гоњења, укључујући и формулисање захтева који треба да буде што прецизнији. Пракса је показала да се судски налози у овом делу у значајној мери ослањају на садржаје захтева за претресањем.

Са класичног правног аспекта за адекватно поступање постоји неопходност ове наредбе или испуњења датих законских услова за случај без наредбе. Већ у старту можемо наслутити које то проблеме ствара. Да би се наредба могла прибавити као неопходан услов, потребна је вероватноћа да се одређени предмети и трагови могу овим путем прибавити или да се може доћи до лица за којима се трага. У наредбу се уносе понаособ предмети, односно лица, који треба пронаћи. У погледу остваривања услова овде нешто вреди рећи, наиме с обзиром да се за претресање према ЗКП-у тражи вероватноћа проналаска ствари у погледу којих се доказном радњом претресања спроводи. У том смислу треба да постоји већи ниво сумње од основа сумње да се одређени садржаји, подаци, предмети налазе у објекту претресања, па се и изостанак таквих ствари треба третирати на адекватан начин. Овде већ можемо назрети који се све проблеми могу појавити – како прецизирати и тачно одредити све могуће трагове и предмете које желимо овим путем да прибавимо (у оваквим случајевима могуће је одузети и предмете који нису прецизно одређени наредбом, што је и регулисано ЗКП–ом, али се ту касније јављају многи други проблеми). Наравно, мањи је проблем у случају претресања без

наредбе. У овом погледу можемо истаћи да се у нашем законодавству помињу и као новина, о којој је већ било речи, која је унета у наше законодавство још изменама и допунама ЗКП -а из јула 2009. године, по којима се међу предметима који се привремено одузимају, уз потврду, убрајају и уређаји за аутоматску обраду података и опрема на којој се чувају или се могу чувати електронски записи. Дакле, уређаји за аутоматску обраду података су појам који може обухватити широк спектар ствари (па и хибридне мобилне телефоне), а посебно опрему за чување електронских записа. Лице које се користи овим уређајима и опремом дужно је да органу који води поступак, на захтев суда, омогући приступ и да пружи обавештења потребна за њихову употребу. Пре одузимања ових предмета, орган који води поступак ће у присуству стручног лица извршити преглед уређаја и опреме и пописати њихову садржину. Ако корисник присуствује овој радњи може ставити примедбе. Све поменуто односи се на право органа који предузима криминалистичке мере и радње да претреса и одузима (привремено) одређене ствари. Може се рећи да, за примену оваквих овлашћења од стране надлежних органа, одузимање одређених компоненти рачунара није проблем, јер се тако у неком каснијем тренутку, ове компоненте могу мирно прегледати у лабораторији или претраживати и прегледати њихови електронски садржаји. У питању су овлашћења која покривају физичке ствари или предмете који садрже електронске (дигиталне) садржаје и, формално, ова овлашћења експлицитно не садрже и право органа гоњења да разматра овакве доказе. Ово је случај са уређајима на којима се трајно записују одређени дигитални подаци. Већи проблем, према класичном концепту, може се појавити у случају привременог дигиталног записивања на одређеним уређајима. Ту се поставља питање да ли се овакви дигитални (или електронски) подаци могу сматрати предметима и траговима. Очигледно је да је наш законодавац изједначио, без икаквог обазирања, дигиталне (електронске) са материјалним доказима, у претходно наведеним изменама и допунама Законика о кривичном поступку. У теорији права принцип минимума принуде или пропорционалности чини незаконитим привремено или било какво одузимање различитих носача података у сврху прибављања веома малих, занемарљивих, количина података са њих. Шта више, овакви поступци могу проузроковати озбиљне последице и предрасуде у пословним активностима или у нарушавању приватности трећих лица. Посебни проблеми се могу појавити у случајевима када се за полицијску претрагу и анализу носилаца података (као на пример чипови, дискови који су фиксирани) мора користити систем у којем се подаци налазе. У свим описаним ситуацијама се, чак, могу створити и нови предмети и трагови, као на пример, одштампање одређене датотеке на штампачу, тако да се у овим случајевима може поставити и питање описаних овлашћења за претресање и одузимање, којим се стварају нови трагови или чак изводе одређени докази – одузимају се и папирни облици оваквог трага, чак, евентуални запис на неком од медија носача података (оптички диск, флеш-диск). „Последице незаконитог или неправилног претресања јесу процесне и материјалне природе. Са процесне стране, тако предузета радња је ништавна, осим ако је лице дало добровољни пристанак. Ако таквог пристанка лица нема, ни пронађени предмети се не могу користити као доказ у материјалном смислу, већ је реч о кривичном делу незаконитог претресања стана и противправног присвајања ствари. При томе, ЗКП прописује неколико услова под којима се може спровести претресање без наредбе суда, тако да је могућност грешке при спровођењу ове радње сведена на немар или

намерну грешку“. Описана конструкција зависи од питања да ли се приликом примене овлашћења претресања и привременог одузимања предмета подразумева и овлашћење примене техничких мера и средстава (опреме и лиценцирани програмских пакета) који припадају сведоку или осумњиченом лицу у циљу претраге или фиксирања података. Ретки су закони у упоредно-правној анализи који предвиђају примену свих неопходних мера у датом тренутку. Управо то значи да је у већини законских решења релативно неефикасна процедура аутоматске претраге рачунара и претресања рачунара у циљу проналаска одређених чистих података. Наш законодавац о томе ништа не говори, међутим у току писања овог рада донет је Закон о електронским комуникацијама којим се чланом 126 прописује да пресретање електронских комуникација, којим се открива садржај комуникације, није допуштено без пристанка корисника, осим на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Члан 127 прописује даљи поступак у вези са овом радњом, али се оставља простор да Министарство, по прибављеном мишљењу министарства надлежног за послове правосуђа, министарства надлежног за унутрашње послове, министарства надлежног за послове одбране, Безбедносно-информативне агенције и органа надлежног за заштиту података о личности, ближе прописује захтеве за уређаје и програмску подршку из става 4 овог члана.

Изнесене примедбе уновом ЗКП–у законодавцац је покушао да отклони, а колико успешно, то ћемо видети. Поред овога, у оквиру Министарства унутрашњих послова донета је обавезна инструкција о прикупљању и обезбеђењу електроснких доказа (26.2.2013. године бр. 01-1000/ 13 12). Оваква ситуација, у којој је најпозванија страна за прикупљање и обезбеђење електронских доказа МУП, значајно је добила на озбиљности и очувању ланца доказивања, подразумева стриктне процедуре у погледу проналаска, изузимања, похрањивања и чувања ове врсте доказа са различитих медијума, окружења и предмета (рачунара, мобилних телефона, мрежних окружења и друго).

Посебни проблеми се јављају код претресања (и евентуалног привременог одузимања предмета) у оквирима, раније помињаног, рачунарског мрежног окружења. Питање је да ли и у којој мери, претрага и претресање мреже обухвата, приликом претресања једног система повезаног на мрежу, и базе података које су са овим рачунаром повезане кроз инсталацију, а налазе се на некој другој локацији, али су доступне њему кроз мрежну везу. Ово питање има веома велику практичну вредност, јер се савремени извршиоци, веома често, користе складиштењем података на удаљеним и нашим полицијским снагама недоступним местима (сервери и складишта података у другој, страној држави). Описана ситуација повлачи са собом питање државине предмета и електронског материјала у виртуелном мрежном окружењу, које повлачи одређене последице, у зависности од схватања правне природе оваквог правног стања. Проблеми у оваквим случајевима сежу до питања међународног јавног права, али се најчешћа питања своде на питања међународног кривичног и кривично –процесног права. Посебна проблематика се тиче овлашћења претресања и привременог одузимања предмета у оквирима мрежних простора других држава кроз телекомуникационе системе, над којима друга држава нема надлежности. У већини земаља продор у дате системе снага или органа друге државе сматра се нарушавањем суверености државе, јер су они од стратешког значаја за државу, што се често инкриминише и то, најчешће,

највишим запрећеним казнама за таква дела. Ипак, у новије време, пројектују се изузеци. На међународном нивоу организују се најшире коалиције владиних и невладиних приватних сектора са циљем заштите од високотехнолошког криминала, којима се тежи остварити сарадња на овом плану у смислу директних приступа (или убрзаних индиректних и сличних модалитета сарадње) банкама података страних земаља кроз телекомуникационе мреже. Према ИТУ-овом приручнику за израду ВТК легислативе неопходно је размотрити и претраге у повезаним системима. Наиме, уколико разматрамо претраге које се у виртуелном свету простиру и на територије других држава, неопходно је предвидети и могућности спровођења оваквих претрага од стране других држава и њихових полиција (органа гоњења). Услови за ово су да се предмет претраге јавља доступним са: рачунара, система, програма или његовог дела, чији власник има приступ или могућност контроле, а за који постоји наредба за претресање (или сличан акт којим се омогућава претрага), па је зато неопходно дати легислативну могућност проширења претрага и кроз овакве могућности. У овом смислу посебно треба водити рачуна о: тзв. опен сорс (отвореним) изворима, који су свима доступни, без обзира где се налазе (па би било парадоксално постављати питање њиховог приступа од стране власти једне државе), али и јавно доступних похрањених података, програма, података о саобраћају комуникација и садржају истих, без обзира на чијој се територији налазе. Што се тиче привременог одузимања предмета оно се односи на претходно помињане дигиталне податке и подразумева следеће: заплену или слична средства за обезбеђење рачунара, рачунарског система или његовог дела, или медијума за похрањивање података; прављење и задржавање „имица“ (врсте идеалне електронске копије) помињаних података; очување интегритета ових података и обезбеђење документовања оваквог очувања интегритета путем примене средстава математичких алгоритама; изазивања прикривених или неприступачних података и њихово изузимање са рачунара (система). Управо у том правцу се ишло са примером из ИТУ–овог приручника за израду ВТК регулативе.

„Кад је реч о претресању лица у случају високотехнолошког криминала, ова радња се своди на проналажење физичких предмета од интереса за поступак, као што су мини-носачи информација (УСБ-меморија, медијумске картице и слично), предмети који на наведене носаче информација упућују или су, пак, писмени трагови у физичком облику“.

Следећи проблем је проблем тумачења у вези посебне заштите информација специфичног или осетљивог садржаја. Овде није реч само о информацијама везаним за специфичне професије (лекари – тајна према пацијенту, исповедници – тајна исповедања, адвокати – адвокатска тајна, новинари – новинарска тајна и заштита извора) већ представља посебно питање специфичних околности и ситуација у којима се могу органи гоњења наћи, везано за овакве професије и податке повезане са њима. Последње недоумице у погледу сличне тематике изазивају питања до којих граница сежу привилегије везане за новинарски позив у погледу е–ББС (electronic bulletin boards). Још интересантније је питање заштите и посебног третмана чланака, докумената и писама у области електронске поште и телекомуникационих система. Већина аутора сматра да оваква заштита мора бити аналогна оној материјалној неповредивости поште и писама уопште.

Посебно питање су сурогат резултати електронских доказа, креирани из електронског окружења и преведени у материјалне документе, нпр. копирани садржај електронског документа. У том смислу поставља се питање овлашћења

органа гоњења на стварање ових сурогата, а у односу на овлашћење прибављања њихових оригинала. Са друге стране, неограничавања овлашћења, sui generis, не само да обезбеђују легалитет и основ за потпуну и темељну истрагу у окружењу за електронску обраду података (ЕОП) већ, и у односу према правној политици, имају основ у аргументу, по којем је копирање података мање задирање у права и слободе људи, од привременог одузимања њихових носилаца. Шта више, оваква овлашћења имају предност у односу на друга, јер решавају специфичне проблеме мера претресања и привременог одузимања предмета, као што су накнада трошкова примене ЕОП система, касније брисање копираних података који више нису потребни у поступку или претраживање, претресање и привремено одузимање предмета у телекомуникационим мрежама.

„О предузетим радњама обавезно је сачинити записник. Овај записник је битан код ВТК, јер управо пронађени докази, трагови и предмети морају бити и технички детаљно описани, што обезбеђује каснију независну експертску проверу, а да би се избегло и довођење у питање идентичности предмета и предузетих радњи. У том смислу, досадашња пракса снимања саме радње претресања, уз јасно одређивање идентитета учесника и предузетих поступака, показала се као максимално ефектна. Сви учесници потписују записник о претресању и имају право да уложе примедбе, које се морају унети у записник, а записнику се прикључују и скице, фотографије, снимци, планови и слично“. Такође је од значаја прављење и службених белешки о поступању са оваквим траговима у дигиталном окружењу, уз додатну употребу софтвера који ово омогућавају од оних који су опен сорс као, на пример, додатак за браузере Фајер шот (FireShot), којим се могу документовати све врсте активности (овлашћених службених лица полиције, али и осумњичених у реалном времену) од значаја у датом окружењу.

Наша држава прописује ЗКП–ом могућност и одбране ћутањем, али и неке друге основе ограничења дужности сведочења (искључење и ослобођење од сведочења). Нарочито је интересантна обавеза сведочења у земљама у којима постоји могућност да сведок освежи своје памћење увидом у списе, књиге, писма и предмете који су му на располагању, као и да саставља белешке о њима и да предмете донесе на суд, а и да користи овакве белешке на суду приликом излагања (у које спада и наша држава).

Обавеза сведочења не може се екстензивно тумачити на штету сведока и не садржи у себи и обавезу да се одређени постојећи дигитални трагови у рачунару одштампају и предају надлежном органу. Овај закључак произилази из чињенице да се од сведока очекује да изнесе све што је њему познато о догађају, а не и да проналази предмете и трагове кривичног дела нити да их на било који начин ствара. Он не сме преузети улогу вештака и других стручних лица као помоћних органа у расветљавању криминалног догађаја. Ово је још интересантније када посматрамо упоредно правно случајеве у којима се сведочење одвија за различите земље. Обично се саслушање (или испитивање како наглашава наш ЗКП) сведока обавља тек у каснијој фази поступка. Ово су случајеви када се сведочење обавља пред судом, међутим, постоје и земље које су усвојиле концепт тужилачке истраге, код којих се саслушање спроводи, евентуално, од стране јавног тужиоца, изузетно од стране полиције. Поменуто питање је од већег значаја за разматрање када се ова дужност јавља у претходној истрази и у преткривичном поступку, него у фази суђења. Наша земља је у кругу ових земаља од јануара 2012. ступањем на снагу новог ЗКП.

Веома су интересантна новија решења у пракси појединих држава, као на пример Велике Британије која својим законом о полицији и кривичним доказима (the police and Criminal Evidence Act 1984) даје овлашћење позорнику (популарном „бобију“, припаднику униформисане полиције) да може захтевати да му се податак постојећи у рачунару, ком се може приступити из дате просторије изда у облику (што обухвата и штампање на папиру) који омогућава да таква информација буде видљива, легитимна и да се може изнети из таквих просторија. У Канади Закон о узајамној правној помоћи (Mutual Legal Assistance Act) даје могућност наредбе за прикупљање података и доказа, која се издаје на име одређеног лица „које може копирати одређене евиденције или сачинити евиденције по основу постојећих података и са собом понети копију такве евиденције“.

Оваква могућност додатно отвара питања домашаја постојећих дужности предаје података и њиховог физичког отелотворавања у облику одштампаног материјала или слично томе. Нарочито је значајно разматрање доступних података преко мреже, којим се обухвата прикупљање и одузимање података који се физички налазе на територији друге државе. Да ли овакве наредбе могу имати тако велики домашај и да ли се са друге стране неко лице може обавезати да прибави податке из друге државе? Мислимо да не. Шта више, нејасно је питање када лице може одбити да сарађује у погледу предаје оваквих предмета и трагова. Питање да ли у дужност предаје предмета може ући и обавеза предаје посебних предмета, у којима би се материјализовала дигитална информација, податак или траг, односно приступа месту где се предмети налазе, веома је комплексно. Приликом предвиђања норми којима се поменуто регулише de lege je ferenda, исте се морају прецизно дефинисати. Неопходно је да се у таквим случајевима диференцирају овлашћења, обавезе и дужности осумњичених или окривљених лица и сведока. У погледу добронамерних сведока овакве обавезе не представљају неки већи проблем, осим што се од њих захтева већ поменуто, излажење из сфере познатог у сферу у којој се креира нова ствар, која се касније може користити као доказ. Са друге стране, оваква обавеза, која би се наметнула осумњиченом или оптуженом, нарушавала би њихово право на одбрану ћутањем, као и право да се не инкриминише сопственим актима. Овим би се прекршила Међународна повеља о грађанским и политичким правима, тачније њен чл. 14 (3) којим се гарантује да, у случају утврђивања било каквог оптужног акта или кривичног гоњења, као минимум поштовања права се одређује да „нико не може бити натеран да сведочи против себе нити да призна кривицу“.

Члан 22 Конвенције о ВТК бави се надлежношћу државе-потписнице када дође до извршења неког од кривичних дела из Конвенције. Држава ће имати надлежност за процесуирање према територијалном принципу (уколико је кривично дело учињено на њеној територији, на броду или авиону који носи њену заставу), у комбинацији са принципом персоналне јурисдикције (као и ако је кривично дело учинио држављанин те државе, под условом да је оно у другој држави која познаје исту такву инкриминацију или ван државних територија (нпр. на слободном мору). Ипак, високотехнолошки криминал измиче класичним обрасцима кривичних дела, па и кривичне надлежности, тако да оваква формулација оставља низ отворених питања. Ситуацију даље компликује став 2 истог члана, који омогућава државама да примене изузетке на овако описане принципе надлежности у одређеним случајевима или под одређеним околностима. Ставови 3 и 4, уводећи принцип универзалне јурисдикције прописују да, ако држава не изврши екстрадицију свог

држављанина, мора му судити за учињена дела на територији друге државе-потписнице. Такође, одредбе о надлежности државе, садржане у Конвенцији, неће имати примат над одредбама домаћег права, према којем држава може и на неки други начин успоставити своју надлежност. Веома је значајно размотрити концепт који нуди ИТУ–ов приручник за легислативу ВТК у овој области. Он поставља оквире за посебно формулисање процесне јурисдикције, омеђавајући је следећим предлозима да једна држава има надлежност над процесирањем дела: 1. уколико су извршена на њеној територији, 2. уколико су извршене средствима – опремом, програмом или подацима која се налазе на њеној територији, без обзира где се извршилац налази или 3. која су усмерена на опрему, програме или податке која се налазе на њеној територији, без обзира где се извршилац налази. Ова решења су и више него прихватљива за наш систем, али нису предвиђена нашим прописима. Принципи које предлаже ИТУ, везано за ваздухоплове и пловила, у погледу јурисдикције су идентични класичним, док код примене принципа lex nationalis предлажу допуне: надлежност ће засновати 1. уколико је дело кажњиво према закону државе на чијој територији се десило као и 2. када је извршено изван територијалне надлежности било које државе. У оквиру предлога о надлежностима ИТУ интересантно предлаже и договорну надлежност у случајевима позитивног сукоба надлежности. Што се месне надлежности тиче она се заснива на сваком месту где је: 1. учинилац радио или био дужан да ради и био физички присутан, као и 2. место са којег је умишљајно коришћен уређај, програм или податак или 3. свако друго место са чије локације је проузрокована последица кривичног дела или је према умишљају учиниоца требала бити проузрокована. Овакво решење помера постојеће границе у материји кривично-процесног права, у позитивном смеру.

2.6.2 Међународна сарадња држава на сузбијању ВТК

Трећи део Конвенције се бави међународном сарадњом држава на сузбијању високотехнолошког криминала, прописујући опште принципе чл. 23 међународне сарадње, у чл. 24 опште екстрадиционе принципе, чл. 25 опште принципе у пружању узајамне правне помоћи, чак и у случајевима изостанка примењивих међународних споразума (чл. 27). Члан 26 говори о сарадњи држава на организованој или спонтаној размени података који се тичу евентуалног извршења неког од кривичних дела везаних за употребу електронских комуникација. Такође чланови 29 и 30 баве се и експедитованим очувањем похрањених рачунарских података на међународном плану и експедитованим откривањем очуваних података о комуникационом саобраћају, опет на међународном нивоу. Посебно се чл. 31 бави приступом похрањеним рачунарским подацима у оквиру пружања међународне правне помоћи, а чл. 33 и 34 покривају прикупљање података о саобраћају у реалном времену и пресретање садржине података на међународном нивоу. Члан 35 уводи, у циљу омогућавања хитног поступања, посебно у случајевима очувања података о комуникацијама у другим државама, мрежу 24/7 тачака за контакт. Она је замишљена и као подршка полицијским и другим органима, као контакт за сва обавештења и почетна тачка за све захтеве који се тичу процесуирања и истраживања кривичних дела високотехнолошког криминала. Државама је остављено да у пракси, додатним

билатералним споразумима, даље прецизирају оне врсте сарадње за које постоји посебан интерес.

Конвенција је специфична по једном, нимало позитивном аспекту, који смо могли назрети раније у тексту – специфичност споре ратификације од стране развијених држава. Од земаља које можемо назвати високоразвијеним када је реч о савременим технологијама, ратификовале су је само САД (2006. године), Француска, Данска и Норвешка. Нису је ни потписале Монако, Русија (која је, децидно, у августу 2009. године одбила да се придружи потписницама) и Сан Марино. Са друге стране, интересантно је да је, у оквирима ЕУ, нису ратификовале Грчка, Ирска, Пољска, Шведска, Лихтенштајн, Луксембург и Монако, иако су је потписале. Чему овакво поступање? Неки аутори наводе као разлог поменута процесна овлашћења државних органа, које Конвенција предвиђа и готово не ограничава. Многи критичари указују на негативне особине Конвенције, из најразличитијих разлога.

Четврто поглавље Конвенције садржи завршне одредбе. Оно је од посебног интереса за земље које нису чланице СЕ, јер се њиме омогућава да споразуму о примени Конвенције приступе и државе које нису у СЕ.

Додатни протокол (ETC 189) уз Конвенцију ВТК

Године 2003. донет је додатни протокол уз Конвенцију ВТК. Он се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система и ступио је на снагу 1. марта 2006. године. Од земаља у окружењу, ратификовале су га Албанија, Босна и Херцеговина, Хрватска и Македонија, Црна Гора и Румунија. Грчка га није ратификовала, као што није ни основну Конвенцију.

Циљ усвајања протокола био је инкриминисање понашања необухваћених Конвенцијом, а која се односе на ширење мржње, нетолеранцију и нетрпељивости према расним, националним, верским и другим групама и заједницама, коришћењем рачунара, рачунарских мрежа и система као средства комуникације и ширења различитих облика мишљења, али и пропаганде. Активности о којима је реч носе са собом велику друштвену опасност због немогућности контроле доступности и растурања веома запаљивих садржаја. Овде не говоримо о праву на јавно изражавање мишљења, већ је у питању веома комплексан феномен, који са собом носи злоупотребу овог, али и других права на интернету или на некој другој мрежи, коришћењем рачунара, где је могућност реаговања адекватних органа значајно умањена. Протокол је, пре свега, усмерен на инкриминацију и кажњавање оваквих испада, без обзира да ли се њима шири мржња, нетрпељивост или се историјске чињенице представљају на неистинит начин, или се неким другим средствима дискриминише или ниподаштава одређена национална, расна, верска група или организација која их представља.

Аутори протокола се у преамбули позивају на Европску конвенцију о људским правима и основним слободама, Протокол 12 уз Европску конвенцију којим се забрањује сваки вид дискриминације појединаца или група на основу њихових заштићених личних својстава, и Конвенцију о елиминацији свих облика расне дискриминације, донету 1965. у оквиру Уједињених нација.

Протокол инкриминише следећа понашања:

- ширење расистичког и ксенофобичног материјала путем рачунарских система подразумева сваку радњу, којом се овакав материјал чини доступним јавности, коришћењем рачунара или рачунарског система. Државама је остављена слобода да одлуче да ли ће овакав поступак бити уведен у кривично законодавство (инкриминисан) и дата им је могућност стављања резерве на оне облике понашања за које се према унутрашњем праву може сматрати да представљају вид изражавања слободе говора;
- претња мотивисана расизмом или ксенофобијом представља стављање у изглед групи или појединцу, озбиљном претњом извршења неког тешког кривичног дела, на начин дефинисан у домаћем законодавству држава, коришћењем рачунара или рачунарских система. Како би ово дело имало специфичан облик предвиђен Протоколом, неопходно је да се лице или група издвајају према својој раси, боји коже, пореклу, националној, етничкој или верској припадности;
- увреда мотивисана расизмом или ксенофобијом - у питању је увреда појединца или групе, заснована на раси, боји коже, пореклу, националној, етничкој или верској припадности. Држава може ставити резерву на овај члан у потпуности, или може ограничити инкриминацију само на оне увреде којима се шири мржња, или се појединац, или група, понижавају или извргавају подсмеху. Вероватно је специфичност интернета и различитост комуникације на њему, уз комбинацију права на слободно јавно изражавање мишљења, омогућила да се у Протоколу на овакав начин дефинише ово дело;
- порицање, значајно умањење, одобравање или оправдање геноцида или злочина против човечности. Основни услов за вршење овог кривичног дела је да се овакав садржај мора, на неки начин, учинити доступан јавности, дакле, већем броју људи који користе рачунар и интернет или другу рачунарску мрежу. У овом делу предмет извршења јесу случајеви који су били предмет одлучивања од стране међународних кривичних судова, почев од Међународног војног трибунала 1945. године у Нирнбергу, преко Токијског процеса 1946. године, па надаље, а што имплицира и кривична дела као предмет одлучивања Трибунала за ратне злочине на територији бивше СФРЈ, као и Руанде, Међународног Кривичног суда у Риму.

Решења о имплементацији, процесним радњама и међународној сарадњи која садржи Конвенција, сходно се примењују и на дела која су утврђена Протоколом.

2.6.3 Конвенција о правима детета

Ратификацијом Конвенције о правима детета земље уговорнице су се, између осталог, обавезале да свако дете заштите од експлоатације и од обављања било ког посла који би могао да буде опасан по живот и здравље детета, односно који представља угрожавање и/или повреду његовог физичког, емотивног и

сексуалног интегритета. Потврђивањем Конвенције о правима детета (у даљем тексту КПД) наша земља је преузела обавезу да предузима мере у циљу спречавања насиља над децом и обезбеђивања заштите од свих његових појавних облика (у породици, институцијама, широј друштвеној средини, итд.). Такође, земље уговорнице су се обавезале да осигурају мере подршке за физички и психички опоравак детета – жртве свих облика експлоатације, као и да осигурају социјалну реинтеграцију, односно обезбеде интеграцију детета у нову социјалну средину (чл. 39 КПД).

Факултативни протокол уз Конвенцију о правима детета, о продаји деце, дечјој проституцији и дечјој порнографији (у даљем тексту Протокол) обавезује државе уговорнице, поред осталог, да усвоје одговарајуће мере за заштиту права детета, жртава радњи забрањених Протоколом у свим фазама кривичног поступка (чл. 8), а нарочито:

- признавањем угрожености деце-жртава и прилагођавањем поступака да би се уважиле њихове посебне потребе, укључујући њихове посебне потребе као сведока;
- обавештавањем деце-жртава о њиховим правима, њиховој улози и обиму, временском распореду и напредовању поступка и разматрању њихових случајева;
- допуштањем да се у поступку у ком су угрожени њихови лични интереси презентирају и размотре гледишта, потребе и преокупације деце-жртава, на начин који је у складу са правилима националног процесног права;
- обезбеђивањем одговарајућих служби подршке деци-жртвама током читавог правног процеса;
- заштитом, када је то одговарајуће, приватности и идентитета деце-жртава и предузимањем мера у складу са националним правом како би се избегло неподесно ширење информација које би могле довести до идентификовања деце жртава;
- обезбеђивањем, у одговарајућим случајевима, безбедности деце-жртава, као и безбедности њихових породица и сведока који сведоче у њихово име, од застрашивања и одмазде;
- избегавањем непотребног одлагања разматрања случајева и извршавања налога или уредби о давању обештећења деци жртвама.

Такође, у смислу Протокола "државе уговорнице ће обезбедити да неизвесност у погледу стварне старосне доби жртве не спречи покретање кривичног поступка, укључујући истражне радње усмерене на утврђивање старосне доби жртве, да у поступању од стране система кривичног правосуђа, са децом-жртвама незаконитих радњи описаних у овом Протоколу, најбољи интерес детета буде приотитет". Државе уговорнице предузеће, такође, мере како би обезбедиле одговарајућу обуку, посебно правну и психолошку, за лица која раде са жртвама незаконитих радњи забрањених према овом Протоколу и усвојити мере како би заштитиле безбедност и интегритет лица и/или организација укључених у спречавање и/или заштиту и рехабилитацију жртава таквих незаконитих радњи.

Конвенција МОР бр. 182 о најгорим облицима дечјег рада, усвојена 1999. године у Женеви, заједно са Препоруком 190 која се односи на забрану и директно деловање ради укидања најгорих облика дечјег рада, такође је од огромног значаја за ову област. Овај међународни уговор односи се на све особе млађе од 18 година

и обавезује стране уговорнице да предузму хитне и ефикасне мере којима ће се обезбедити забрана и укидање најтежих облика дечјег рада.

Државе уговорнице Конвенције Савета Европе о заштити деце од сексуалне експлоатације и сексуалног злостављања обавезале су се на предузимање неопходних законодавних и других мера у смислу санкционисања:

а) производње дечје порнографије;
б) нуђења или стављање на располагање дечје порнографије;
в) дистрибуције или преноса дечје порнографије;
г) набављања дечје порнографије за себе или другу особу;
д) поседовања дечје порнографије;
е) односно свесно прибављање приступа, преко информационо-комуникационих технологија, дечјој порнографији (чл. 20 Конвенције о заштити деце од сексуалне експлоатације и сексуалног злостављања).

Такође, овај документ изричито обавезује државе уговорнице и на предузимање неопходних законских и других мера у смислу установљавања посебног кривичног дела "учешће детета у порнографским наступима" (чл. 21). Као радње извршења овог кривичног дела предвиђене су:

а) регрутовање детета за учешће у порнографским наступима или узроковање да дете учествује у таквим наступима (ст. 1а);
б) приморавање детета да учествује у порнографским наступима или стицање користи од таквих наступа, или на други начин експлоатисање детета у такве сврхе (ст. 1б);
в) свесно присуствовање порнографским наступима у којима учествују деца (ст. 1ц - потписнице могу да задрже право у целости или делимично да не примењују ст. 1ц).

На основу овог документа државе уговорнице су се обавезале и да ће се постарати да жртвама: 1) од првог контакта са надлежним органима, буду доступне информације о релевантним судским и управним поступцима, усклађене са њиховим старосним добом и зрелошћу и на језику који разумеју; 2) буде доступна, бесплатна правна помоћ, када могу да имају статус странке у кривичном поступку; 3) као и да ће предвидети могућност да правосудни органи именују специјалне представнике жртава када носиоци родитељске одговорности не могу да представљају дете због сукоба интереса у односу на дете.

3. НАУЧНО ИСТРАЖИВАЊЕ У ОКВИРУ ПРОЈЕКТА

3.1 Узорак

Узорак ове анкете у оквиру истраживања твининг-пројекта је чинило 48 испитаника оба пола, различитих старосних доби, занимања, економског статуса и друдо. У одабиру узорка се водило рачуна да буде довољан број испитаника, али је обраћана пажња и на то да расподела испитаника не буде крајње диспропорцијална по полу и другим критеријумима. Узорак су чинили припадници полиције, УГП-а и СБПОК-а, Одељења за борбу против ВТК, Вишег јавног тужилаштва у Београду односно Тужилаштва за ВТК, као и одређене судије. Упућеност и

познавање материје о ВТК и ирегуларним миграцијама и трговини људима није неопходно образлагати. Узорак је према свим анализама свеобухватан по свим критеријумима. По многим критеријумима он није репрезентативан за популацију, већ је више вођено рачуна да он буде паритетан и да структура узорка дозвољава поређења и укрштања са другим критеријумима.

3.2 Анализа резултата

Спроведено истраживање о појавним облицима високотехнолошког криминала у Србији, обухватило је, поред анкете намењене општој популацији, и анкету коју су попуњавали представници надлежних органа за борбу против високотехнолошког криминала у оквиру Службе за борбу против организованог криминала, Управе криминалистичке полиције, Управе граничне полиције, Посебног тужилаштва за борбу против високотехнолошког криминала при Републичком јавном тужилаштву и неколицину судија који су водили поступке из ове области. Испитивање је било анонимно и временски није било ограничено. Сакупљени подаци су обрађивани статистичком анализом у програмима SPSS и Microsoft Exel.

Напомена: На сва питања анкете било је могуће заокружити више одговора.

Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију као кривично дело из чл.185 КЗ према Вашим сазнањима обухвата:

Табела 1. Питање бр.1 анкете

	n	% упитника
а. лица до 14 година	41	85.42
б. лица 14 -18 година	40	83.33
в. лица 14-16 година	16	33.33
г. лица 18 -21 година	1	2.08
д. не знам	1	2.08

Због редоследа понуђених одговора, као и преклапања понуђених старосних категорија, на појединим анкетама је одговарано навођењем нове опције до 18 година, што је интерпретирано као понуђене старосне категорије под а, б, в.

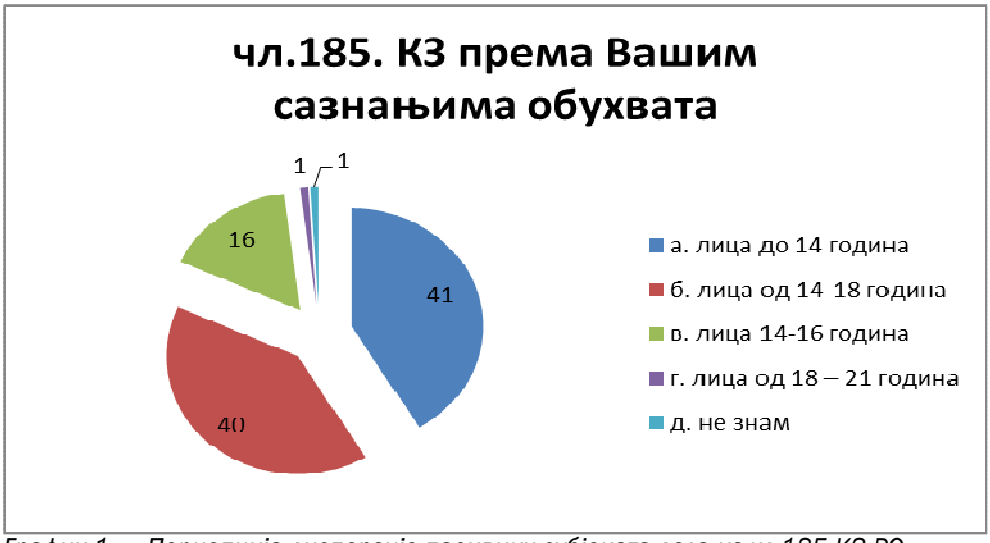


График 1. Перцепција дисперзије пасивних субјеката дела из чл.185 КЗ РС

Питање бр.1 имало је за идеју да прикаже перцепцију фокус-група које обухватају полицајци, тужиоци (заменици и сарадници) и судије овог кривичног дела и да укаже у најдаљем домашају проценат оних који имају релативно померену перцепцију у односу на пасивне субјекте овог кривичног дела. Као што се из резултата може приметити перцепција је дисторзирана у веома малом проценту испитаника – који носе 2.08%, који су дали одговор да КД из чл.185 обухвата лица од 18 до 21 година. У бројкама је у питању један испитаник што је на укупан проценат занемарљива бројка. Са друге стране, могли смо видети и фокусирање на године пасивних субјеката од стране испитаника, па тако имамо 41 испитаника, што укупно чини 85.42%, који указују на апсолутну заступљеност лица до 14 година као пасивних субјеката дела. Затим можемо приметити да 40 испитаника (83.33%) указују на присуство узраста 14-18 година, као и уже узрасно опредељење од 16 испитаника (33.33%) који указују да су се у њиховој пракси сусрели са узрастом од 14 до16 година. Према резултатима можемо закључити да су заступљени сви битни узрасти, са благом предношћу узраста деце (до 14 година), али и веома интересантан резултат, иако он представља занемарљив део студије од 2,08%. Његова интересантност се може тумачити и као тежња покушају инкриминације у наше законодавство приказа порнографског материјала особа које личе популацији малолетника, а обухватају популацију млађих пунолетних лица. О томе се може расправљати, али можда је ипак бољи пут дефинисање кроз термине „особе која, без обзира на узраст, својим изгледом подсећа на особу млађу од 18 година“ или нешто слично. Но, овако конципиран и анализиран резултат указује на могућност побољшања ове регулативе у том правцу, а посебно у светлу имплементације Конвенција СЕ и ОУН у овој области.

Ово дело се може вршити и у оквиру:

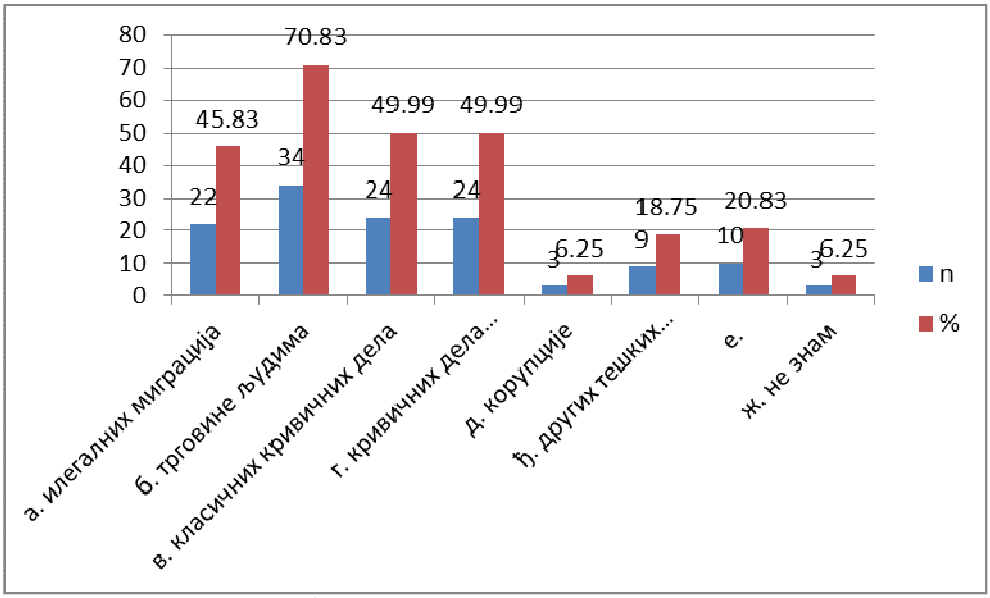


График 2. Перцепција области криминалитета у коју спада дело из чл.185 КЗ РС

Испитаници су перципирали дело из чл.185, првенствено у области криминалитета чије је главно дело кривично дело трговине људима, њих 34 (или 70,83%), затим у области организованог криминала - 24 испитаника (49.99%), колико их је указало на то да по њиховој перцепцији ово дело спада у област класичног криминалитета. Следеће области према перцепцији испитаника су биле област илегалних миграција - 22 испитаника (45,83%), других тешких кривичних дела - 9 испитаника (18.75%), корупције - 3 испитаника (6.25%) као и 3 испитаника који су одговорили да не знају. Значајно је приметити и да 10 испитаника (20.83%) није одредило област у којој перципирају ово кривично дело. Резултат перцепције је разумљив и у светлу приказа структуре испитаника, с обзиром да је већина испитаника припадника полиције из УКП-а СБПОК-а или УГП-а, као и генералног позиционирања овог дела у области дела организованог криминала, али је од значаја и укупна бројка од око 27%, који ово дело нису могли сврстати у понуђене области криминалитета.

Табела 2. Питање бр. 2

	n	%
а. илегалних миграција	22	45.83
б. трговине људима	34	70.83
в. класичних кривичних дела	24	49.99
г.кривичних дела организованог криминала	24	49.99
д. корупције	3	6.25
ђ. других тешких кривичних дела	9	18.75
е.	10	20.83
ж. не знам	3	6.25

Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду.

Табела 3. Питање бр. 3

	n	%
продајом, приказивањем или јавним излагањем или на други начин чињење доступним текстова, слика, аудио-визуелних или других предмета порнографске садржине малолетнику или приказивањем порнографске представе малолетнику	21	43.75
искоришћавањем малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу	20	41.67
дело из ст. 1 и 2 овог члана вршено према детету,	14	29.17
прибављањем за себе или другог, поседовањем, продајом, приказивањем, јавним излагањем или електронски или на други начин чињењем доступним слика, аудио-визуелних или других предмета порнографске садржине настале искоришћавањем малолетног лица	26	54.16
Није их било	13	27.08

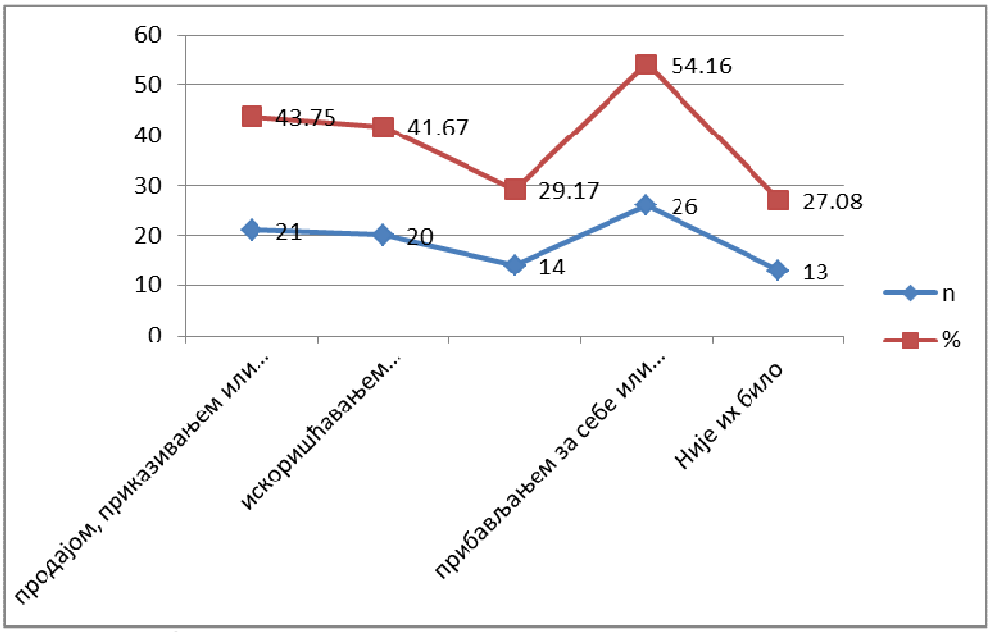


График 3. Облици дела из чл.185 КЗ РС

Питање бр.3 ишло је ка прибављању информација о заступљености појавних облика овог кривичног дела у пракси. У том смислу за испитанике најчешће примећени облик био је: прибављањем за себе или другог, поседовањем, продајом, приказивањем, јавним излагањем или електронски или на други начин чињењем

доступним слика, аудио-визуелних или других предмета порнографске садржине настале искоришћавањем малолетног лица, који је перципирало 26 испитаника (54.16%). У овом смислу, први основни облик се појављује као најчешћи облик овог дела, при чему није рађена даља диференцијација како би се утврдио најзаступљенији начин у оквиру овог облика. За њим следи: продајом, приказивањем или јавним излагањем или на други начин чињењем доступним текстова, слика, аудио-визуелних или других предмета порнографске садржине малолетнику или приказивањем порнографске представе малолетнику које је приметио 21 испитаник (43.75%), а потом: искоришћавањем малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу, које је приметило 20 испитаника (41.67%). Посебно интересантно је тумачити резултат овог питања који перципира облик када је ово кривично дело извршено према детету, 14 испитаника (29.17%). На крају је присутна перцепција по којој ових кривичних дела није било у њиховој пракси: 13 испитаника (27.08%).

Анализом овог одговора можемо утврдити да је, што се проактивног приступа тиче, неопходно деловати у правцу првог основног облика. Као препоруку можемо дати рад на превенцији стварања случајних фотографија и других облика материјала о искоришћавању деце и малолетника у порнографске сврхе. Едукативна улога школа и других образовних институција је од значајног утицаја у овом погледу, неопходно је направити широку мрежу невладиних и владиних агенција, органа и организација које пружају различите облике савета и едукативних активности међу популацијом која је најугроженија у овом смислу. Као резултат ове анкете јавља се пинпоинтовање групе деце и млађих малолетних лица као најбројније фокус-групе од интереса за деловање у проактивном смислу.

Да ли има оних појавних облика који нису обухваћени законом?

Табела 4. Питање бр. 4

	n	%
а. да	9	18.75
б. не	7	14.58
в. не знам	30	62.50

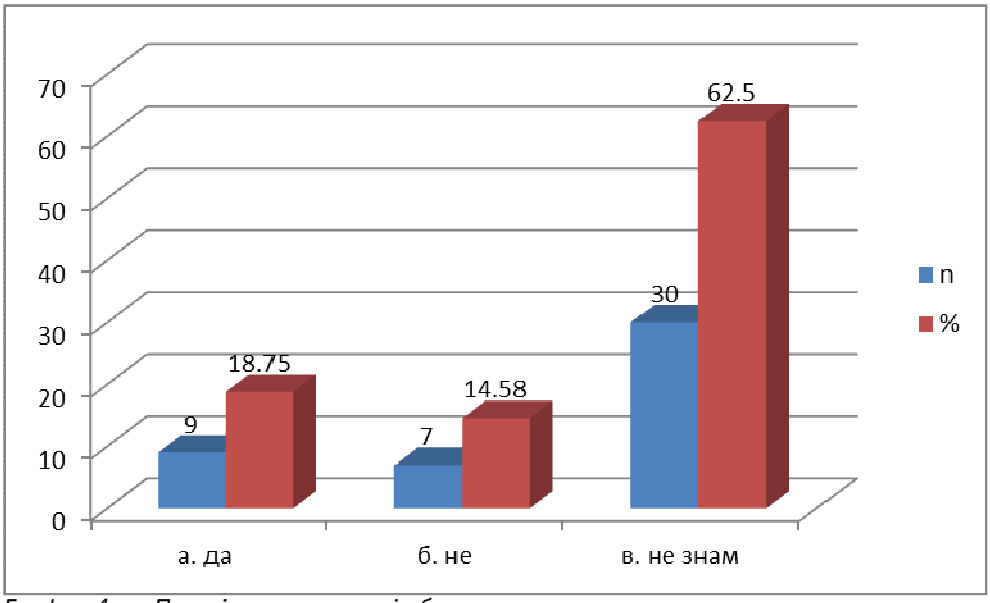


График 4. Постојање радњи које би се могле инкриминисати

Ово питање било је замишљено као покушај да се од праксе добије некакав вид предлога за измену легислативе у овој области као пројекција проблема до којих долази у практичној примени норми, па су и резултати у складу са тим околностима. Тако можемо приметити да 37 испитаника (77.08%) не види постојање облика кривичног дела који нису инкриминисани, док њих 9 (18.75%) такво нешто перципира. При том се од њих нису захтевали појединачни облици о којима би се разматрало, али овај резултат може бити водиља у спекулисању о присуству одређеног, а ипак не занемарљивог броја понашања која би се могла класификовати као криминогена а која нису инкриминисана. У том смислу могуће је и даље истраживање у продубљивању анализе понашања и радњи које би се у том смислу могле додатно инкриминисати. Као основни циљ овог питања је препозната перцепција испитаника који представљају најадекватнију и довољно репрезентативну популацију за испитивање ове проблематике, с обзиром да су они најпозванији да о њој расправљају. У питању су лица која директно примењују законске норме из ове области на конкретне случајеве у пракси.

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела?

Табела 5. Питање бр. 5

	n	%
све расположиве	7	14.58
мониторинг интернет саобраћаја, тј. фајлова који садрже аудио-визуалне сцене сексуалног злостављања деце и малолетника	1	2.08
рачунари	1	2.08

примена софтвера који омогућавају идентификацију картица	1	2.08
не	1	2.08
мере надзора интернета и телефона	1	2.08
примена посебног софтвера	1	2.08
контрола интернета	2	4.17
не знам	1	2.08
интернет, мобилна и фиксна телефонија	5	10.42
интернет	2	4.17
све врсте писаних и електронских медија у циљу едукације грађана и све врсте доступних ИТ које могу допринети откривању и проналажењу доказа за несметано вођење поступка	1	2.08
ми смо запослени у ОТ, а ово је у надлежности ВТК	1	2.08
контрола друштвених мрежа на интернету и претрага огласа сумњиве садржине	1	2.08
бесплатан Микрософтов програм "PhotoDNA", "NetCleanAnalyze", sistem "ChildExploatationTracking System (CETS)" - глобални програми за полицију и тужилаштво	1	2.08
ТВ, интернет, други медији	1	2.08
све доступне	1	2.08
медији	1	2.08
друштвене мреже, интернет	1	2.08
није унето	17	35.42

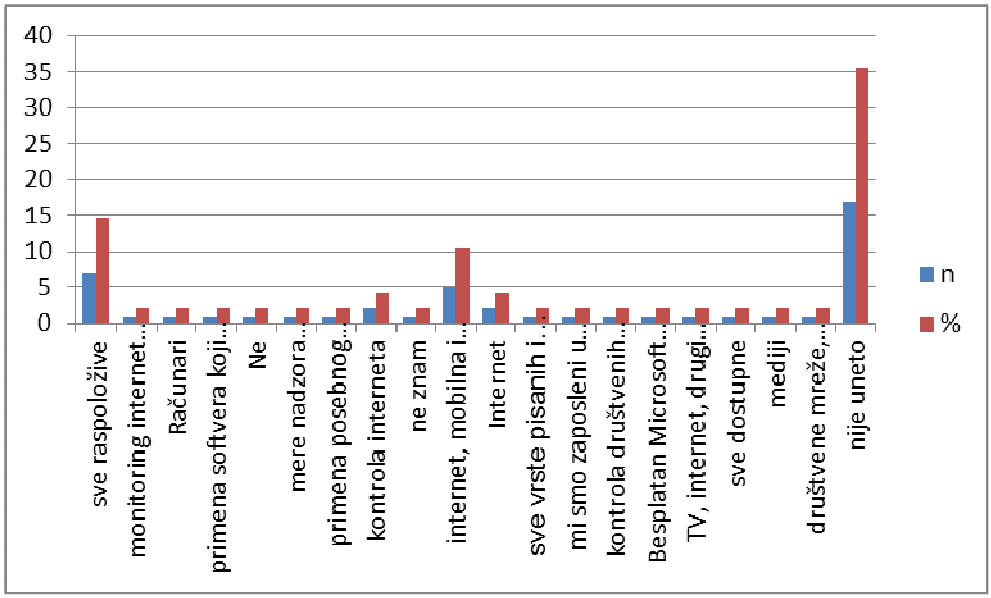


График 5. Предлози ИКТ у расветљавању и откривању дела

У вези са питањем бр. 5 замишљено је да практичари из својих аспеката дају предлоге могуће примене одређених ИКТ које се у том правцу могу користити у расветљавању и откривању ових дела. Такође је од значаја да код овог питања није било битно већинско опредељење већ предлози који могу бити од важности за будуће случајеве у пракси. Тако можемо приметити да један испитаник (2,08% укупног броја испитаника) указује на бесплатан Microsoft програм "PhotoDNA", "NetCleanAnalyze", систем "ChildExploatationTracking System (CETS)" - глобални програми за полицију и тужилаштво, а други на мониторинг интернет саобраћаја, тј. фајлова који садрже аудио-визуалне сцене сексуалног злостављања деце и малолетника и по један на мере надзора интернета и телефона, или примену посебног софтвера или контролу интернета. Генерално већина указује на веће коришћење свих врста писаних и електронских медија у циљу едукације грађана, као и на све врсте доступних ИТ које могу допринети откривању и проналажењу доказа за несметано вођење поступка, као и на контролисање друштвених мрежа на интернету и претраге огласа сумњиве садржине. Као резултат анализе овог питања можемо препознати две целине за разматрање препорука у даљим активностима, једна коју чине одређене групе софтверских облика помоћи у истрагама и у расветљавању кривичних дела као и хватању учинилаца, али и у идентификацији жртава кривичних дела у области илегалних миграција, трговине људима и ВТК. Могуће је препознати и другу целину која би се односила на ОСИНТ[732], а коју је практичарски пул нашег узорка дефинитивно подвукао као основни извор информација и средстава који јесу и све више ће бити од значаја у овој области. У том смислу, са једне стране, неопходно је прибавити већи број адекватних и значајних бесплатних или отворених софтверских алата у циљу њихове примене у расветљавању кривичних дела, као и обезбедити обуку стручних лица за рад у тим софтверским окружењима у том циљу. Са друге стране од значаја је и препознавање адекватних стратегија, тактика, метода и техника поступања са ОСИНТ–ом и алоцирање ресурса за активности у оквирима ове нове старе технике и методе прикупљања информација.

732 Према Википедији OSINT обухвата веома широк дијапазон информација и извора. Медије: штампане медије, радио и телевизијске медије као и рачунарски базиране податке. Заједнице везане за веб, као и садржај креиран од стране корисника: информације са сајтова социјалних мрежа, сајтова за дељење виде-садржаја, викија, блогова и фоксономија (систем класификовања изведен из праксе и метод заједничког – колаборативног креирања и управљања ознакама или обележивачима – популарно названим таговима); јавно доступне информације – информације од јавног значаја, извештаје владе, министарстава који су јавно доступни, званични подаци, као нпр. буџет, демографски подаци, скупштински пословници и записници скупштинских заседања, образложења у законским предлозима предлагача закона, конференција за штампу, јавних обраћања, говора и сл. Осматрања и извештаји: аматерски осматрачи цивилне авијације, радио-аматери, осматрачи сателита могу пружити различите информације које се на други начин не могу прибавити. Професионална или академска (тзв. сива литература): материјали са конференција, симпозијума, професионалних удружења, објављени зборници радова, апстраката и друге врсте материјала са оваквих манифестација;

Да ли сте били на посебним обукама и тренинзима за примену ИКТ у области којом се бавите и наведите којим?

Табела 6. Питање бр. 6

	n	%
да, анализа дигиталних доказа	1	2.08
да	7	14.58
да, дигитална форензика, истраге ВТК, фалсификовање и злоупотреба платних картица	1	2.08
не	24	50.00
да, било их је више	1	2.08
да, бихевиористичка анализа учинилаца ових КД	1	2.08
надлежно више ЈТ	1	2.08
да, невезано за члан 185 КЗ	1	2.08
није унето	11	22.92

Табела 7. Питање бр. 6 груписано

	n	%
да	13	27.06
не	24	50.00
није унето	11	22.92

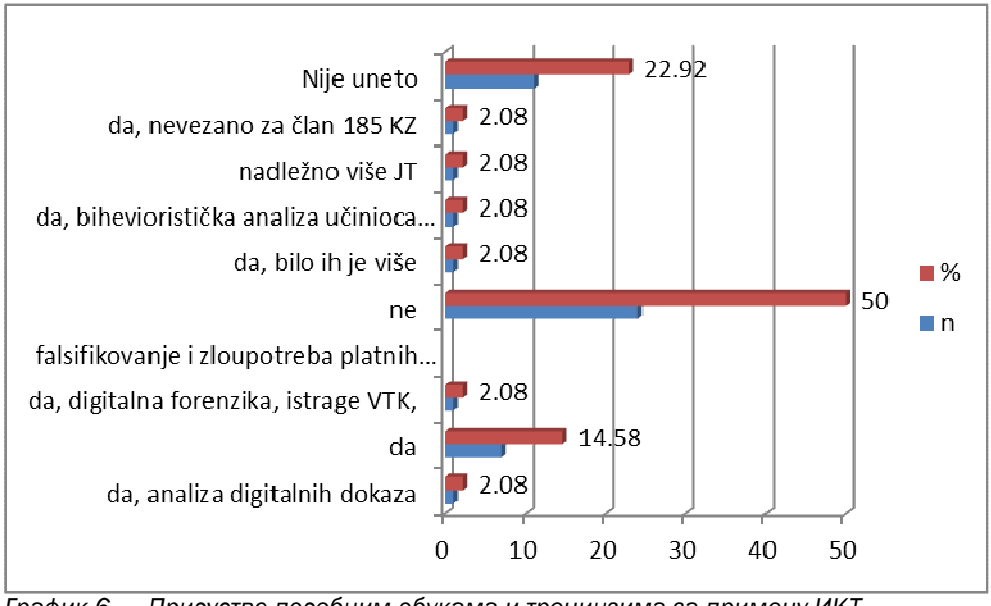


График 6. Присуство посебним обукама и тренинзима за примену ИКТ

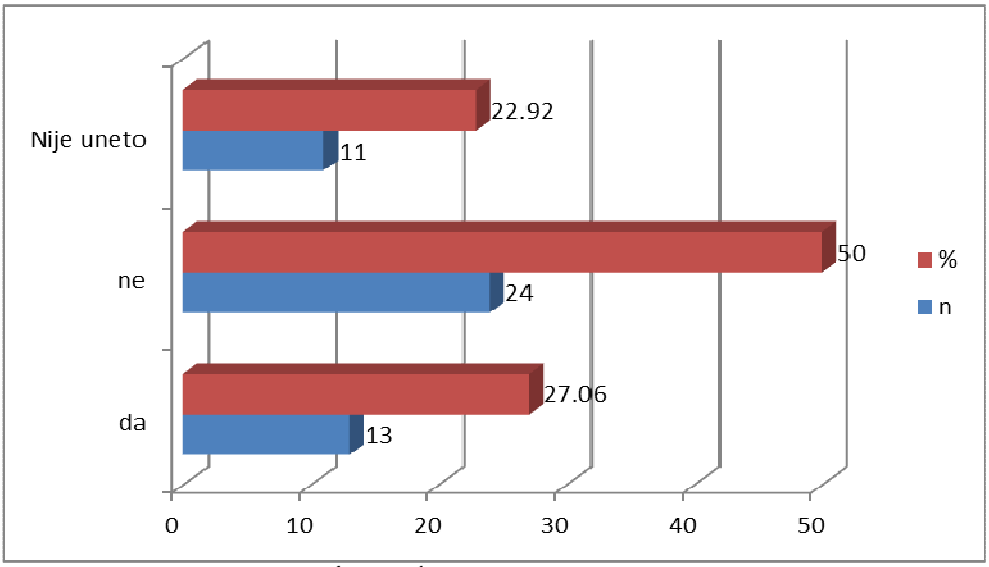


График 7. Присуство посебним обукама и тренинзима за примену ИКТ груписано

Генерално, питањем бр. 6 се хтело постићи остваривање увида у облике стручног усавршавања и њихову адекватну расподелу у овој области. Тако можемо видети да је 24 (50%) испитаника изнело да није било ни на каквим обукама, док 11 испитаника (22.92%) није ни унело одговор на ово питање. Значајан је податак да је 13 испитаника (27.06%) похађало обуке и тренинге за примену ИКТ. Када посматрамо појединачно, најбројније су обуке у погледу поступања са дигиталним доказима, дигитална форензика, истраге ВТК, обуке у погледу спречавања фалсификовања и злоупотребе платних картица, као и бихевиористичке анализе извршилаца. Када спроведемо анализу ових одговора неопходно је констатовати да за област илегалних миграција и трговину људима за коју су, између осталог, били одређени испитаници, није било превише обука, док је то ипак случај са припадницима полиције, тужиларства и суда у области ВТК. Као једна од могућих препорука јесте учесталије и интензивније спровођење обука у области илегалних миграција и трговине људима, као и да се припадници УГП-а и СБПОК-а, односно тужилаштва за организовани криминал, такође обучавају из области ВТК[733].

733 Милошевић, М. Ивановић, З. Едукација припадника криминалистичке полиције у сузбијању високотехнолошког криминала у Републици Србији и иностранa искуства са освртом на стратешка опредељења Републике Србије на сузбијању вискотехнолошког криминала, Тематски зборник Полиција, безбедност и високотехнолошки криминал, (ур. Жељко Никач), стр. 81-110. КПА, Београд 2010;

Уколико сте на питање бр. 4 одговорили са ДА објасните да ли се и на који начин недоследности злоупотребљавају:

Табела 8. Питање бр. 7

а. злоупотребљавају се	1	2.08
б. не	2	4.17
в. не знам	14	29.17

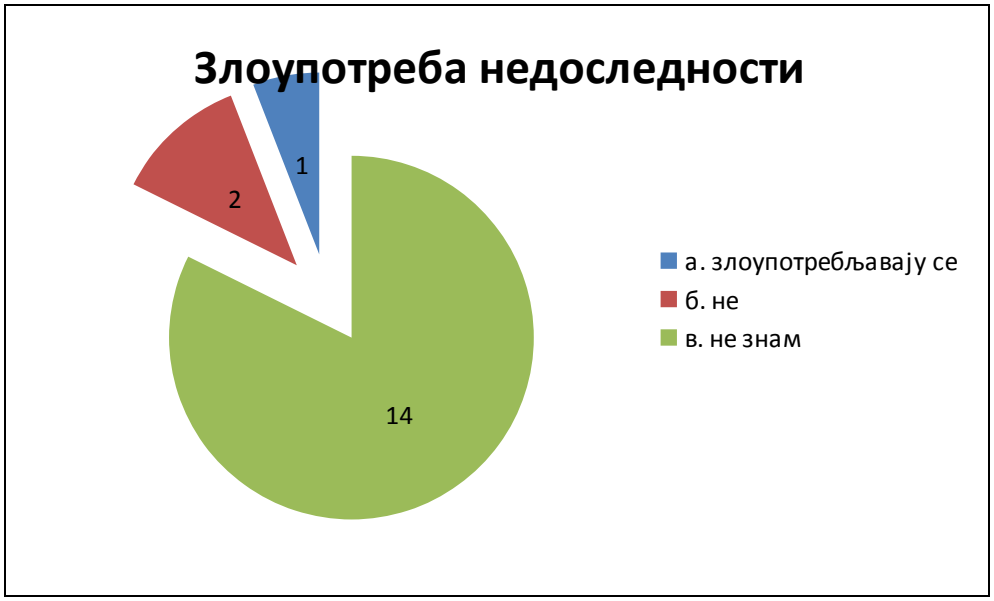


График 8. Злоупотреба недоследности

Код овог питања циљ и смисао је био прецизирање конкретних злоупотреба неинкриминисања појединих радњи које би се могле подвести под радње које би представљале кривично дело, али се у датом случају не могу гонити због непрецизности законске формулације. Међутим, испитаници нису прецизније формулисали поједине случајеве. Код давања оваквог одговора неопходно је разумети и да је велики проблем код изношења својих ставова у случајевима недоследности законодавца могућност да се погрешно протумачи или схвати и добронамеран коментар припадника структура које су овом анкетом биле обухваћене, па је зато вероватно изостао неки екстензивнији облик образлагања, поред тога што је анкета, наравно, била анонимна.

Навођење малолетног лица на присуствовање полним радњама (члана 185а, КЗ РС) односи се на:

а. малолетна лица

Табела 9. Питање бр.8 прва алинеја

увек	често	понекад	ретко	никад	није унето
19	18	1	1		6
39.58	37.50	2.08	2.08		12.5

Три анкете садрже одговор под а без учесталости што је укупно 42 одговора под а (87.5%)

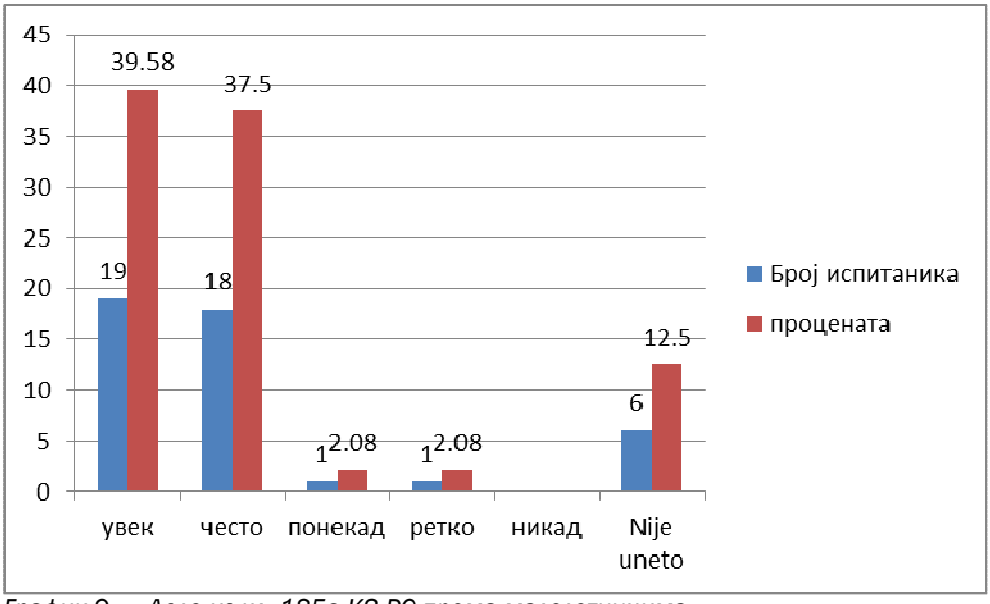


График 9. Дело из чл. 185а КЗ РС према малолетницима

Овим питањем се желело постићи остваривање увида у категорије лица које представљају пасивни субјекат овог кривичног дела, па тако 42 одговора (87.5%) као пасивног субјекта одређује искључиво малолетно лице, док је учесталост у том смислу приказана са 39.58% (19 испитаника) који кажу да су малолетници „увек“ пасивни субјекти, односно 37.5% (18 испитаника) који указују да су малолетници пасивни субјекти „често“. Индикативност датог одговора је веома интересантна, посебно уколико се посматра у склопу заједништва са одговорима који нису унети, што укупно чини већину испитаника од 50%.

Тумачење овог резултата је могуће увезати са резултатом следећег одговора.
б. децу

Табела 10. Питање бр.8 друга алинеја

увек	често	понекад	ретко	никад	није унето
13	10	10	1		12
27.08	20.83	20.83	2.08		25.0

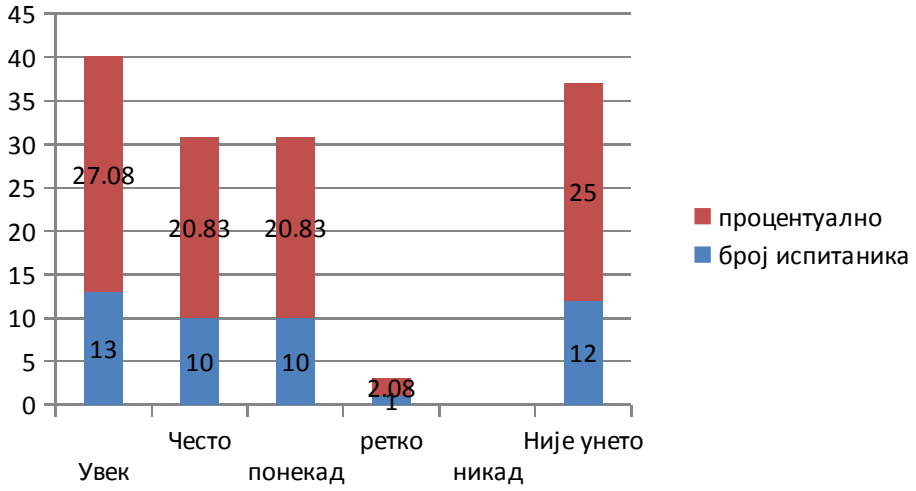


График 10. Дело из чл. 185а КЗ РС према деци

Две анкете садрже одговор под б без учесталости што је укупно 36 одговора под б (75%)

У одговорима испитаника, као пасивни субјекат се појављују деца у 36 одговора (75%) док је учесталост приказана на следећи начин, „увек“ су присутна деца код 13 испитаника (27.08%) „често“ код 7 испитаника (14.58%), а „понекад“ код 13 испитаника (27.08%). У вези са увезивањем са претходним, видећемо да је укупан број од 12 испитаника или 25% изоставио уношење одговора, а када то упоредимо са претходним одговором, где је дупло мањи проценат изоставио унос, онда можемо закључити да од поменутих 50% претходних испитаника негде око њих 12.5% садржано у одговору „често“, понекад и „ретко“ – малолетних лица. Овај проценат је индикативан за познавање бића овог кривичног дела од стране оних који га примењују у практичном смислу.

в. примену силе или претње

Табела 11. Питање бр. 8 трећа алинеја

увек	често	понекад	ретко	никад	није унето
8	7	13	1		17
16.67	14.58	27.08	2.08		35.42

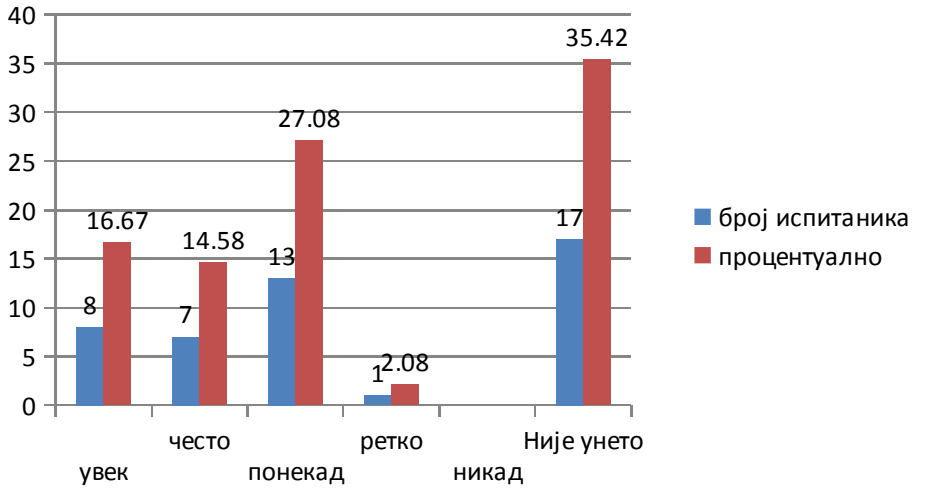


График 11. Дело из чл. 185а КЗ РС уз употребу принуде

Две анкете садрже одговор под в без учесталости што је укупно 31 одговора под в (64.58%)

За дистрибуцију учесталости овог одговора у питању бр. 8, најинтересантнији је укупан резултат од 28 испитаника (58.33%) који дају велику учесталост примени силе или претње у извршењу овог кривичног дела, што га у пракси сврстава у дела уз употребу насиља. Дакле, велика већина извршилаца ово дело чини уз помоћ претње односно силе. У том смислу могуће је пооштрити казнену политику у погледу овог кривичног дела, а такође и посебно обратити пажњу код примена мера из Закона о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (Службени гласник РС бр. 32-13), према лицима која чине ова дела са елементнима насиља. У том смислу подразумева се да сваки орган који у случају одређеном овим законом поступа са лицем које је извршилац оваквог кривичног дела, посебно обрати пажњу на њега.

г. посредно присуство кажњивим радњама путем интернета малолетног лица или детета

Табела 12. Питање бр. 8 четврта алинеја

увек	често	понекад	ретко	никад	није унето
2	7	10	2		26
4.17	14.58	20.83	4.17		54.17

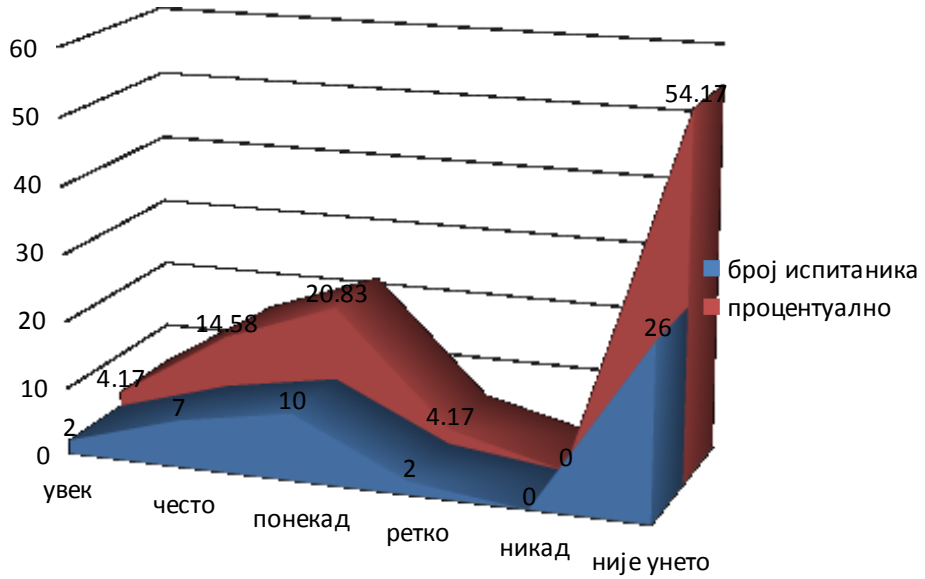


График 12. Дело из чл. 185а КЗ РС уз посредно присуство детета или малолетног

Једна анкета садржи одговор под г без учесталости што је укупно 22 одговора под г (45,83%)

Учесталост одговора испитаника на ово питање и овај одговор у овом питању даје увид у чињеницу да 19 испитаника (39.58%) „често“ проналази малолетнике као пасивне субјекте у посредном присуству у вршењу овог дела. У том смислу веома је значајан овај проценат испитаника у инверзном облику, наиме 54.17% испитаника или није никада пронашло у таквом виду или није унело своја запажања у овом правцу. Дакле, може се рећи да је велика већина оних који нису имали прилике да се са оваквим случајевима сретну у пракси, али у вези са претходним одговором могуће је закључити да поједини облици овог дела ипак јесу фреквентни и да се мора повести рачуна о овоме у будућности.

д. нешто друго

један одговор је под д и један додат не знам (4.17%)

Табела 13. Питање бр. 8 пета алинеја

увек	често	понекад	ретко	никад
42	36	31	22	1
87.5	75	64.58	45.83	4.17

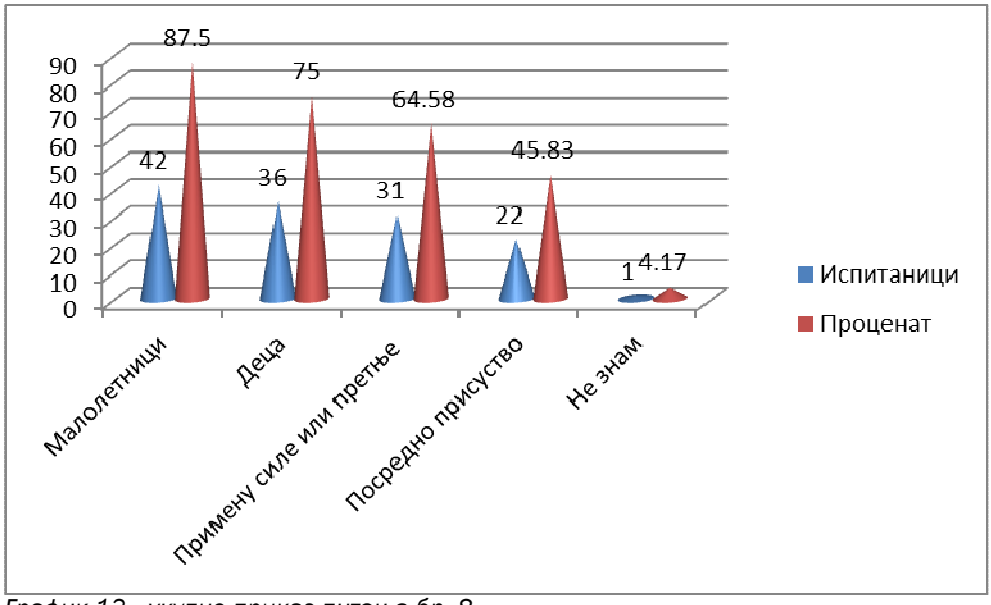


График 13. укупно приказ питања бр. 8

Генерално можемо видети да се у одговорима на ово питање линеарно смањује заступљеност различитих категорија лица деца – малолетници, односно примена силе или претње и феномен посредног присуства пасивних субјеката у вршењу дела.

Ово дело се према Вашим сазнањима може вршити и у оквирима:
а. илегалних миграција

Табела 14. Питање бр. 9 прва алинеја

увек	често	понекад	ретко	никад	није унето
	14	16	3		14
	29.17	33.33	6.25		29.17

Једна анкета садржи одговор под а без учесталости што је укупно 34 одговора под а (70.83%)

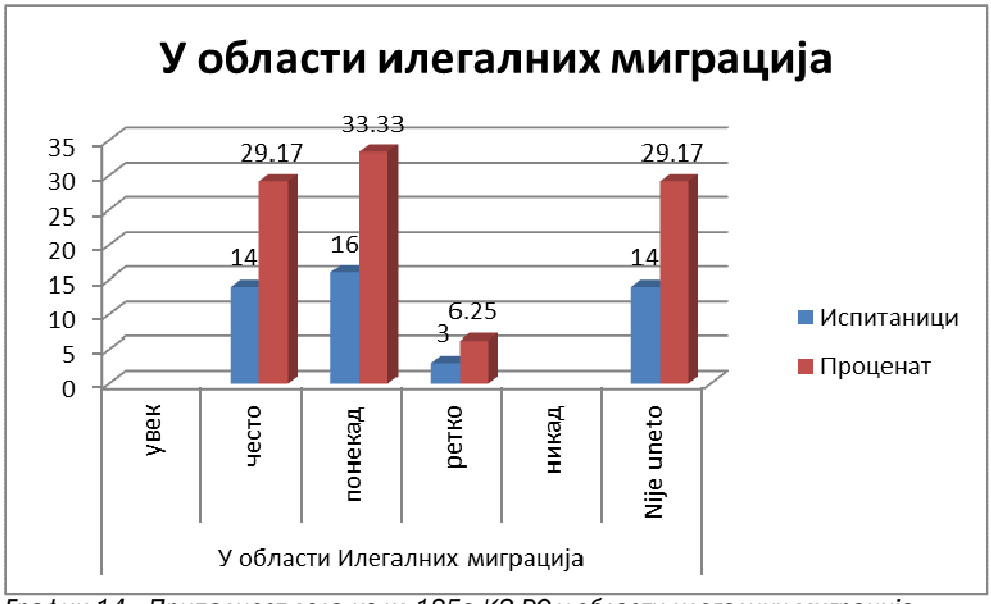


График 14. Припадност дела из чл.185а КЗ РС у области илегалних миграција

Из приказаног можемо видети да је 30 испитаника (62.5%) препознало ово дело у области илегалних миграција као „чест“ или „периодичан“ проблем. Могуће је тумачити и ове одговоре на начин којим ћемо добити и дисперзацију припадности испитаника одређеним областима.

б. трговине људима

Табела 15. Питање бр. 9 друга алинеја

увек	често	понекад	ретко	никад	није унето
1	23	11	2		9
2.08	47.92	22.92	4.17		18.75

Две анкете садрже одговор под б без учесталости што је укупно 39 одговора под б (81.25%)

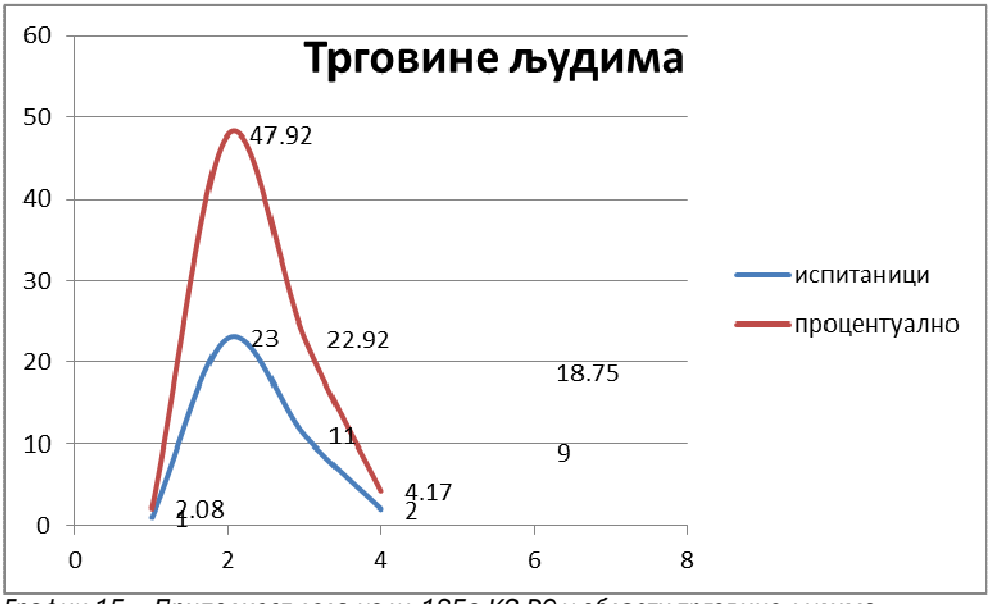


График 15. Припадност дела из чл.185а КЗ РС у области трговине људима

в. класичних кривичних дела увек често понекад ретко никад

Табела 16. Питање бр. 9 трећа алинеја

увек	често	понекад	ретко	никад	није унето
1	10	17	2		17
2.08	20.83	35.42	4.17		35.42

Једна анкета садржи одговор под в без учесталости што је укупно 31 одговора под в (64.58%)

У оквиру резултата учесталости овог одговора у питању бр. 9 можемо закључити да 28 испитаника (58.33%) види ово дело као учестало у области трговине људима.

График 16. Припадност дела из чл.185а КЗ РС у области класичних кривичних дела

г. кривичних дела организованог криминала, корупције и других тешких кривичних дела увек често понекад ретко никад

Табела 17. Питање бр. 9 четврта алинеја

увек	често	понекад	ретко	никад	није унето
	5	11	5	1	23
	10.42	22.92	10.42	2.08	47.92

Три анкете садрже одговор под г без учесталости што је укупно 25 одговора под г (52.08%)

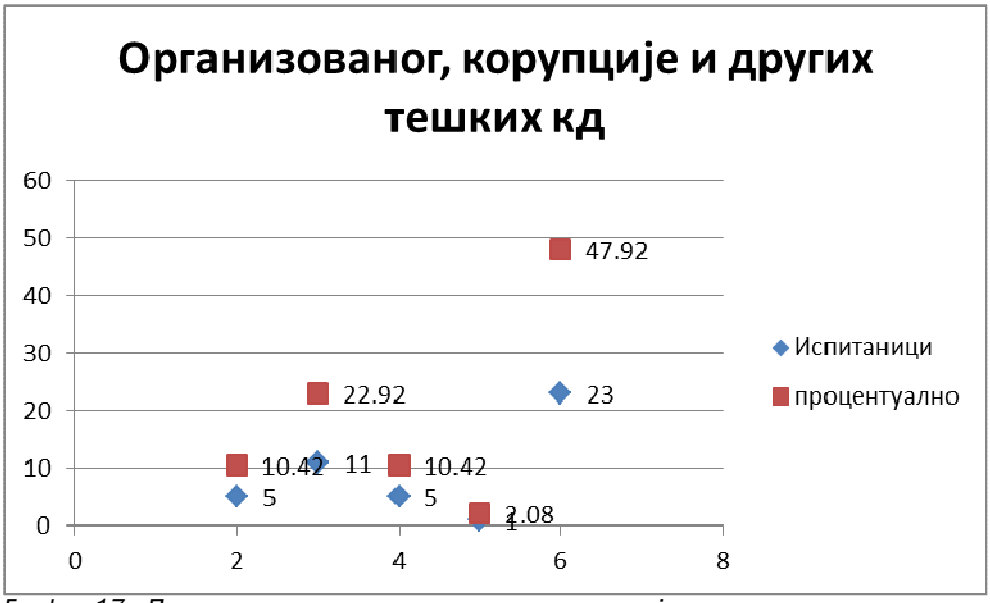


График 17. Приказ организованог криминала, корупције и других тешких дела

У анализи овог одговора се може приметити да је 16 испитаника (33,34%) перципирало учесталост овог дела у области класичног криминалитета.

д. један одговор под д – уз свако КД

Табела 18. Укупна дисперзија питања бр.9

	илегалних миграција	трговине људима	класичних КД	организованог криминала корупције и других тешких	уз свако КД
Испитаници	34	39	31	25	1
Процентуално	70.83	81.25	64.58	52.08	2.08

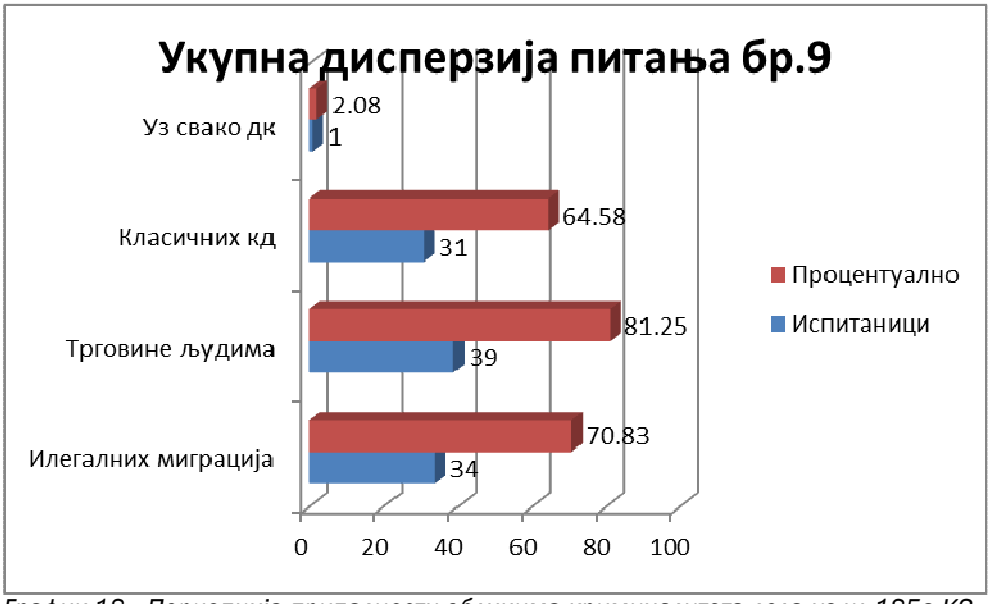


График 18. Перцепција припадности облицима криминалитета дела из чл.185а КЗ РС

Испитаници су, њих 39 (или 81.25%) перципирали дело из чл. 185а првенствено у области криминалитета чије је главно дело кривично дело трговине људима, затим у области илегалних миграција 34 испитаника (70.83%), односно 31 (64.58%) колико их је указало да по њиховој перцепцији ово дело спада у област класичног криминалитета. Један испитаник (2.08%) је указао да се ово дело може приметити уз свако крвично дело, а не специфично за поједине области. Резултат перцепције је разумљив и у светлу приказа структуре испитаника с обзиром да су већина испитаника припадници полиције из УКП-а, СБПОК-а или УГП-а. Овоме погодује са друге стране и законска детерминација кривичних дела која спадају у област високотехнолошког криминала, која мегаломански покушава да у корпус ВТК убаци скоро сва значајнија кривична дела. У том смислу није новост да свако покушава да перципира тангентна дела својој области као своја основна задужења, што наши испитаници здушно раде.

Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

График 19. Начини извршења и појавни облици дела из чл. 185а КЗ РС

Табела 19. Питање бр.10

начини извршења	испитаници	процентуално
а. навођењем малолетника да присуствује силовању, обљуби или са њом изједначеним чином или другој полној радњи	24	50.0
б. дело учињено употребом силе или претње, или према детету	17	35.42
в. не знам	12	25.0

У анализи одговора на питање бр.10, 24 испитаника (50%) је као најчешћи начин извршења овог кривичног дела навело први основни облик - навођењем малолетника да присуствује силовању, обљуби или са њом изједначеним чином или другој полној радњи, док је други навело њих 17 (35.42%). Од укупног броја испитаника за „не знам“ се определило њих 12 (25%). Као делотворан механизам анализе овог питања неопходно је усвојити и коментаре дате у претходном корпусу анализе, па у склопу истог разумети да је ипак блажи облик предоминантнији, али да треба обратити пажњу на могућности утицаја на смањење и једног и другог облика кроз проактивно деловање и примену свих расположивих механизама у том правцу.

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела?

Табела 20. Питање бр.11

	n	%
све расположиве	5	10.42
не знам	4	8.33
интернет, рачунарске мреже	1	2.08
рачунар	1	2.08
примена софтвера	1	2.08
мере надзора интернета и телефона	1	2.08
коришћење рачунара	1	2.08
контрола интернета и превентивно деловање путем друштвених мрежа	1	2.08
интернет, мобилна и фиксна телефонија, софтвер	5	10.42
интернет	3	6.25
интернет, ТВ	1	2.08
надлежност вишег, а не основног ЈТ	1	2.08
контрола друштвених мрежа на интернету и претрага огласа сумњиве садржине	1	2.08
интернет, аутоматско рачунарско претраживање података, снимање телефонских разговора и слично	1	2.08
ограниченост доступности таквог садржаја на интернету, веб- сајтови, надзор и мониторисање налога на facebook-у	1	2.08
ТВ, интернет, други медији	1	2.08
средства јавног информисања	2	4.17
све доступне	1	2.08
медији	1	2.08
није унето	15	31.3

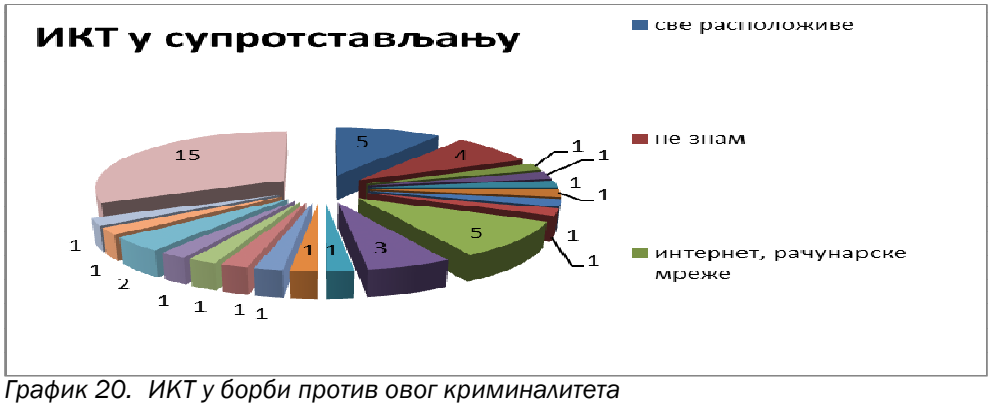


График 20. ИКТ у борби против овог криминалитета

У односу на претходно питање у вези са кривичним делом из чл.185 поред уобичајених одговора везаних за социјалне мреже, интернет и надзор комуникација уопште, овде је дошло и до додатних продирања у ову материју, па тако имамо и предлог: ограниченост доступности таквог садржаја на интернету, веб-сајтови, надзор и мониторисање налога на Facebook-у (2.08%). Од значаја је и чињеница да 15 испитаника (31.3%) није дало одговор. Оно што је додатно интересантно у анализи овог питања је да ни један од приказаних одговора није претерано конкретизован, већ су они на јако високом нивоу општости. Чињеница да ни питање није експлицитно захтевало конкретизацију, опет умањује могућност добијања конкретног одговора, но очекивало се од професионалаца, који се директно баве овом материјом, да буду конкретнији. Из предложених одговора могу се закључити следеће околности и ставови. Наиме, већина учесника анкете указала је на потребу коришћења интернета, без прецизирања начина и средства у расветљавању ових кривичних дела. У том смислу могуће је даље закључивати о посебним проблемима у овој области, наиме овде је могуће тврдити да испитаници нису у потпуности разумели питање или да су се одговарајући на ово питање усмерили ка неком другом. Разлог овоме налази се у проблему проналажења ИКТ којима се ова дела могу адекватно расветљавати, с обзиром да се принуда састоји у физичким активностима и евентуално психичкој принуди, а које не носе са собом употребу рачунара нити било које ИКТ. У сваком случају могуће је да су анкетирани имали у виду могућност да се информације у вези ових кривичних дела могу појавити по различитим садржајима на интернету, посебно у вези блогова или видео-записа о личним исповестима, па чак и као посредно везане информације о оваквим делима. Но, без обзира на одређене пропусте могуће је дати следеће препоруке у погледу будућих облика и средстава која би помогла у расветљавању ових дела. Могуће је да се на појединим социјалним мрежама, односно одређеним сервисима на интернету или у оквирима затворених група, могу користити садржаји са истих у циљу доказивања ових дела. Но, приликом коришћења оваквих информација мора се водити рачуна о проблематици начина њиховог прибављања с обзиром на правила (прибављања доказа) доказивања која са собом носи нови ЗКП. Такође у том смислу треба водити рачуна и о многим аспектима оваквих информацијама, у погледу заштите података о личности, обрађивању таквих података од стране државног органа, питању приватности оваквих информација на интернету, с обзиром на њихово постављање од стране лица чији су и слично. У овом правцу неопходно је и код нас установити које области би се у циљу истраге или других полицијских послова могле користити у овом смислу (прикупљања и обраде података о личности), а када су у питању само могући основи сумње да је извршено кривично дело. Такође, од значаја је и прикупљање и обрада ових података у случајевима извршења других кажњивих дела, односно у случајевима кривичних дела која се гоне по приватној тужби (или по предлогу одређених лица, односно у случајевима имунитета и слично), када је полиција у обавези да оштећеном пружи одређене податке о лицу које је учинилац кривичног дела, у циљу обезбеђивања информација о његовој личности и евентуалног покретања прекршајног или другог поступка. На нама је у будућности да предвидимо процедуре и правила по којима се мора поступати у оваквим случајевима и да искристалишемо начине обезбеђивања ових информација у оперативне и истражне сврхе.

Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу, из члана 185б, према Вашем искуству чинило се следећим средствима ИКТ:

а. различити уређаји за аудио-визуелно снимање

Табела 21. Питање бр.12 прва алинеја

увек	често	понекад	ретко	никад	није унето
3	19	1	2	1	17
6.25	39.58	2.08	4.17	2.08	35.42

Пет анкета садржи одговор под а. без учесталости што је укупно 31 одговора под а. (64.5%)

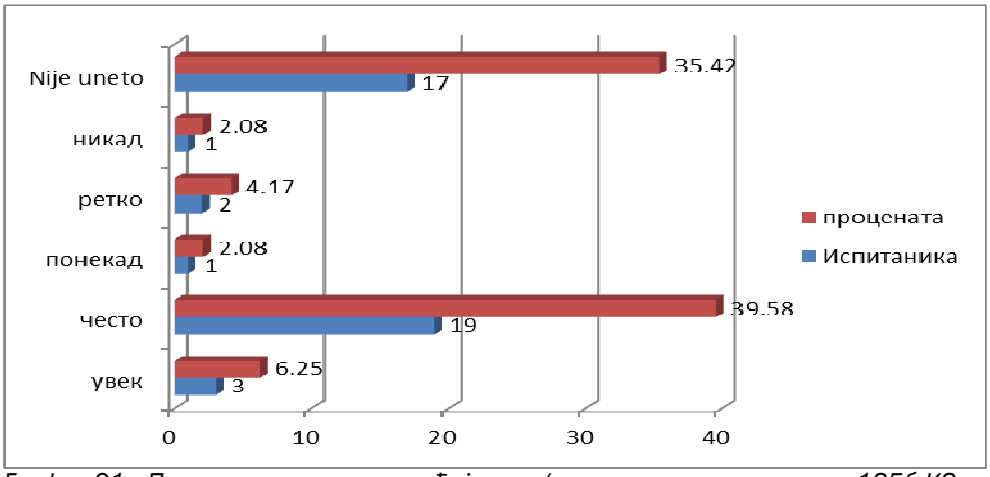


График 21. Примена различитих уређаја за а/в снимање код дела из чл.185б КЗ РС

Циљ питања је био да се добију подаци о врстама уређаја који се користе у вршењу дела из чл.185б, као и о њиховој учесталости, односно заступљености у вршењу овог дела. Па тако су уређаји за аудио и видео-снимање поменути у 23 одговора као учестали (увек, понекад и често). Уколико им додамо и поменутих пет онда имамо укупну суму од 28 одговора (58.33%) испитаника који сматрају знатно учесталом примену а/в уређаја за снимање у вршењу овог кривичног дела. Интересантно би било добити податке о субјектима који су их користили и њиховим релацијама са жртвама или пасивним субјектима кривичног дела, а што може бити неки од даљих праваца истраживања. У погледу могућих смерница везаних за резултате овог питања требало би у вези расветљавања обратити пажњу на садржаје ових уређаја, односно законито прибављање ових садржаја путем примене адекватних мера (испуњење законом предвиђених услова), с обзиром да у случају овог кривичног дела отпада примена посебних доказних радњи (због услова из чл.162 ЗКП). Генерално овај коментар одговара целокупним резултатима у погледу овог питања, што значи да се може применити на сваком.

б. смарт телефони

Табела 22. Питање бр.12 друга алинеја

увек	често	понекад	ретко	никад	није унето
4	19	4	1	1	16
8.33	39.58	8.33	2.08	2.08	33.33

Три анкете садрже одговор под б без учесталости што је укупно 32 одговора под б (66.67%)

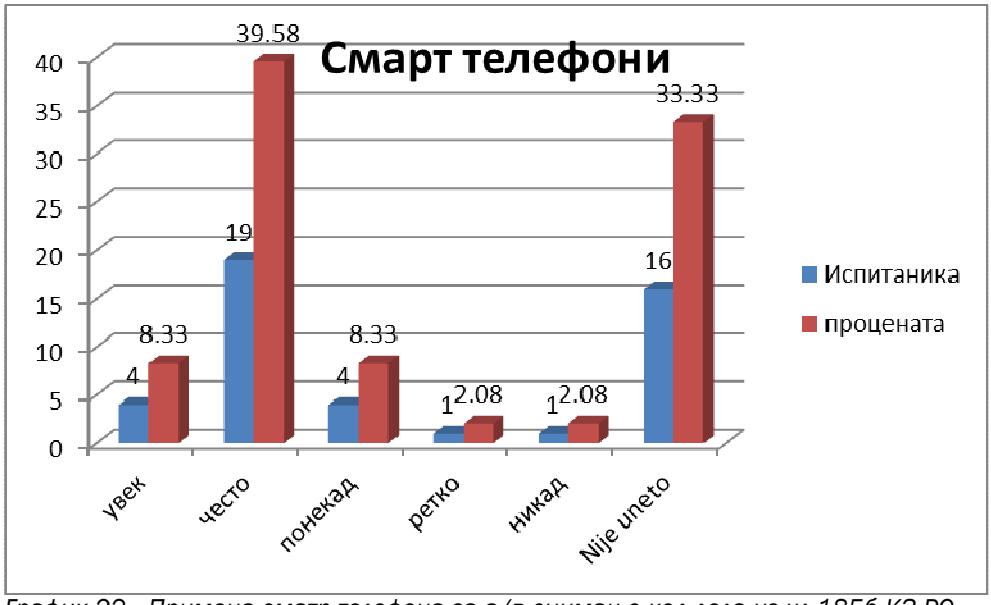


График 22. Примена сматр телефона за а/в снимање код дела из чл.185б КЗ РС

У случају смарт телефона је 27 одговора (56.64%), а када на то додамо укупан број приписаних одговора, онда та цифра износи укупно 32 одговора под б (66.67%) и она указује да су коришћени смарт телефони снабдевени уређајима за снимање аудио/видео садржаја у апсолутној већини овог случаја. Ово је интересантан податак с обзиром на њихову доступност. У том смислу веома је тешко замислити захтев који би ишао према произвођачима телефона да се ово на неки начин онемогући, дакле правци деловања би морали ићи у неким другим смеровима. У том смислу веома је лако наћи материјал за расветљавање и гоњење ових облика овог кривичног дела, уз ограду у вези коментара који је дат у претходном одговору.

в. таблети

Табела 23. Питање бр.12 трећа алинеја

увек	често	понекад	ретко	никад	није унето
2	14	8	1		21
4.17	29.17	16.17	2.08		43.75

Две анкете садрже одговор под в без учесталости, што је укупно 27 одговора под в (56.25%)

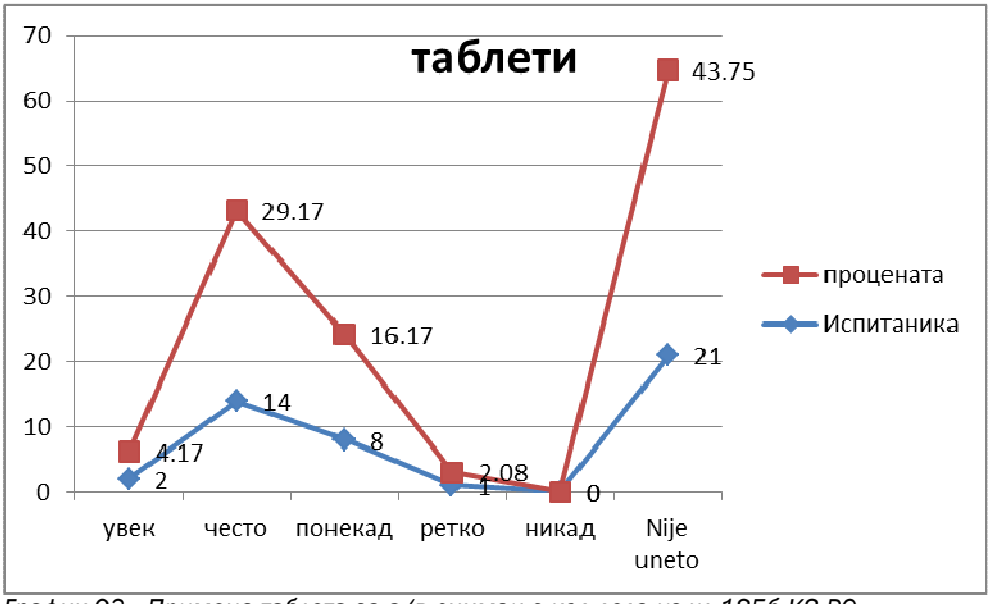


График 23. Примена таблета за а/в снимање код дела из чл.185б КЗ РС

У случају таблета 24 одговора (39.51%) указује на њихово учестало коришћење. Очекује се је да у будућности овај број буде повећан услед њихове све веће доступности и подизања популарности.

г. лаптоп

Табела 24. Питање бр.12 четврта алинеја

увек	често	понекад	ретко	никад	Није унето
4	12	5			25
8.33	25.0	10.42			52.08

Две анкете садрже одговор под г без учесталости што је укупно 23 одговора под г (47.92%)

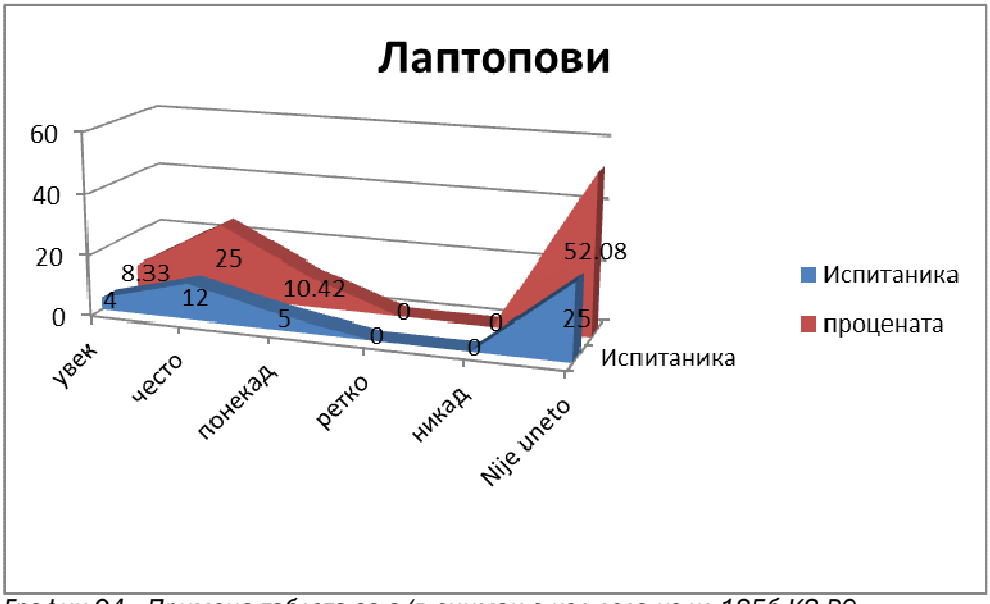


График 24. Примена таблета за а/в снимање код дела из чл.185б КЗ РС

Лаптопови су често коришћени у вршењу овог дела, у 21 случају (43.75%). Уз додатак две анкете без учесталости, то износи 23 или 47.92%, што указује на тренд у честом коришћењу ових уређаја у односу на друге, с обзиром на доступност цене.

д. друго

Две анкете су са овим одговором без учесталости (4.17%)

Табела 25. Збирно

	различити а/в уређаји	смарт телефони	таблети	лаптопови	друго
Испитаника	31	32	27	23	2
Проценат	64.5	66.67	56.25	47.92	4.17

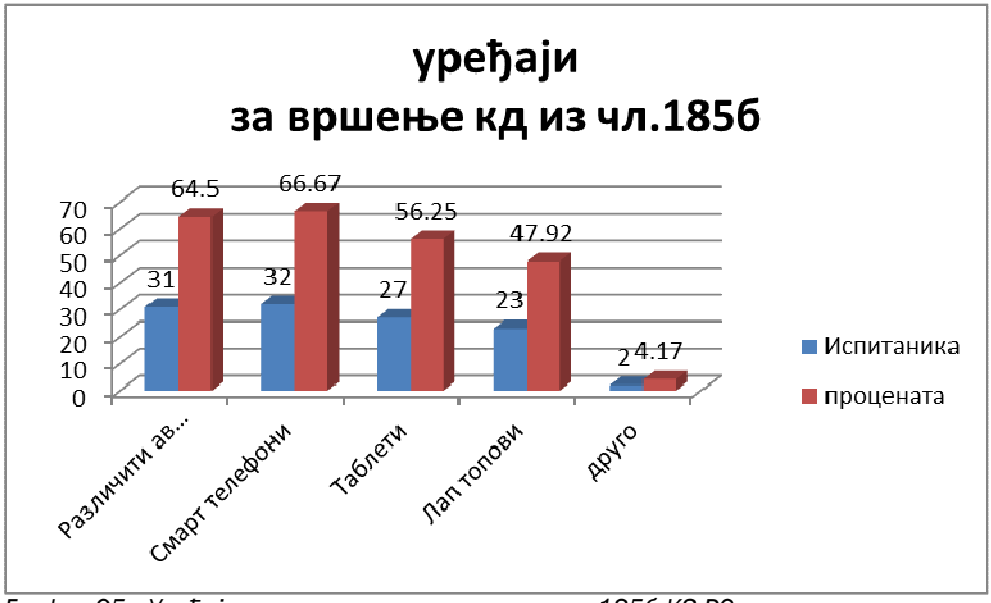


График 25. Уређаји скупно за вршење дела из чл. 185б КЗ РС

У генералном учешћу уређаја најзаступљенији су смарт телефони, па за њима следе различити а/в уређаји, таблети, лаптопови и остали уређаји. У овом смислу значајно је развити и средства и процедуре или уређаје и системе у циљу прибављања и анализе података са уређаја који су овде приказани. У првом реду, потребно је, поред постојећих законских и подзаконских аката, уредити стандардне оперативне процедуре у погледу поступања са уређајима, односно предвидети одговорност свих припадника полиције у поступању са оваквим дигиталним траговима. Након овога неопходно је прибавити адекватне уређаје и софтвере који у том смислу могу бити коришћени, као нпр. Celebrite© или неки сличан софтвер и пратећи уређај, при чему треба водити рачуна о односу цене и квалитета.

Ово дело се може вршити и у оквирима:
а. илегалних миграција

Табела 26. Питање бр.13 прва алинеја

увек	често	понекад	ретко	никад	није унето
	13	8		2	22
	27.08	16.17		4.17	45.83

Три анкете садрже одговор под а без учесталости што је укупно 26 одговора под а (54.17%)

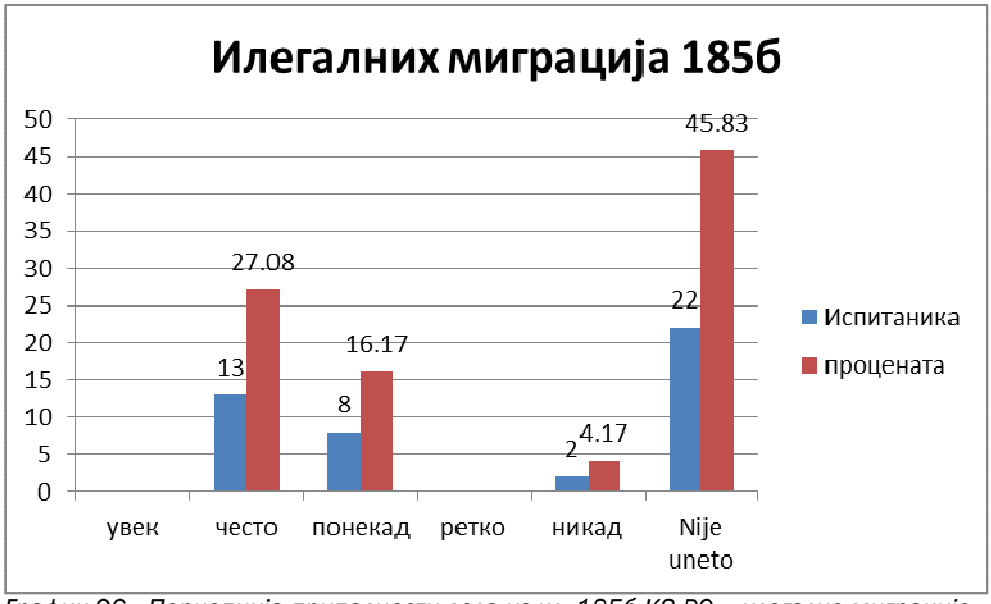


График 26. Перцепција припадности дела из чл. 185б КЗ РС – илегалне миграције

Из графикона видимо да је најзаступљеније у 21 одговору (43.25%) по учесталости. Уколико додамо и три без учесталости онда је то 24 одговора или 50% (у смислу често и понекад) одређење овог кривичног дела у области илегалних миграција.

б. трговине људима

Табела 27. Питање бр.13 друга алинеја

увек	често	понекад	ретко	никад	није унето
	19	6	2		16
	39.58	12.5	4.17		33.3

Пет анкета садрже одговор под б без учесталости што је укупно 32 одговора под б (66.67%)

График 27. Перцепција припадности дела из чл. 185б КЗ РС – трговина људима

Учесталост одговора према овој анкети је 25 одговора (52.08%). Уколико додамо и оних пет без учесталости онда је то 30 одговора или 62.5% испитаника који мисле да је ово дело из области трговине људима.

в. класичних кривичних дела

Табела 28. Питање бр.13 трећа алинеја

увек	често	понекад	ретко	никад	није унето
1	10	10	2		24
2.08	20.83	20.83	4.17		50

Једна анкета садржи одговор под в без учесталости што је укупно 24 одговора в (50%).

График 28. Перцепција припадности дела из чл. 185б КЗ РС – класичан криминалитет

1 испитаник, односно 43.75% (22 са оним без учесталости или 45.83%) позиционирао је ово дело првенствено по учесталости у област класичног криминалитета.

г. кривичних дела организованог криминала

Табела 29. Питање бр.13 четврта алинеја

увек	често	понекад	ретко	никад	није унето
	8	7	2	2	27
	16.17	14.58	4.17	4.17	56.25

Две анкете садрже одговор под г без учесталости што је укупно 21 одговора под г (43.75%).

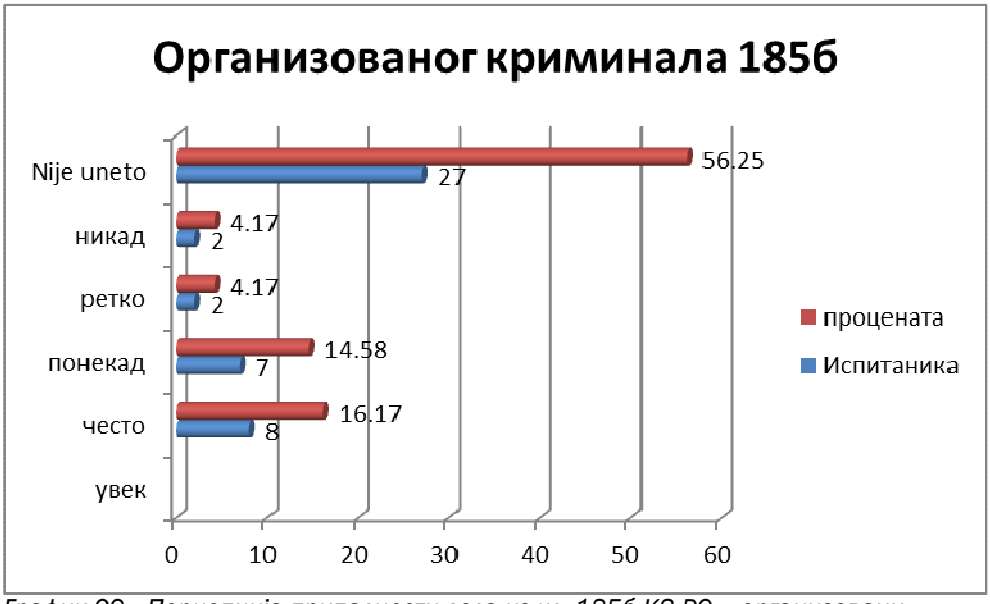


График 29. Перцепција припадности дела из чл. 185б КЗ РС – организовани криминал

15 одговора (30.75%) ових испитаника (17 са оним без учесталости или 35.41%) позиционирало је ово дело по учесталости у области организованог криминала.

д. корупције и других тешких кривичних дела

Табела 30. Питање бр.13 пета алинеја

увек	често	понекад	ретко	никад	није унето
		4	3	3	38
		8.33	6.25	6.25	79.17

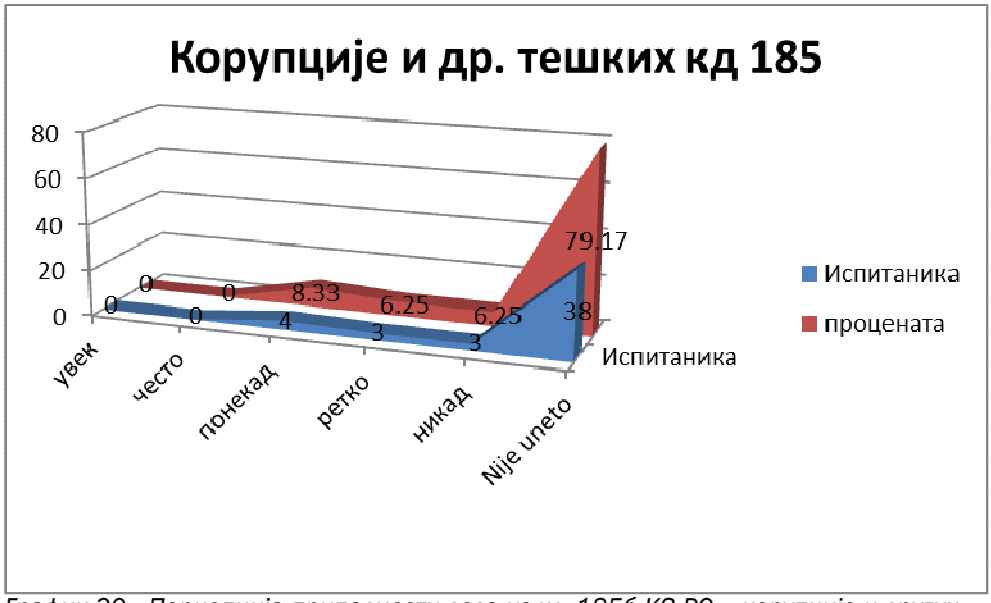


График 30. Перцепција припадности дела из чл. 185б КЗ РС – корупције и других тешких дела

Из овог графикона се може видети да је веома мали проценат ово дело позиционирао у области корупције и других кривичних дела, свега 3 испитаника га је позиционирало као редак случај, њих 4 као појаву која понекад бива случај, а 3 да никада није спадало у ову област.

ђ. један одговор – свим другим КД (2.08%)

Табела 31. Питање бр.13 збирно

	илегалних миграција	трговине људима	класичних КД	КД организованог криминала
Испитаника	26	32	24	21
процената	54.17	66.67	50	43.75

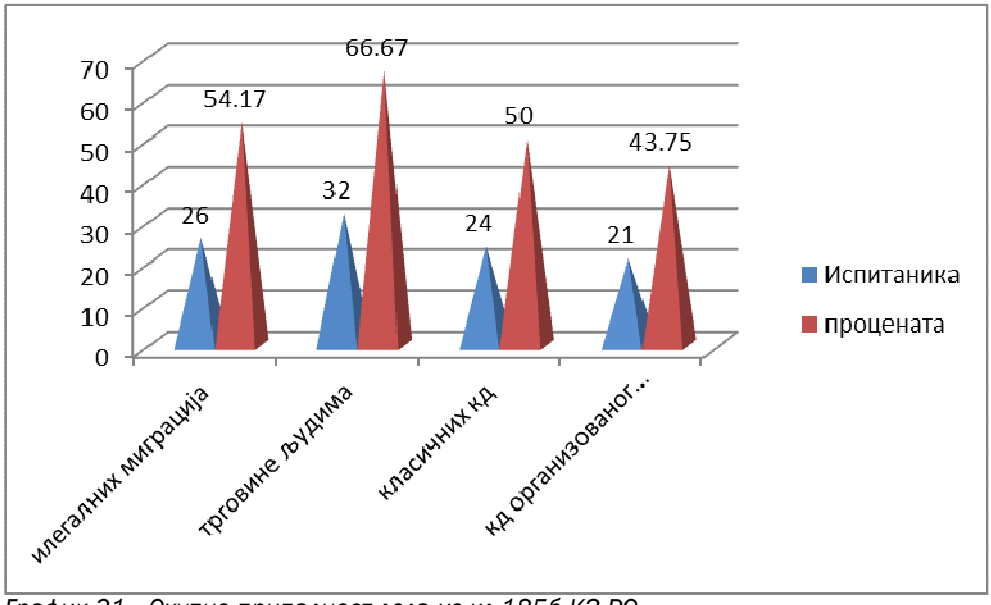


График 31. Скупно припадност дела из чл.185б КЗ РС

Из приложеног се може закључити да испитаници у највећем броју случајева позиционирају ово кривично дело у области илегалних миграција и трговине људима, а да га у мањем броју (при чему постоји сличност учесталости са илегалним миграцијама због односа 54.17% и 50%) одређују као дело из области класичног криминалитета, односно много мање организованог криминалитета.

Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

Табела 32. Питање бр.14

одговори	n	%
а. у намери извршења кривичног дела из чл. 178 став 4, 179 став 3, 180 ст. 1 и 2, 181 ст. 2 и 3, 182 став 1, 183 став 2, 184 став 3, 185 став 2. и 185а КЗ, користећи рачунарску мрежу или комуникацију другим техничким средствима договори са малолетником састанак и појави се на договореном месту ради састанка	22	45.83
б. ко дело изврши према детету	12	25.0
в. не знам	14	29.17

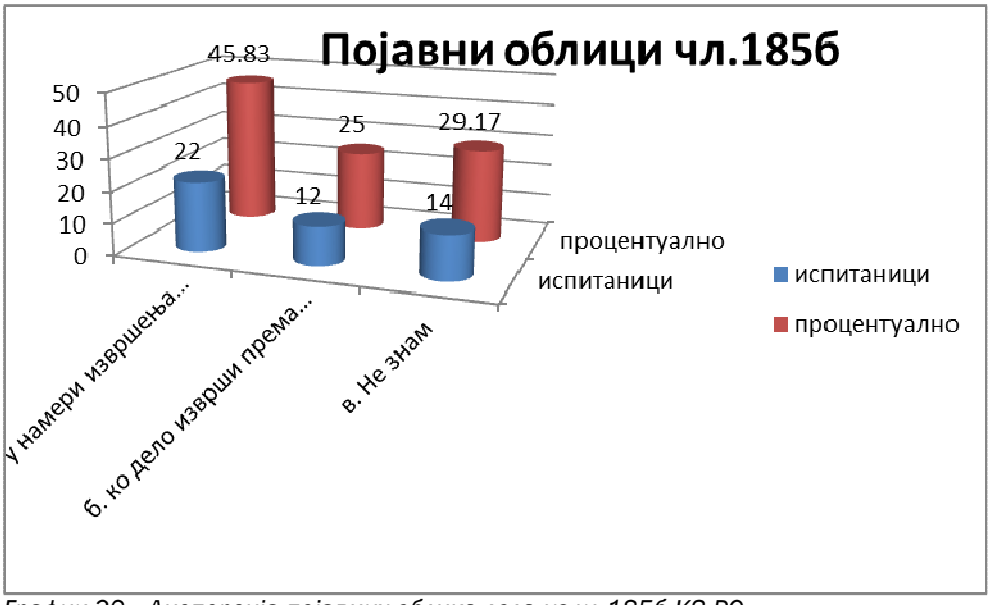


График 32. Дисперзија појавних облика дела из чл.185б КЗ РС

Према одговорима испитаника ово дело се најчешће јавља у првом појавном облику (22 испитаника – 45.83%). Други – тежи, појавни облик, када је ово дело извршено према детету, дало је одговор 12 испитаника (25%) и на крају смо имали 14 испитаника (29.17%) који нису дали одговор о учесталости бирајући опцију под в.“не знам“. Очекивано, најзаступљенији је основни облик дела, а видело се и да је близу 30% испитаника изостало са одговором, што може бити знак да са истим делом нису дошли у додир. Ако се укупно размотри резултат који су наши испитаници постигли он говори о постојању велике заступљености овог дела у нашој пракси, без обзира на облик, што је алармантни податак. У том смислу свако ко буде радио неке дубље анализе у овој области криминалитета, мора предвидети начине проактивног деловања у овом смеру, односно треба да води рачуна о

примени мера из Маријиног закона на извршиоце овог дела. Само на тај начин и генерална и специјална превенција могу имати смисла.

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

Табела 33. Питање бр.15

одговори	n	%
све расположиве	8	16.67
не знам	4	8.33
рачунарске мреже	2	4.17
примена софтвера	1	2.08
мере надзора интернета и телефона	1	2.08
контрола интернета	1	2.08
интернет, мобилна и фиксна телефонија, софтвер	4	8.33
интернет, ТВ	1	2.08
надлежност вишег, а не основног ЈТ	1	2.08
контрола друштвених мрежа на интернету и претрага огласа сумњиве садржине	1	2.08
бесплатан Microsoft програм "PhotoDNA", "NetCleanAnalyze", систем "ChildExploatationTracking System (CETS)" – глобални програми за полицију и тужилаштво	1	2.08
ТВ, интернет, други медији	1	2.08
ТВ, радио и друга средства јавног информисња	1	2.08
средства јавног информисања	1	2.08
нема вредности	20	41.67

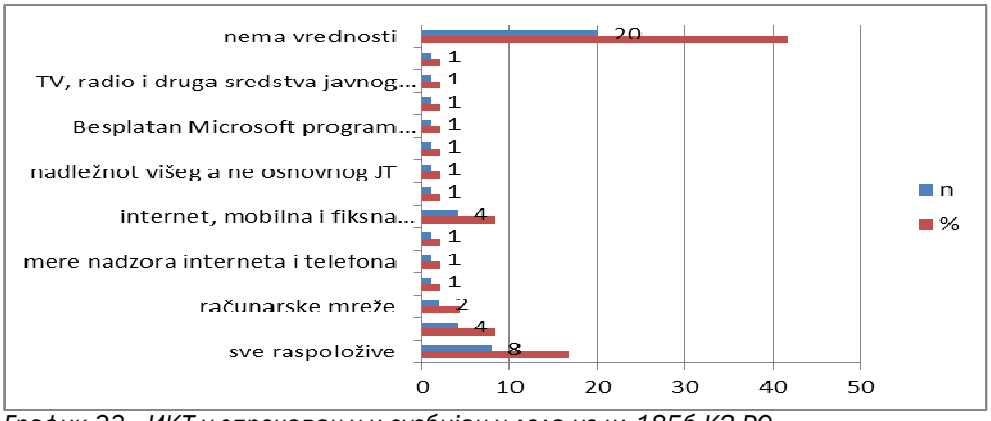


График 33. ИКТ у спречавању и сузбијању дела из чл.185б КЗ РС

Као и у претходним питањима ове врсте, као средства ИКТ која се могу користити у спречавању и сузбијању ових кривичних дела, јављају се одређени софтверски и програмски пакети, односно мере надзора интернета и социјалних мрежа, односно средства јавног информисања.

Повреда моралних права аутора и интерпретатора из члана 198 КЗ врши се у ком облику:

Табела 34. Питање бр. 16

одговор	n	%
а. када извршилац под својим именом или именом другог у целини или делимично објави, стави у промет примерке туђег ауторског дела или интерпретације, или на други начин јавно саопшти дело или интерпретацију	35	72.92
б. без дозволе аутора измени или преради туђе ауторско дело или измени туђу снимљену интерпретацију	38	79.17
в. не знам	2	4.17

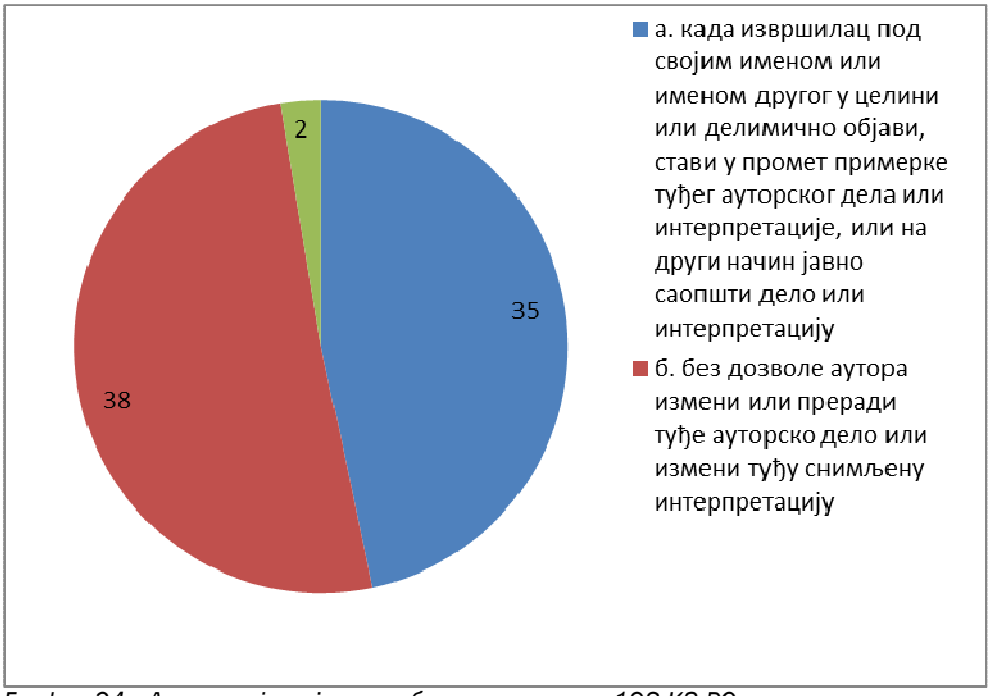


График 34. Дисперзија појавних облика дела из чл. 198 КЗ РС

Кривично дело из чл.198 се јавља са сличном заступљеношћу оба облика – првог у 38 случајева (79.17%), а другог у 35 (72.92%) случајева. Уколико разматрамо ово дело са аспекта ВТК можемо напоменути да је други мање заступљени одговор од већег значаја, с обзиром да се у оквирима он-лајн „пиратерије“ много мање баве изменама ауторског дела (морални аспект) у односу

на онај други економски аспект ауторског дела. У овом моменту најчешће се јавља ова ситуација кроз различите облике искоришћавања ауторског дела путем интернета, који се јавља у највећој заступљености кроз П2П или torrent размену материјала. Сви остали облици су много мање заступљени него овај.

Ово дело се према Вашим сазнањима може вршити и у оквирима:
а. илегалних миграција

Табела 35. Питање бр.17 прва алинеја

увек	често	понекад	ретко	никад	Није унето
		1	13	2	32
		2.08	27.08	4.17	66.67

б. трговине људима увек често понекад ретко никад

Табела 36. Питање бр.17 друга алинеја

увек	често	понекад	ретко	никад	није унето
		1	10	5	32
		2.08	20.83	10.42	66.67

Дело се у области илегалних миграција и трговине људима појављује веома ретко

в. класичних кривичних дела

Табела 37. Питање бр.17 трећа алинеја

увек	често	понекад	ретко	никад	није унето
5	9	10	1	1	15
10.42	18.75	20.83	2.08	2.08	31.25

График 35. Дело из чл. 198 КЗ РС перципирано у области класичног криминалитета

Седам анкета садржи одговор под в без учесталости што је укупно 33 одговора под в (68.75%)

Оно што је интересантно у одговорима на ово питање је да су 24 испитаника или 50% (31 са оним без учесталости или 64.5%) позиционирала ово кривично дело најчешће у класичан криминалитет. Ово је и нормално с обзиром да га је веома тешко позиционирати у било којем другом облику криминалитета.

г. кривичних дела организованог криминала, корупције и других тешких кривичних дела

Табела 38. Питање бр.17 четврта алинеја

увек	често	понекад	ретко	никад	није унето
	5	7	9	1	24
	10.42	14.58	18.75	2.08	50

Две анкете садрже одговор под г без учесталости, што је укупно 24 одговора под г (50%)

У овом случају 12 одговора или 25% (14 са оним без учесталости, 29.16%) позиционира дело из чл.198 КЗ РС у област организованог криминала, корупције и других тешких кривичних дела. И овај одговор је разумљив с обзиром на перцепцију учесника у анкети који су и припадници УКП СБПОК-а.

Табела 39. Питање бр.17 последња алинеја

одговори	n	%
других КД	1	2.08
не знам	1	2.08
немам сазнања	1	2.08
није унето	45	93.75

Наведите посебна средства извршења овог кривичног дела на које сте наилазили у свом раду:

Табела 40. Питање бр.18

одговори	n	%
комуникација кроз затворене "SAAT" собе, у оквиру различитих игрица и слично	1	2.08
средства ИКТ	2	4.17
не знам	3	6.25
рачунар	1	2.08
уцена, принуда	1	2.08
софтвер	1	2.08

одговори	n	%
рачунар, интернет	2	4.17
писаним путем, електронским путем, медији	5	10.42
уџбеници, текстови у часописима, преузети текстови са интернета	1	2.08
нису коришћене компјутерске технике, посредна сазнања - коришћен је интернет	1	2.08
компјутер	1	2.08
дискови, књиге, рекламни материјали итд.	1	2.08
нисам наилазио	1	2.08
књиге публикације, рекламни материјали, дискови, музичке касете	1	2.08
није унето	26	54.17

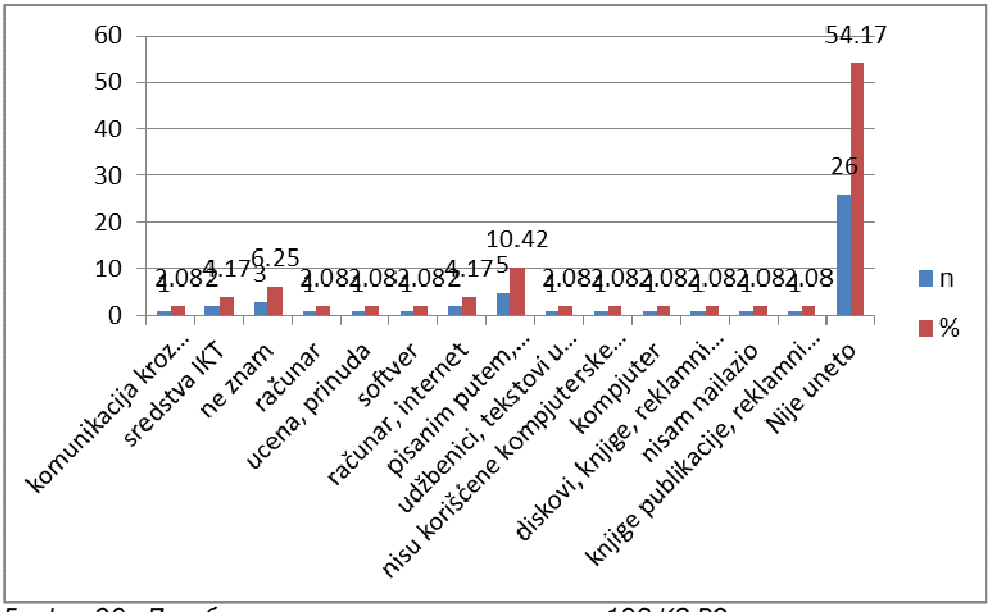


График 36. Посебна срдства извршења дела из чл.198 КЗ РС

У претходно описиваним одговорима овог типа указивано је на груписање одговора, па ће се том систематиком наставити и овде. Може се видети да је међу испитаницима било разлике у схватању средстава вршења, па тако имамо и начине и средства измешана у одговорима – софтвери, посебни облици комуникације специфичне софтверске техникае, предмети у којима се сублимира продукт ауторских права и слично. Највећи проценат испитаника није унео одговор на ово питање. Прелиминарном анализом се може утврдити да је актуелност у вршењу овог дела померила простор у виртуелно окружење, од којих предњаче средства ИКТ, рачунари, интернет, комуникација преко „SAAT“ затворених соба за чет. Један од понуђених одговора (2.08%) веома интересантно позиционира ово дело у дела

која се врше путем уцене или принуде. Смернице које би се могле дати у погледу поступања поводом овог дела, а у вези расветљавања дела и откривања учиниоца, могу се свести на отежавање приступа оваквим актима, пооштравање казнене политике према учиниоцима. Са друге стране интересантно је размотрити шта су све испитаници понудили као предмете, па је тако група предмета, који су објекат дела, посебно интересантна: текстови у часописима, рекламни материјал и публикације. Интересантност ових предмета је специфична за наше подручје, јер ко би се бавио рекламним материјалом у погледу искоришћавања ауторских права или неким публикацијама или текстовима у часописима.

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

Табела 41. Питање бр. 19

одговори	n	%
све расположиве	6	12.50
не знам	4	8.33
рачунар	1	2.08
анализа интернета, софтвер за анализу	1	2.08
интернет и рачунарске мреже	1	2.08
интернет, мобилна и фиксна телефонија, софтвер	5	10.42
интернет	3	6.25
интернет, надзор разговора и слично	1	2.08
примена до сада познатих технологија није дала добре резултате	1	2.08
ТВ, интернет, други медији	1	2.08
није унето	24	50.00

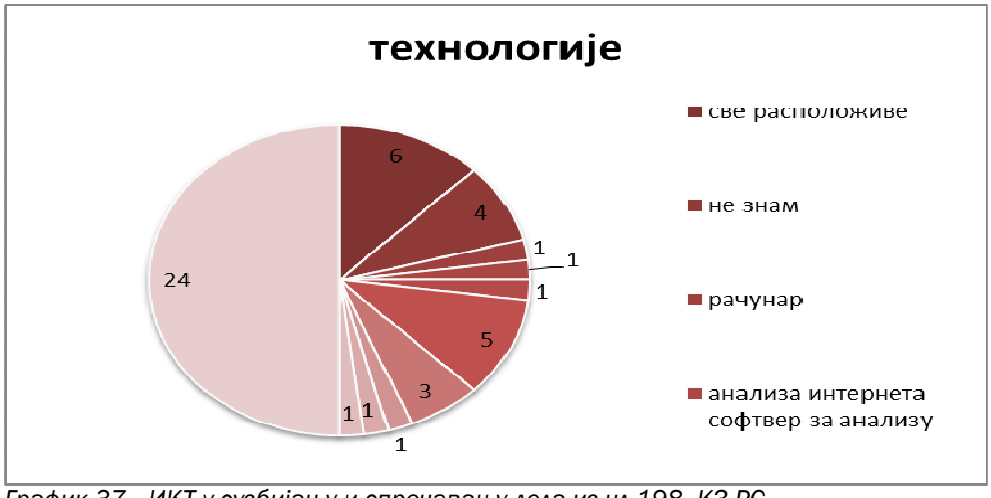


График 37. ИКТ у сузбијању и спречавању дела из чл.198. КЗ РС

Што се тиче средстава ИКТ, којима би се требало борити против овог кривичног дела, најбројнији одговор је све расположиво (6 испитаника - 12.5%), затим, интернет, мобилна и фиксна телефонија, софтвер (5 испитаника – 10.42% док је 3 испитаника навело само интернет – а што ипак чини овај одговор најбројнијим), не знам (4 испитаника – 8.33%), треба напоменути и да највећи број испитаника није унело одговор на ово питање (24 испитаника – 50%). Поред неколико интересантних одговора – нпр. анализа интернета – софтвер за анализу, могуће је констатовати да ни један испитаник није пружио конкретне начине и средства за борбу против извршилаца овог кривичног дела. У том смислу од значаја је да смо и ми у могућности да дамо поједине смернице у овом смислу. У погледу спречавања и сузбијања овог кривичног дела веома је интересантно размотрити мере предвиђене у СОПА у САД или Хадопи закон у Француској, којима се веома значајни резултати могу постићи у овој области, у погледу спречавања пиратерије која је у нашој земљи дефинитивно узела маха. Суштина мера јесте да се превентивни део активности препусти ИСП – овима и да се њима да оруђе којим би се корисницима њихових услуга ускратиле услуге на одређено време, а да то буде праћено реакцијом државе у смислу санкција према учиниоцу кривичног дела, које иду чак дотле да се одређеном лицу забрани коришћења интернета.

Ваше искуство са прибављањем предлога за кривично гоњење оваквих кривичних дела?

а. лако се прибављају (52.08%)

Табела 42. Питање бр. 20 прва алинеја

увек	често	понекад	ретко	никад	није унето
10	12	1	2		23
20.83	25.0	2.08	4.17		47.92

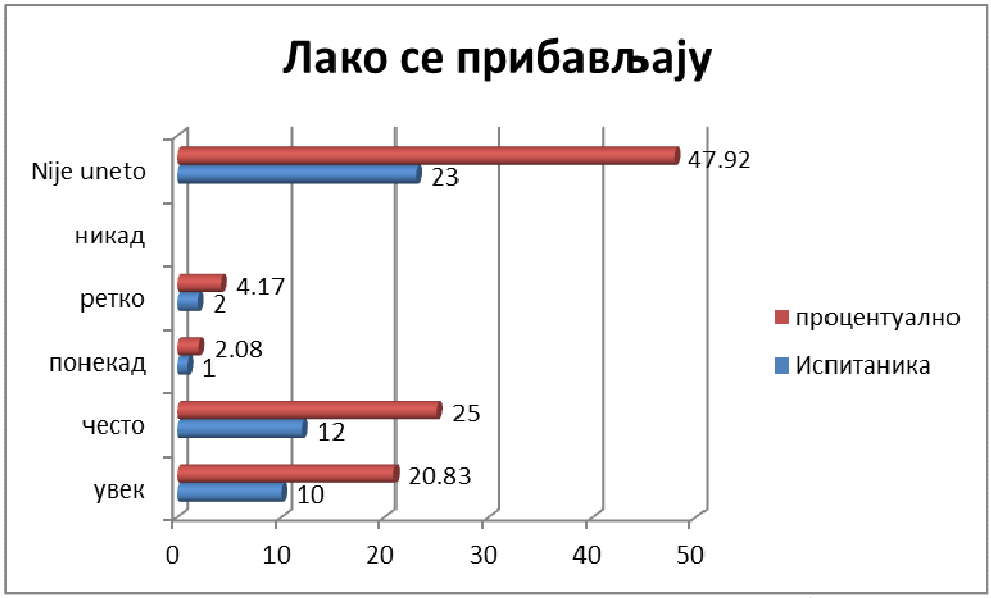


График 38. Предлози за гоњење дела из чл.198 КЗ РС – лакоћа прибављања

На основу анализе одговора могло би се закључити да 23 испитаника сматра да се предлози за кривично гоњење оваквих кривичних дела (чл.198 КЗ РС) релативно често (увек, често и понекад) добављају. Ово је јако значајан податак у светлу разумевања да се на други начин не би ни могли гонити учиниоци ових кривичних дела у другачијим околностима случајева. За овај одговор је могуће дати једну смерницу у вези свих представника носилаца права, где је веома лако од удружења лица која су носиоци права захтевати да се оформи један јаван регистар носилаца права и њихових заступника, како би се лако отклањале препреке које би подразумевале проналажење истих, чиме би се смањило време неопходно за тако нешто.

б. постоје одређенин проблеми

Табела 43. Питање бр.20. друга алинеја

увек	често	понекад	ретко	никад	није унето
	11	6	1	1	28
	22.92	12.5	2.08	2.08	58.33

Једна анкета садржи одговор под б без учесталости што је укупно 20 одговора под б (41.67%).

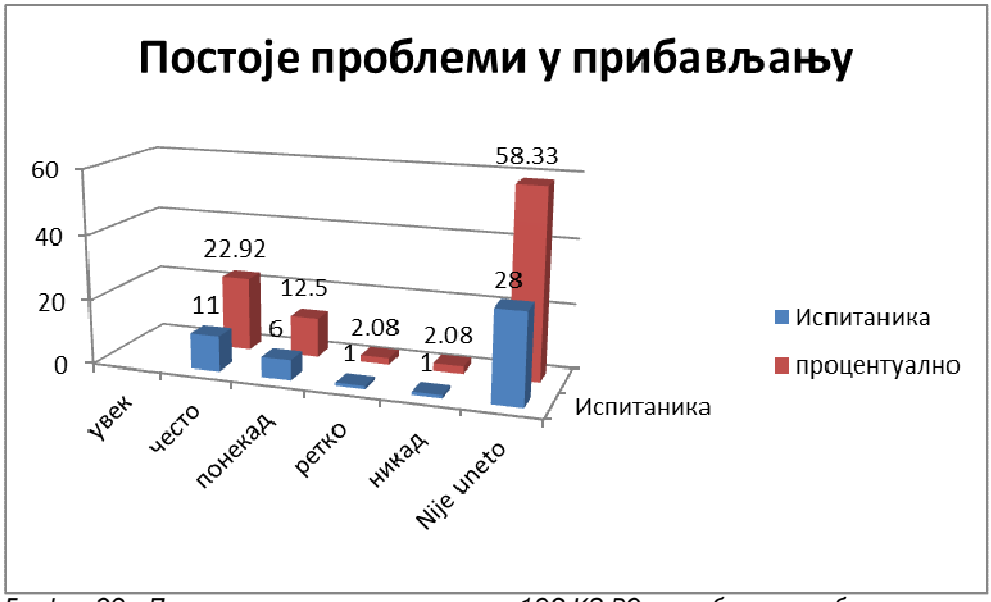


График 39. Предлози за гоњење дела из чл.198 КЗ РС – проблеми прибављања

Са друге стране коментари 17 испитаника (38.42%) нам указују да се они одређују у правцу постојања одређених проблема приликом прибављања предлога, али да они нису толико озбиљни да захтевају значајнију обраду.

в. најчешће се не добијају (22.92%)

Табела 44. Питање бр. 20 трећа алинеја

увек	често	понекад	ретко	никад	није унето
	1	2	5	3	37
	2.08	4.17	10.42	6.25	77.08

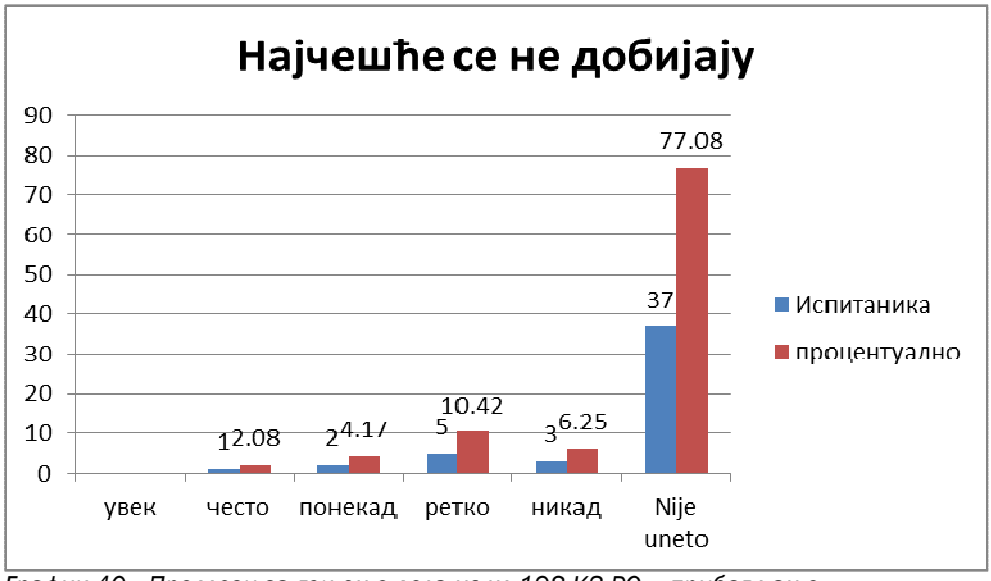


График 40. Предлози за гоњење дела из чл.198 КЗ РС – прибављање

У овом случају 3 испитаника (6.25%) указују на недобијање ових предлога.

Табела 45. Питање бр.20. последња алинеја

	n	%
не знам	3	6.250
немам искуства са 198	1	2.083
предлог	1	2.083
немам искуства	1	2.083

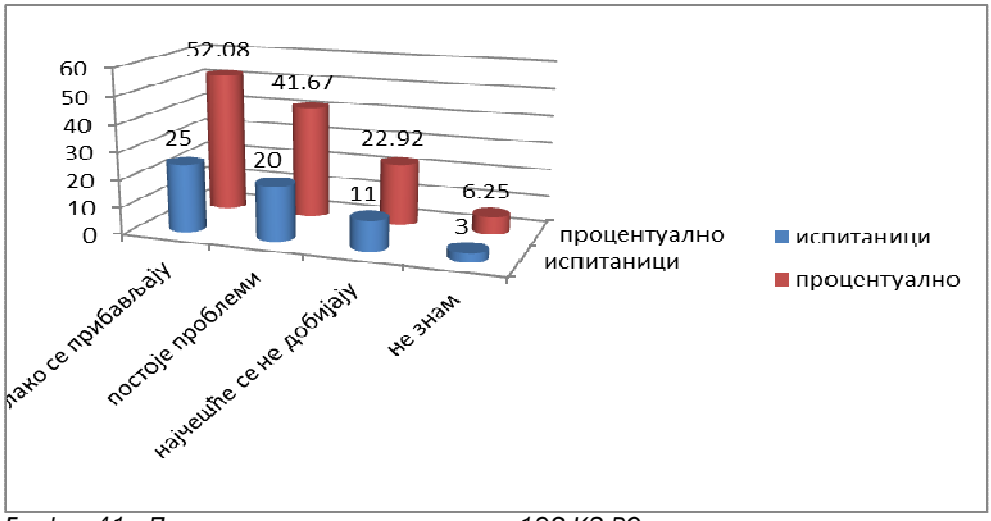


График 41. Предлози за гоњење дела из чл.198 КЗ РС – скупно

Генерално, најчешће нема проблема са привабљањем предлога за кривично гоњење у овом случају (25 испитаника или 52.08%), али је велики проценат код којег постоји неки проблем или када се ови предлози не добијају (20 испитаника са проблемима, односно 11 без добијања предлога што је укупно 64.59%).

Неовлашћено искоришћавање ауторског дела или предмета сродног права члан 199, према Вашем искуству се најчешће гоне:

а. основни облици кривичног дела

Табела 46. Питање бр. 21. Прва алинеја

увек	често	понекад	ретко	никад	није унето
13	18	1	1		11
27.08	37.5	2.08	2.08		22.92

Четири анкете садрже одговор под а без учесталости што је укупно 37 одговора под а (77.08%)

График 42. Дисперзија основног облика дела из чл.199 КЗ РС

Учесталост извршења појединих облика кривичног дела из чл.199 КЗ РС према анализи анкете је следећа – основни облик је са значајном учесталошћу одређен у 32 одговора (66.66%).

б. тежи облик

Табела 47. Питање бр. 21 друга алинеја

увек	често	понекад	ретко	никад	није унето
4	8	10	3		21
8.33	16.67	20.83	6.25		43.75

Две анкете садрже одговор под б без учесталости што је укупно 27 одговора под б (56.25%)

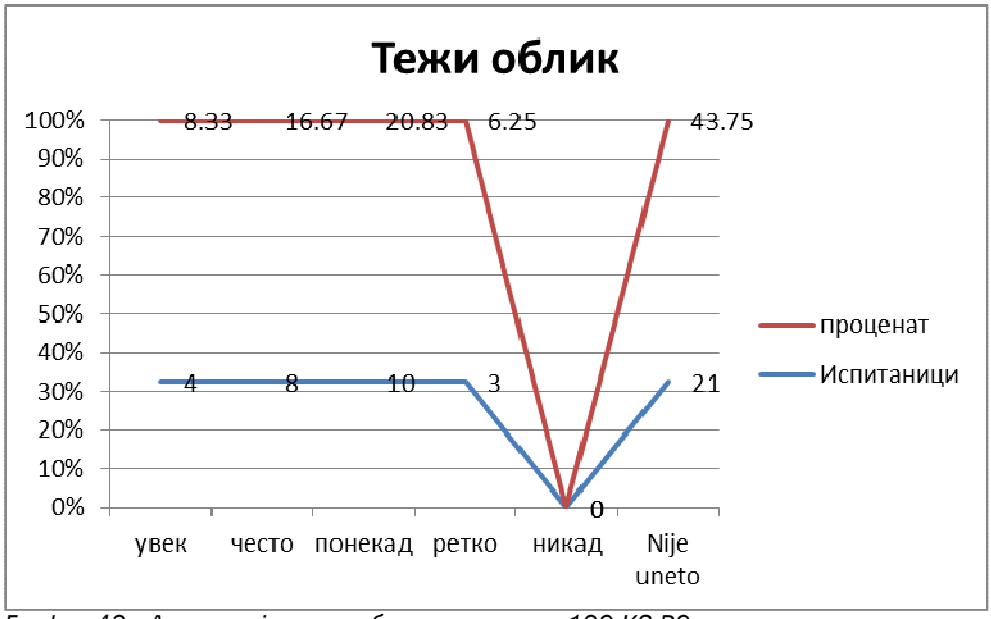


График 43. Дисперзија тежег облика дела из чл.199 КЗ РС

Тежи облик је заступљен са значајном учесталошћу у 22 случаја (45.83%) .

в. посебни облик (29.17%)

Табела 48. Питање бр. 21 трећа алинеја

увек	често	понекад	ретко	никад	није унето
	5	6	3		34
	10.42	12.5	6.25		70.83

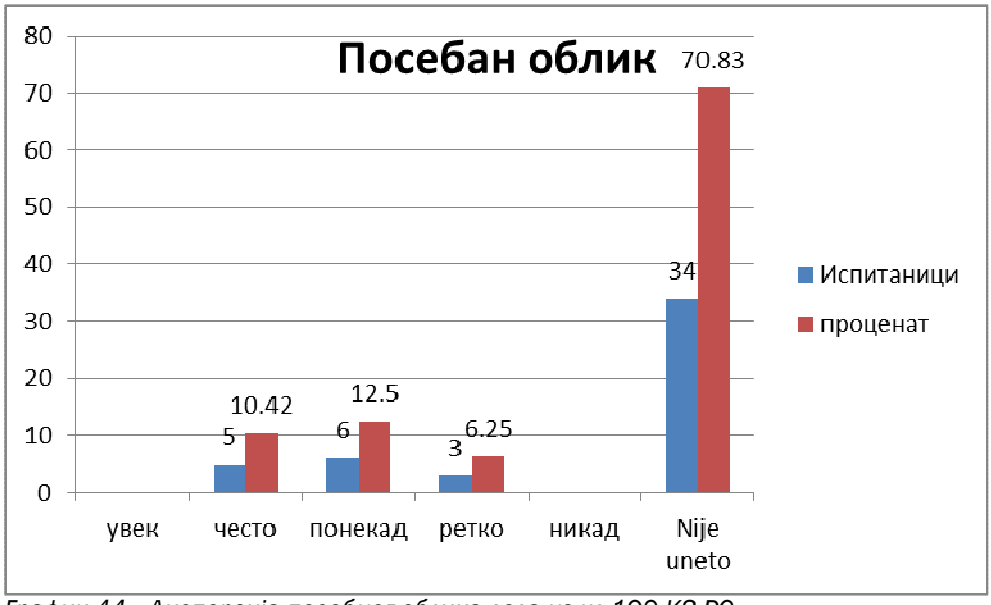


График 44. Дисперзија посебног облика дела из чл.199 КЗ РС

Посебан облик заступљен је по учесталости у релативној учесталости од 11 одговора (22.92%)

г. припремне радње за извршење овог дела (20.83%)

Табела 49. Питање бр. 21 четврта алинеја

увек	често	понекад	ретко	никад	није унето
	1	3	2	7	38
	2.08	6.25	4.17	8.33	79.17

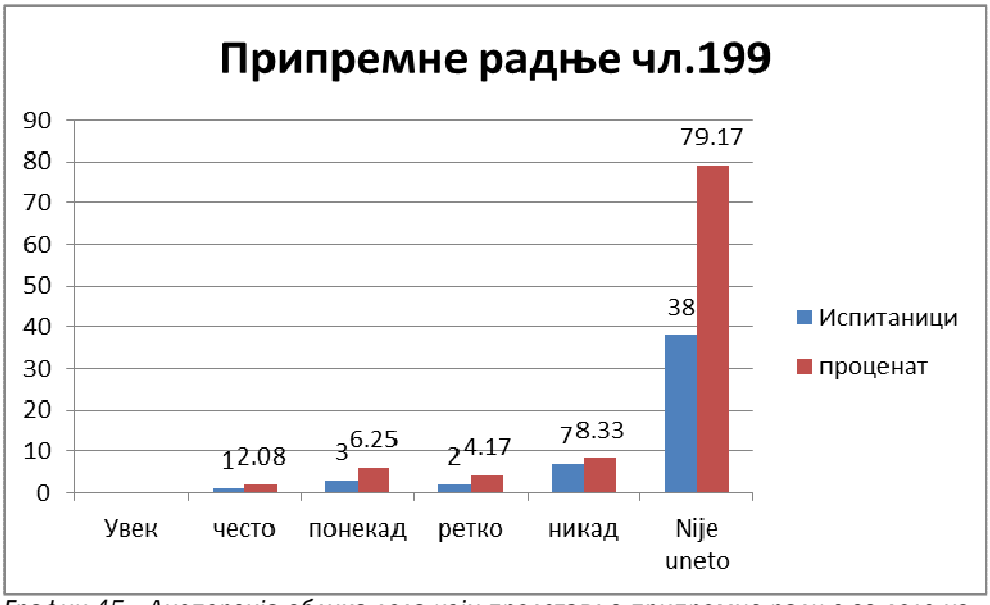


График 45. Дисперзија облика дела који представља припремне радње за дело из чл.199 КЗ РС

Овде је од значаја анализирати број од испитаника 9 испитаника (12.5%) који су изнели да ово није учестала појава јер се ретко или никада не јавља у пракси.

д. један одговор – не знам (2.08%)

Табела 50. Питање бр. 21. збирно

	основни облик	тежи облик	посебан облик	припремне радње за извршење овог дела	не знам
испитаници	37	27	14	13	1
процентуално	77.08	56.25	29.17	20.83	2.08

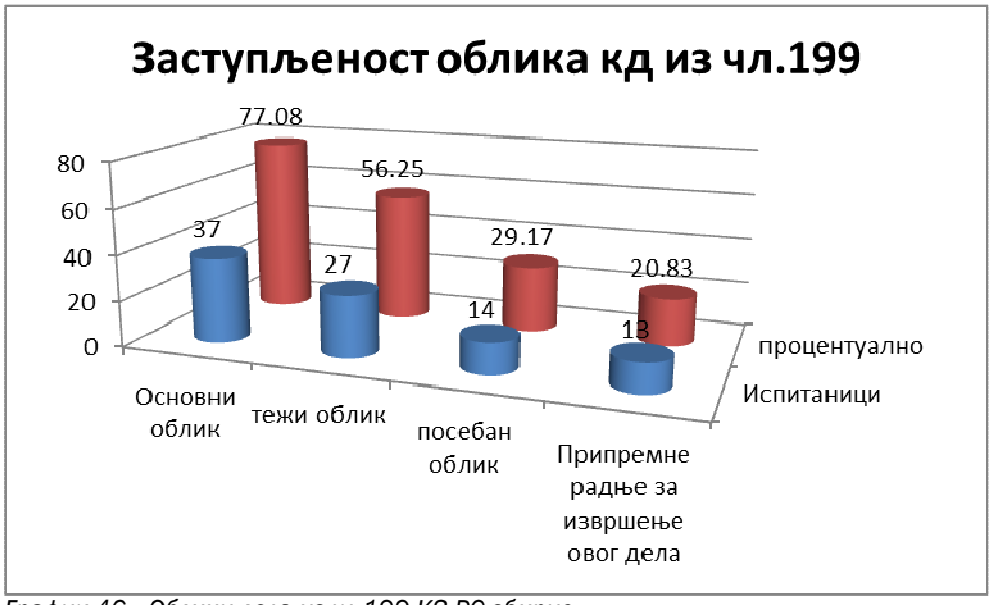


График 46. Облици дела из чл.199 КЗ РС збирно

Можемо видети да је уопштена заступљеност највећа за основни облик овог дела, 37 одговора што чини 77.08% испитаника, 27 за тежи облик или 56.25%, 14 за посебан облик или 29.17% и 13 испитаника за припремне радње или 20.84% од укупног броја испитаника.

Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду.

Табела 51. Питање бр. 22

а. списак из закона и	34	70.83
б. не знам	10	20.83
није одговорено	4	8.33

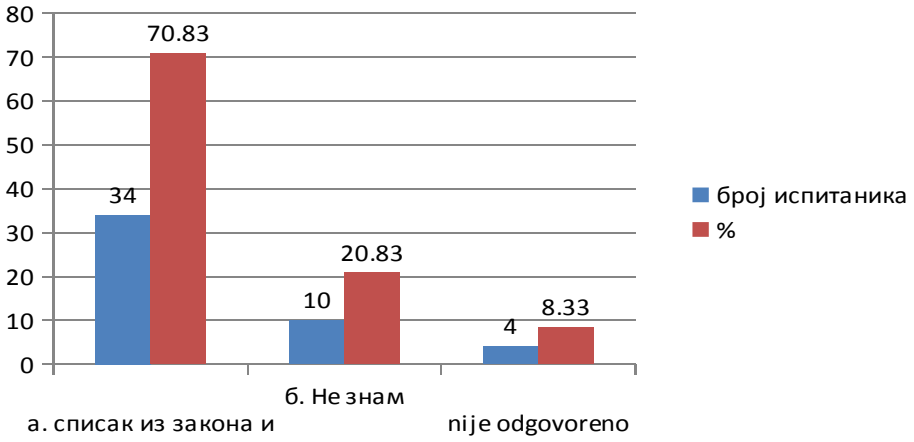


График 47. Дисперзија начина извршења дела из чл.199 КЗ РС

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела?

Табела 52. Питање бр. 23

	n	%
све расположиве	6	12.50
не знам	6	12.50
рачунарске мреже	1	2.08
рачунар	1	2.08
софтвер за анализу интернет саобраћаја, мере надзора	1	2.08
рачунар, интернет, посебни уређаји за обраду звука и слике	1	2.08
интернет, мобилна и фиксна телефонија, софтвер	5	10.42
интернет	4	8.33
надлежност вишег, а не основног ЈТ	1	2.08
претрага огласа на мрежама и интернет сајтовима	1	2.08
примена до сада познатих технологија није дала добре резултате	1	2.08
ТВ, интернет, други медији	1	2.08
није унет одговор	19	39.58

Одговор на ово питање показује сличне тенденције као са претходним.

График 48. ИКТ у сузбијању и спречавању дела из чл.199 КЗ РС

Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима, члан 200 КЗ РС најчешће се врше:

Табела 53. Питање бр.24

	n	%
а. посебним уређајима	20	41.67
б. посебним рачунарским програмима	31	54.58
в. друго	2	4.17

График 49. Дисперзија појавних облика дела из чл. 200 КЗ РС

Ово кривично дело врши се најчешће посебним рачунарским програмима – 31 одговору (54.58%), посебним уређајима према 20 одговора – 41.67% испитаника. Интересантно је да 2 одговора нуде варијанту других средстава којима се врши ово кривично дело, без неког значајнијег прецизирања. У погледу смерница које се могу дати у овој области неопходно је инкриминисати неовлашћену продају и дистрибуцију уређаја који се у овом смислу могу користити или инкриминисати припремне радње.

Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

Табела 54. Питање бр. 25

одговори	n	%
а.неовлашћено уклањање или измена електронске информације о ауторском или сродном праву	23	47.92
б. стављањем у промет, увозом, извозом, емитовањем или на други начин јавним саопштавањем ауторског дела или предмета сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена	17	35.42
в. на други начин	6	12.5

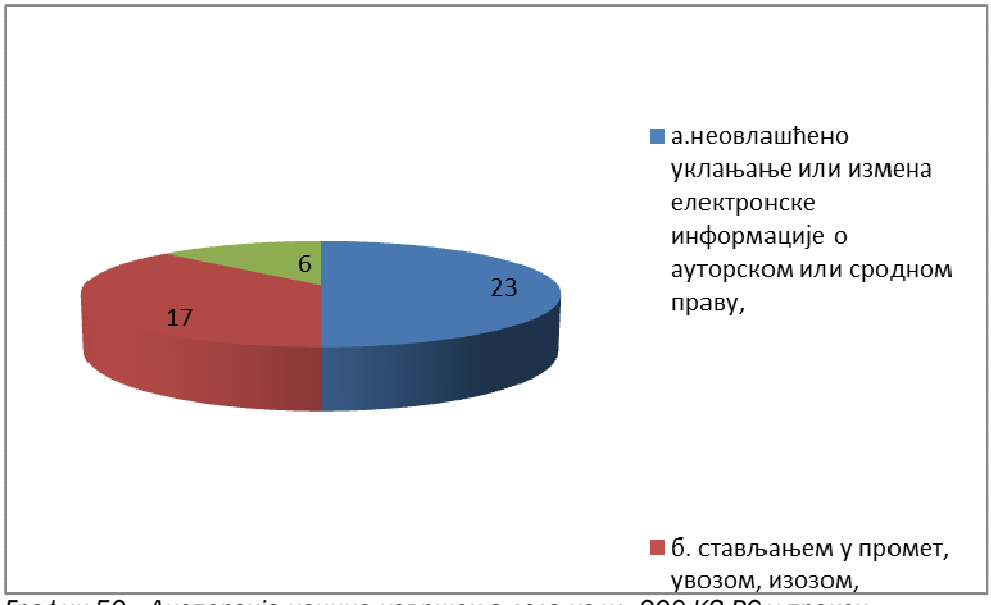


График 50. Дисперзија начина извршења дела из чл. 200 КЗ РС у пракси

Најчешћи начин извршења кривичног дела из чл. 200 КЗ РС у пракси је први појавни облик који се јавља у 23 одговора или 47.92%, а следећи по учесталости је други појавни облик 17 одговора или 35.42%.

Које информационокомуникационе технологије би требало користити у сузбијању и спречавању овог дела?

Табела 55. Питање бр. 26

одговори	n	%
све расположиве	6	12.50
не знам	6	12.50
рачунарске мреже	1	2.08
рачунар	1	2.08
мере надзора, вештачење	1	2.08
интернет, рачунарске мреже, програми за електронску претрагу података	1	2.08
интернет, мобилна и фиксна телефонија, софтвер	5	10.42
интернет	3	6.25
надлежност вишег, а не основног ЈТ	1	2.08
претрагом база носилаца ауторских права	1	2.08
ТВ, интернет, други медији	1	2.08
није унет податак	21	43.75

Одговор на ово питање показује сличне тенденције претходним.

Како се утврђују носиоци ових права, која се штите овим делом (чл. 200 КЗ РС)?

Табела 56. Питање бр. 27

одговори	n	%
постоји евиденција о носиоцима код ЗИС-у, колективна организација и агенције за ауторска права	1	2.08
преко Завода за интелектуалну својину	3	6.25
уговором	1	2.08
коелктивним системом заштите кроз разне организације преко Завода за интелектуалну својину	1	2.08
појединачно и колективно	1	2.08
законом	1	2.08
проверама	1	2.08
најчешће су они за који пријављују извршење КД	1	2.08
не знам	4	8.33
доказивањем правног основа суштинског права	1	2.08
доказивањем правног основа, ауторство	1	2.08

доказивањем правног основа ауторска права	1	2.08
доказивањем правног основа	2	4.17
увидом у јединствени регистар аутора	1	2.08
увидом у регистре	1	2.08
надлежност вишег, а не основног ЈТ	1	2.08
претрагом база носилаца ауторских права	1	2.08
на начин на који се иначе утврђује информација о ауторским и сродним правима као и на основу изјаве сведока	1	2.08
путем утврђивања самог ауторског дела, претраживањем база података доступних на интернету	1	2.08
преко СОКОЈ-а, преко ПКС-а и њихове евиденције носилаца ових права	1	2.08
носилац обично подноси пријаву или се провером утврђује носилац права	1	2.08
увидом у регистар аутора	1	2.08
преко аутора или фирме која је ставила на сајт електронску информацију	1	2.08
преко регистра аутора	1	2.08
није унет податак	18	37.50

График 51. Начини утврђивања носилаца права – оштећених делом из чл. 200 КЗ РС

Као најчешћи одговори на ово питање јављају се: увидом у евиденције и регистре или претрагом база података - 6 одговора 12.5%, затим доказивањем правног основа - 3 одговора 6.25%, о овој проблематици је већ на претходним странама било речи, па се могу поновити смернице из поменутог.

Наведите начине извршења кривичног дела превара (члан 208 КЗ), а које не спадају у КД из чл. 301 КЗ и његове облике на које сте наилазили:

Табела 57. Питање бр. 28

одговори	n	%
а. ко у намери да себи или другом прибави противправну имовинску корист, доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини	44	91.67
б. дело учињено само у намери да другог оштети	16	33.33
в. када је делом из ст. 1 и 2 овог члана прибављена имовинска корист или је нанета штета у износу који прелази 450 хиљада динара	25	52.08
г. када је делом из ст. 1 и 2 овог члана прибављена имовинска корист или је нанета штета у износу који прелази милион и петсто хиљада динара	22	45.83
д. не знам	4	8.33

График 52. Дисперзија појавних облика дела из чл. 208 КЗ РС

Најбројнији је први облик овог дела – 44 одговора или 91.67%, затим први тежи облик – 25 одговора или 52.08%, па други тежи облик – 22 одговора или 45.83%, а потом посебан облик – 16 одговора или 33.33%. Веома је значајно указивање наших испитаника на специфичности кривичног дела преваре из чл. 208 КЗ у односу на дело из чл. 301 КЗ и наравно као најчешћи облик се јављао основни облик, али је значајно и указивање на заступљеност тежег облика.

Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

Табела 58. Питање бр. 29

одговори	n	%
све расположиве	7	14.58
не знам	7	14.58
рачунарске мреже	1	2.08
рачунар	1	2.08
мере надзора интернета и телефона	1	2.08
интернет, рачунари	1	2.08
фиксна, мобилна телефонија, интернет	5	10.42
интернет	3	6.25
надлежнот ВТК у вишем ОЈТ	1	2.08
базе података у правосудним системима и осталим системима	1	2.08
ТВ, интернет, други медији	1	2.08
није унет податак	19	39.58

Одговор на ово питање показује тенденције сличне претходним.

У ком обиму се ова дела врше само у циљу наношења штете другоме као привилегованом облику овог дела?

Табела 59. Питање бр. 30

	n	%
увек	1	2.08
често	3	6.25
понекад	10	20.83
ретко	27	56.25
никад	1	2.08
није унето	6	12.50

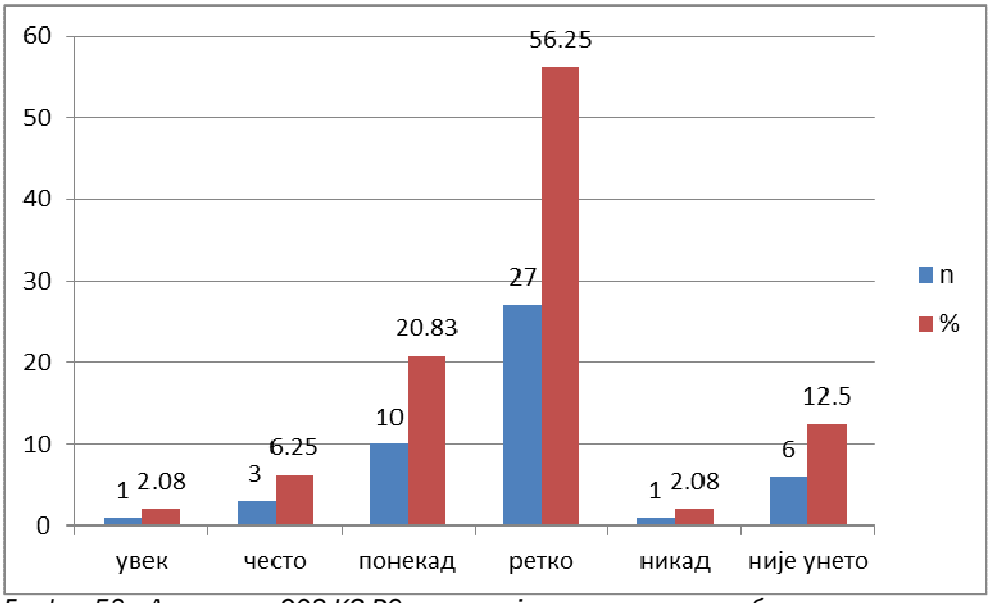


График 53. Дело из чл. 208 КЗ РС дисперзија привилегованог облика

Анализом ових одговора долазимо до резултата да се у 14 одговора (29.16%) често јавља овај облик кривичног дела, али и да, са друге стране, 28 испитаника (58.33%) опредељује ово дело као ретко или да га никада нису у својој пракси сусрели у овом облику. У том смислу веома је значајно разумети учесталост појаве вршења овог дела у сврху наношења штете другоме, као једног од пакосних начина вршења кривичних дела са простим циљем и намером наношења штете. Исто говори о извршиоцима, њиховим личностима и њиховим мрачним побудама, а са друге стране говори и о заступљености овакве мотивације у овој области кривичних дела.

Наведите начине извршења кривичног дела фалсификовање и злоупотреба платних картица из члана 225 и његове облике на које сте наилазили.

Табела 60. Питање бр. 31

одговори	n	%
прављење лажних или преиначење правих платних картица. Углавном се нове платне картице праве помоћу података прибављених са компромитованих рачуна, услед необезбеђеног система плаћања, који је коришћен од стране оштећеног приликом трансакције	1	2.08
преављење лажне платне картице, преиначење праве ради употребе, неовлашћеном употребом туђе платне картице или поверљивих података који уређују ту картицу	1	2.08
превљење лажне платне картице, преиначење праве ради употребе, неовлашћеном употребом туђе платне картице или поверљивих података који уређују ту платну картицу	1	2.08

одговори	n	%
употребом картице, прављењем лажне картице	1	2.08
употреба туђе картице, прибављање података у намери употребе	1	2.08
неовлашћена употреба личних података о платним картицама на интернету, скимовање платних картица, фишинг..	1	2.08
скимовањем долази до података о картици и онда се она фалсификује	1	2.08
било их је више	1	2.08
скиминг	1	2.08
скиминг, фишинг...	1	2.08
куповина (плаћање) путем интернета, злоупотреба картица на банкоматима	1	2.08
клониране картице, дамлови	1	2.08
скиминг, фишинг	1	2.08
крађа картице и дизање новца са туђом картицом	1	2.08
не знам	1	2.08
неовлашћена употреба поверљивих података	1	2.08
неовлашћрна употреба поверљивих података, превенција лажних картица	2	4.17
неовлашћена употреба поверљивих података, прављење лажних копија	2	4.17
неовлашћена употреба туђе картице	1	2.08
употреба лажне картице као праве, неовлашћена употреба туђе картице, набављање лажне картице ради употребе као праве	1	2.08
употреба лажне платне картице као праве у циљу присвајања против правне имовинске користи, неовлашћена употреба туђе картице	1	2.08
скимовање	1	2.08
прављење лажних, употреба лажних, употреба туђе картице	1	2.08
законски текст	1	2.08
процесуирање правних лица и страних држављана	1	2.08
прављене, преиначене праве, употреба праве картице	1	2.08
непосредно 225 ст. 4 неовлашћена употреба туђе картице, посредно 225 ст. 1	1	2.08
члан 225, ст. 1, ст. 4 КЗ	1	2.08
злоупотреба платне картице, сачињавање лажне картице	2	4.17
фалсификовање платних картица и кредитних картица на штету иностраних фондова, неовлашћена употреба картица	1	2.08
издавање меница без покрића, члан 228 ст. 2 и ст. 3	1	2.08

одговори	n	%
прављење или преиначавање картице или употреба туђе	1	2.08
употреба лажне картице као праве, неовлашћена употреба туђе картице	1	2.08
најчешће ст. 4	1	2.08
прављење, преиначавање, употреба	1	2.08
најчешће по основу става 4	1	2.08
није унето	9	18.75

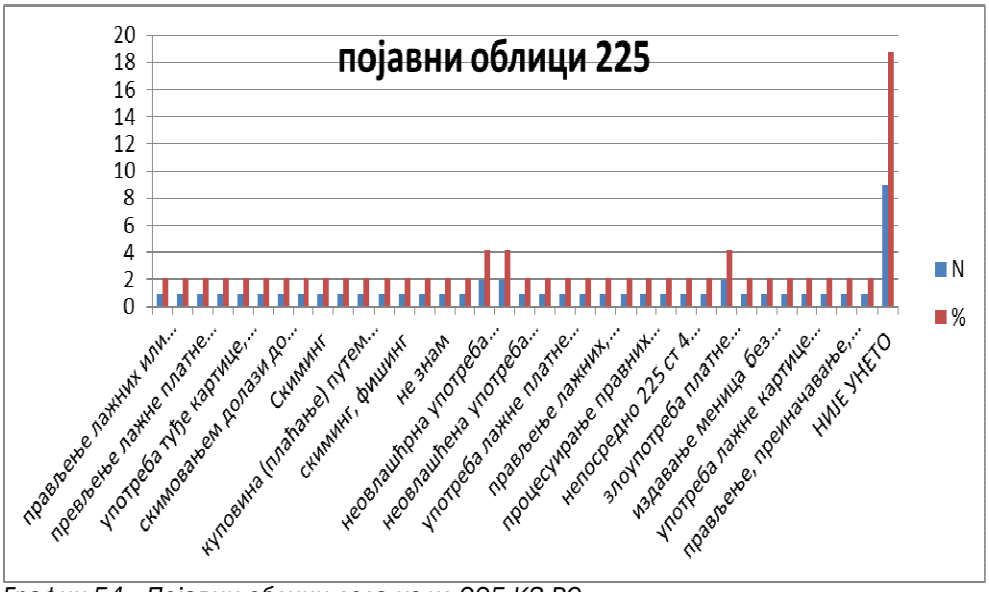


График 54. Појавни облици дела из чл.225 КЗ РС

Видимо да је процентуално најчешћи резултат вредности који није унет, 9 одговора (18.75%), али анализом одговора долазимо до 21 одговора који означавају 43.75% укупних одговора, а представљају облик кривичног дела које подразумева крађу или на преваран начин прибављање података у вези са платним картицама у циљу њихове злоупотребе и само злоупотребљавање овим путем, затим 17 одговора 35.42% у одговорима првог облика. Ова инкриминација омогућила је гоњење кривичних дела фишинга, али у том смислу треба ићи и даље, тј. инкриминисати и само прибављање ових података и њихово нуђење на продају.

У ком обиму се појављује облик овог кривичног дела из ст. 4 којим се инкриминише неовлашћена употреба туђе картице или података о личности власника картице и шифара које уз њу иду.

Табела 61. Питање бр.32

одговори	n	%
увек	7	14.58
често	27	56.25
понекад	7	14.58
ретко	2	4.17
никад	2	4.17
није унето	3	6.25

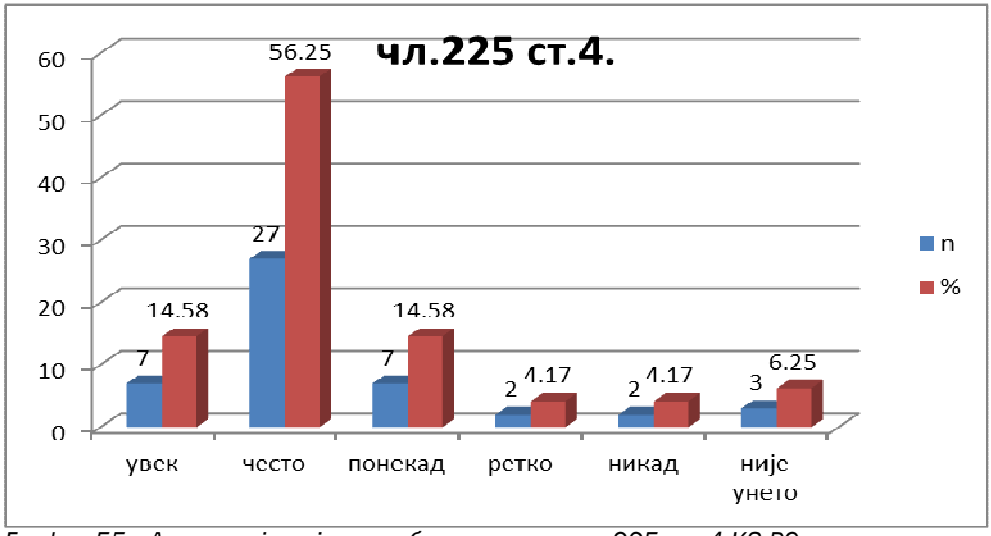


График 55. Дисперзија појавног облика дела из чл. 225 ст. 4 КЗ РС

Из приложеног се може закључити да је према 41 одговору (93.51%) учесталост облика који представља прибављање података у намери злоупотребе путем картица (неовлашћена употреба туђе картице или података о личностивласника картице и шифара које иду уз исте).

У ком обиму облик из ст. 5 инкриминише набављање лажне платне картице у намери њене употребе као праве или прибављање података у намери да се исти искористе за прављење лажне платне картице?

Табела 62. Питање бр. 33

одговори	n	%
увек	7	14.58
често	21	43.75
понекад	14	29.17
ретко	1	2.08
никад	1	2.08
није унето	4	8.33

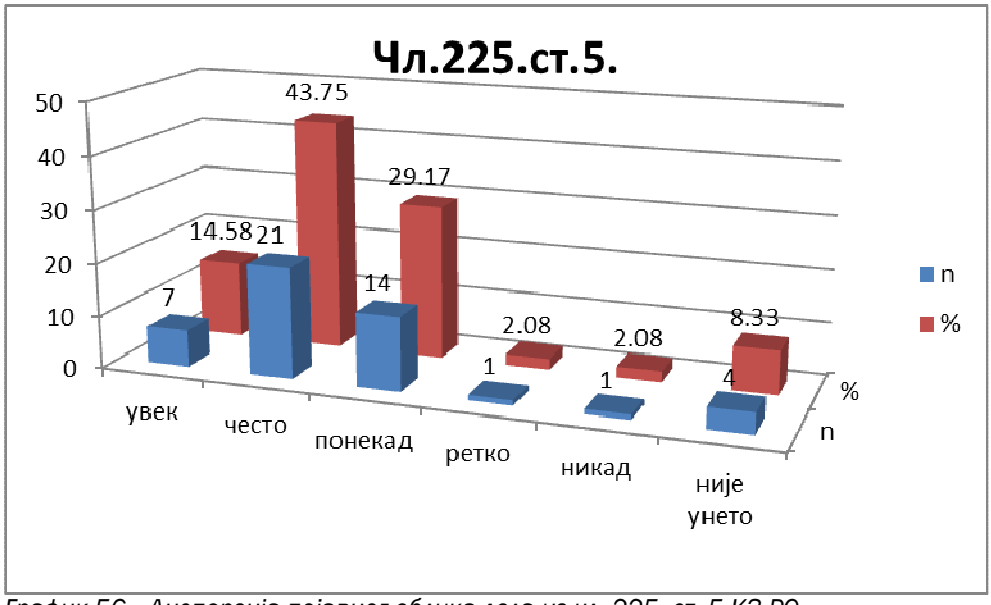


График 56. Дисперзија појавног облика дела из чл. 225 ст. 5 КЗ РС

Оно што је занимљиво јесте да се може извести закључак да је према 42 одговора (77.5%) испитаника ово чест облик кривичног дела из чл. 225 ст. 5 КЗ РС. Овај облик треба истаћи као чешћи облик кривичног дела и посебно треба размислити о његовом криминално политичком значају, као и о пооштравању казнене политике у погледу овог дела.

Наведите начине извршења кривичног дела оштећење рачунарских података и програма из члана 298 КЗ и његове облике на које сте наилазили.

Табела 63. Питање бр. 34

одговори	н	%
а. неовлашћено брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма	33	68.75
б. уколико је делом из става 1 овог члана проузрокована штета у износу који прелази 450 хиљада динара.	13	27.08
в. уколико је делом из става 1 овог члана проузрокована штета у износу који прелази милион и петсто хиљада динара,	10	20.83
г. неки други	4	8.33

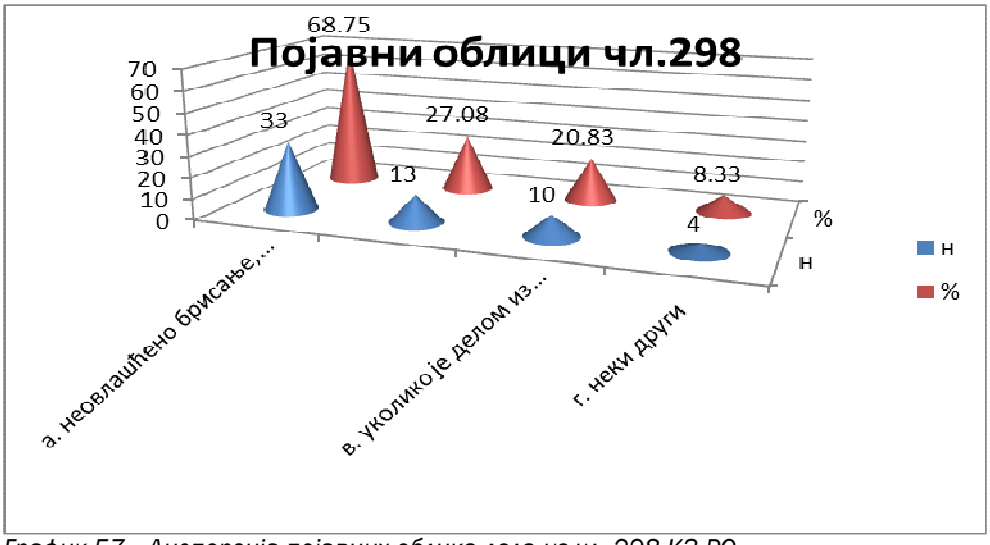


График 57. Дисперзија појавних облика дела из чл. 298 КЗ РС

Према одговорима 33 испитаника (68.75%) основни облик овог кривичног дела је најчешћи облик у пракси, следећи по учесталости први је тежи облик са 13 одговора (27.08%), а потом и други тежи облик са 10 одговора (20.83%).

Инкриминација овог дела (чл. 298 КЗ) оправдана је у тежем облику за износ штете који прелази 450 000 динара.

Табела 64. Питање бр. 35

одговори	н	%
а. јесте	21	43.75
б. није оправдана	3	6.25
в. могла је бити и у мањем износу	5	10.42
г. могла је бити и у већем износу	2	4.17
д. не знам	6	12.50

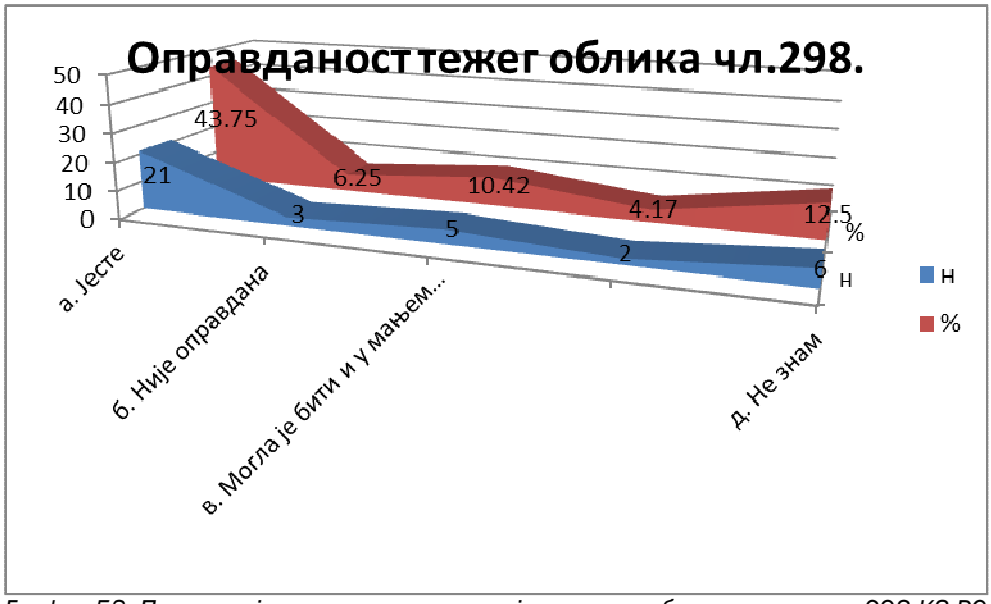


График 58. Перцепција оправданости постојања тежег облика дела из чл. 298 КЗ РС

У погледу резултата овог питања може се видети да је 21 испитаник (велика већина њих 43.75%) сматрао оправданим износ новца неопходан за квалификацију тежег облика дела, али је такође интересантно и да укупно 10 испитаника (20.83%) ово доводи у питање. Питање оправданости се може посматрати на начин како су наши испитаници видели, и у смислу ниског и у смислу високог прага за квалификацију, али и могућности да није оправдано његово постојање.

Наведите начине извршења кривичног дела рачунарска саботажа из члана 299 КЗ и његове облике на које сте наилазили.

Табела 65. Питање бр. 36

одговори	н	%
а. уношењем, уништењем, брисањем, изменом, оштећењем, прикривањем или на други начин чињењем неупотребљивим рачунарског податка или програма	31	64.58
б. уништењем или оштећењем рачунара или другог уређаја за електронску обраду и пренос података	17	35.42
в. не знам	7	14.58

График 59. Дисперзија појавних облика дела из чл. 299 КЗ РС

Према најбројнијој групи одговора на ово питање први основни облик је знатно заступљенији у пракси (31 одговор или 64.58%) у односу на други (17 одговора или 35.42%). Такође ћемо моћи извести закључак да 14.58% испитаника (7 одговора) не може дати ове податке јер није у практичном смислу могло да сретне ова дела. Оно што је из овог резултата значајно јесте да се перфиднији облик, који би ишао ка уништењу или оштећењ,у ипак мање јавља или је мање заступљен, што је јако добро.

У којој мери је ово дело различито од кривичног дела прописаног делом оштећење рачунарских података и програма?

Табела 66. Питање бр.37

одговори	n	%
зато јер није "неовлашћен приступ", дакле може то да учини и нпр. запослени који је овлашћено службено лице	1	2.08
намера онемогућавања поступака електронске обраде који су од значаја за државне органе	1	2.08
намера онемогућавања поступака електронске обраде који су од значаја за државне органе, јавне службе, ...	1	2.08
разлика је у оштећењу сервиса који су од важности за предузећа или појединце	1	2.08
примењује се за државне органе јавне службе и друге	1	2.08
гони се када су у питању владине институције, јавна предузећа, државни органи итд.	1	2.08
врло су слична, овисно о чињеницама у току истраге врши се квалификација	1	2.08
разликује се	1	2.08
односи се на државне органе или органе од јавног значаја	1	2.08
тотално непотребан систем	1	2.08
не знам	5	10.42
у намери да се онемогући или омете рад државних органа и јавних предузећа	1	2.08
у намери да се онемогући или знатно омете рад државних органа и јавних установа	4	8.33
разликују се по врсти умишљаја	1	2.08
битан елемент је ометање података од значаја за државне органе, а код чл. 298 проузрокована је штета	1	2.08
разлика је у намери	1	2.08
код саботаже је потребна намера да се онемогући или омете поступак електронске обраде података	1	2.08
немам искуства	1	2.08
субјективни елемент дела, намера, као и последица у знатној мери разликују дела	1	2.08
није унето	22	45.83

График 60. Перцепција разлике рачунарске саботаже и оштећења рачунарских података

Анализом се утврђује да у 10 одговора (20.84%) намера има кључни значај у разликовању ових дела за практичаре, али такође је од значаја и да 22 одговора (45.83%) нису унета, односно да 6 одговора (12.5%) носи одредницу да не зна разлику или нема искуства у тој области.

Наведите начине извршења кривичног дела прављење и уношење рачунарских вируса члан 300 и његове облике на које сте наилазили.

Табела 67. Питање бр. 38

одговори	n	%
а. прављење рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу	26	54.17
б. уношење рачунарског вируса у туђ рачунар или рачунарску мрежу и тако проузроковање штете	29	60.42
в. не знам	8	16.67

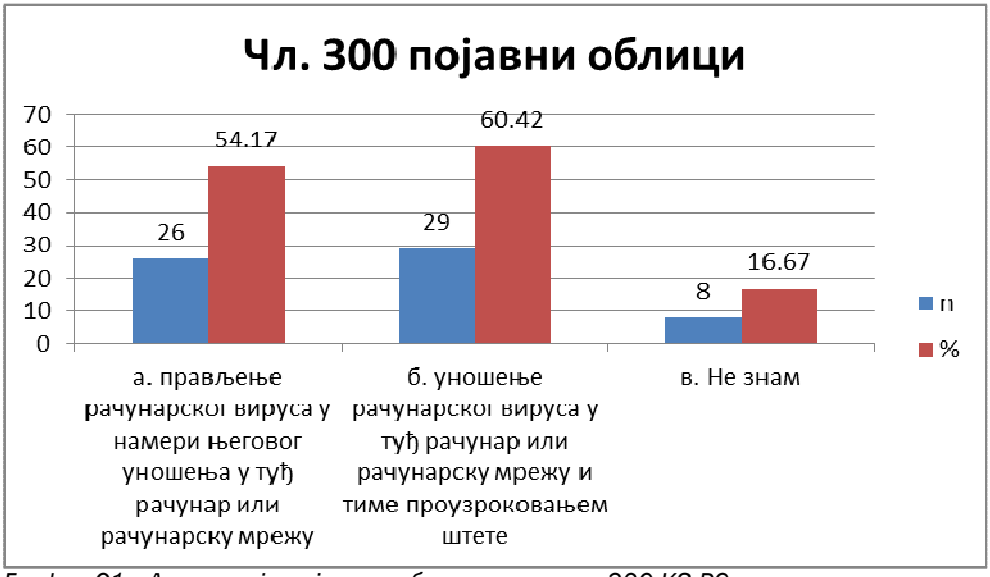


График 61. Дисперзија појавних облика дела из чл.300 КЗ РС

Анализом овог питања у вези дела из чл. 300 КЗ РС видећемо да је други основни облик (уношење рачунарског вируса у туђ рачунар или рачунарску мрежу и тако проузроковање штете) најфреквентнији облик овог дела, према 29 одговора (60.42%%), док је први појавни облик следећи по учесталости, према 26 одговора (54.17%) који се односи на прављење рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу. Од значаја је у том смислу дати смернице у погледу пооштравања казнене политике, односно покушајима додатне инкриминације у овој области.

Колико је прављење рачунарских вируса у намери уношења у рачунар и рачунарску мрежу?

Табела 68. Питање бр. 39

одговори	n	%
увек	6	12.50
често	18	37.50
понекад	11	22.92
ретко	2	4.17
није унето	11	22.92

График 62. Учесталост дела из чл. 300 КЗ РС

Анализом одговора на ова питања може се закључити да је вршење овог дела релативно учесталије у облику прављења вируса у намери уношења у рачунар или у мрежу у укупном броју од 35 одговора (72.92%). Исто показује и правац у којем би требало деловати у смислу проактивног поступања, али и генералне и специјалне превенције.

Наведите начине извршења кривичног дела рачунарска превара члан 301 и његове облике на које сте наилазили:

Табела 69. Питање бр. 40

одговори	n	%
а. уношење нетачног податка, пропуштање уношења тачног податка или на други начин прикривање или лажно приказивање података и тиме утицање на резултат електронске обраде и преноса података	31	64.58
б. ако је делом из става 1 овог члана прибављена имовинска корист која прелази износ од 450 хиљада динара	13	27.08
в. уколико је делом из става 1 овог члана прибављена имовинска корист која прелази износ од милион и петсто хиљада динара, учинилац ће се казнити затвором од две до десет година	11	22.92
г. када дело учини само у намери да другог оштети	9	18.75

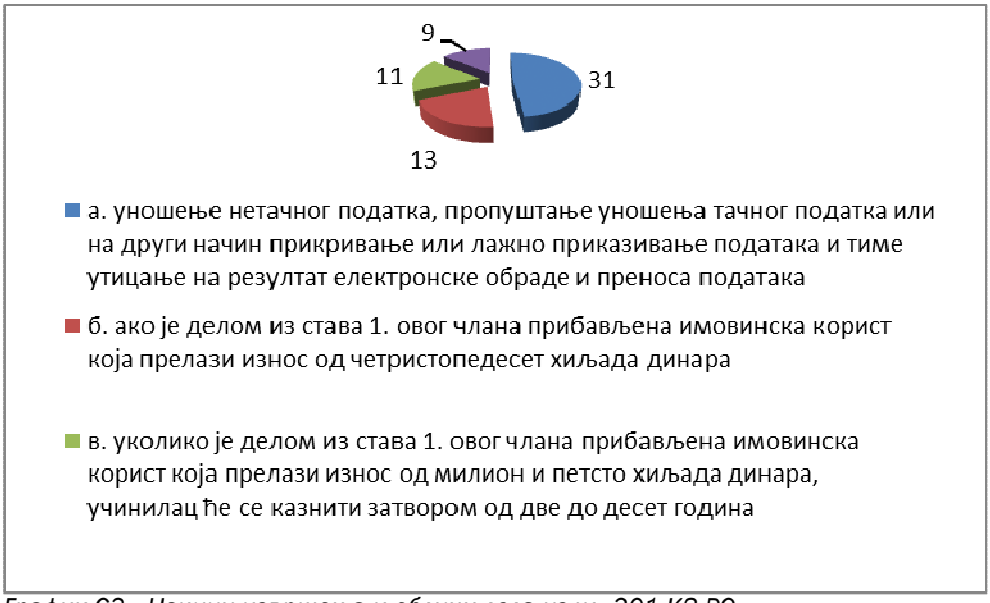


График 63. Начини извршења и облици дела из чл. 301 КЗ РС

У погледу анализе овог дела као најчешће заступљен облик у пракси јавља се основни облик у 31 одговору (64.58%), следећи по учесталости је први тежи облик (13 одговора или 27.08%), затим други тежи облик са 11 одговора (22.92%) и на крају ту је и посебан облик у намери наношења штете другоме у 9 одговора (18.75%). Дисперзија одговора испитаника нам даје релативан увид у расподелу реалних облика извршења овог дела, па је, очекивано, основни облик најзаступљенији, а следе га први и други тежи облик, док је најмање заступљен посебан облик.

Колико је у практичном раду заступљено ово дело у свом облику који се састоји у вршењу основног облика у намери наношења штете другоме?

Табела 70. Питање бр. 41

одговори	n	%
увек	3	6.25
често	17	35.42
понекад	11	22.92
ретко	4	8.33
није унето	13	27.08

График 64. Учесталост дела из ч.301 КЗ РС

Када обратимо пажњу на фреквентност основног појавног облика у намери наношења штете можемо утврдити да се у 28 одговора (58.34%) овај облик јавља често или понекад у пракси. Претходно помињани најнезаступљенији облик је у овом одговору добио на фреквентности, па је могуће говорити о својеврсном контролисању претходног одговора испитаника. Видимо да је проценат порастао са непуних деветнаест на скоро шездесет процената, али је веома значајан моменат да су у питању два облика блаже учесталости (често и понекад), па је могуће образлагати овакву дистрибуцију одговора као додатне тзв. неопредељене испитанике у претходном питању. У сваком случају оваква дистрибуција је вероватнија реалности. У том смислу веома је значајно разумети да се извршењем кривичног дела из чл.301. КЗ у намери наношења штете другоме ипак на неки начин може стати у крај прописивањем оштријих казни за овај облик дела или укупном казненом политиком у погледу овог дела у односу на његове извршиоце или учиниоце.

Наведите начине извршења кривичног дела неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података члан 302 и његове облике на које сте наилазили:

Табела 71. Питање бр. 42

одговори	n	%
а. кршењем мера заштите неовлашћеним укључивањем у рачунар или рачунарску мрежу	27	56.25
б. неовлашћено приступање електронској обради података	28	58.33
в. снимање или употреба података добијених на начин предвиђен у ставу 1	12	25.0
г. ако је услед дела из става 1 овог члана дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице	21	43.75
д. не знам		

График 65. Дисперзија појавних облика дела из чл.302 КЗ РС

Видимо да је најчешћи облик други основни облик овог дела према 28 одговора (58.33%), затим први основни облик према 27 одговора (56.25%), па други тежи облик (21 одговор или 43.75%), а на послетку први квалификовани облик овог дела (12 одговора или 25%). У фреквентности појавних облика овог кривичног дела веома је интересантно увидети да је неовлашћено приступање електронској обради података најчешћи облик овог дела. Наиме приликом извршења овог кривичног дела у скоро 60% јавља се овај облик, који подразумева и одређену стручност извршилаца, нарочито са аспекта потребног нивоа струке учиниоца у циљу савлађивања препрека које се при вршењу овог дела морају савладати. Са друге стране, ово је случај и са другорангираним обликом по фреквентности (кршењем мера заштите, неовлашћеним укључивањем у рачунар или рачунарску мрежу), тако да дефинитивно имамо закључак који индицира пораст оваквих облика

кривичног дела и способности и знања извршилаца. У случају трећег по фреквентности кривичног дела реч је о тежем облику кривичног дела. А најмање фреквентан случај је у посебно перфидном облику који представља квалификови облик претходна два основна (снимање или употреба података добијених на начин предвиђен у ставу 1). Што се тиче смерница у погледу овог кривичног дела, треба обратити пажњу на развој околности и ситуација (техничких знања, способности, средстава и уређаја у употреби) и могућности ширења последица и захвата у погледу жртава (пасивних субјеката), како физичких тако и правних лица. У том смеру се може предвидети све шира употреба интернета у свакодневном животу, која носи и веће могућности злоупотреба, о чему се мора водити рачуна приликом разматрања казнене политике и последица по извршиоце.

Наведите начине извршења кривичног дела спречавање и ограничавање приступа јавној рачунарској мрежи члан 303 и његове облике на које сте наилазили.

Табела 72. Питање бр. 43

одговори	n	%
а. неовлашћено спречавање или ометање приступа јавној рачунарској мрежи	23	47.92
б. ако дело из става 1 овог члана учини службено лице у вршењу службе	13	27.08
в. не знам	15	31.25

График 66. Дисперзија начина извршења дела из чл. 303 КЗ РС

Најчешћи појавни облик овог дела је први (23 одговора или 47.92%), а за њим следи одговор по којем испитаници не знају који је најчешћи облик (15 одговора или 31.25%), а потом и други појавни облик по учесталости (13 одговора

или 27.08%). У погледу овог дела и у односу на најфреквентнији први основни облик, веома је значајно да се схвати да оно представља актуелну појаву DDOS-напада, која је веома лоше санкционисана у нашем законодавству. О томе дефинитивно треба водити рачуна због потенцијала које овакви облици кривичног дела могу у будућности проузроковати, у смислу последица по заједницу (Треба се само сетити последица које је имао напад хакерских удружења у Естонији или дејства чувених Анонимуса у свету). Ово се може одредити као један од посебно значајних резултата нашег истраживања и у том смислу морало би се повести много више рачуна о будућим инкриминацијама и, генерално, о казненој политици.

Наведите начине извршења кривичног дела спречавање и ограничавање приступа јавној рачунарској мрежи безбедности рачунарских података члан 304а и његове облике на које сте наилазили.

Табела 73. Питање бр. 44

одговори	n	%
а. поседовањем	20	41.67
б. прављењем	18	37.5
в. набављањем	17	35.42
г. продајом	15	31.25
д. давањем другом на употребу рачунара, рачунарских система, рачунарских података и програма ради извршења кривичног дела из чл. 298 до 303 овог законика.	19	39.58

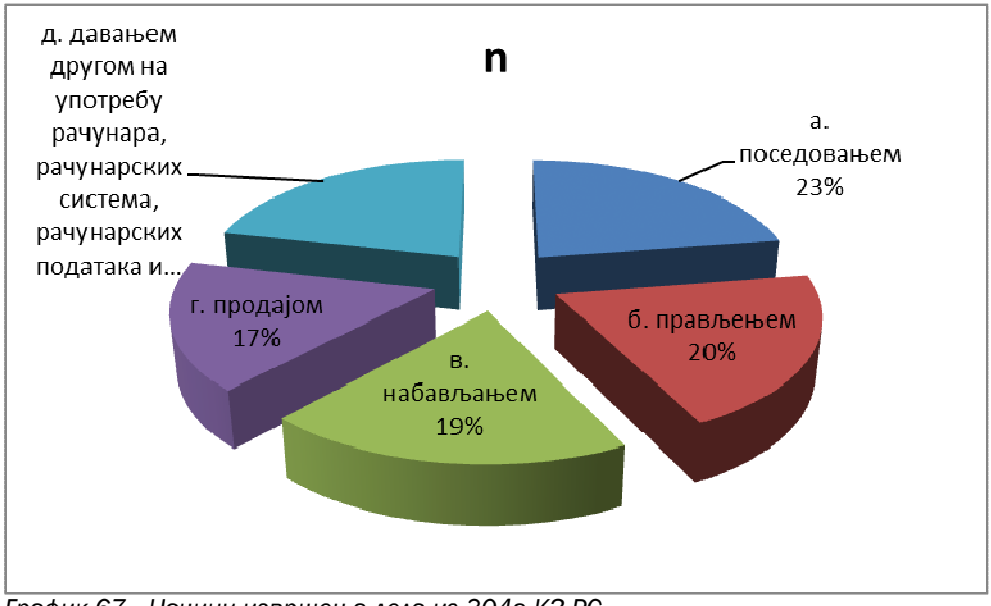


График 67. Начини извршења дела из 304а КЗ РС

Као резултат овог питања добили смо рангирање начина вршења овог дела према учесталости појавних облика у пракси, па тако најчешће имамо

поседовањем (20 одговора 41.67%), давањем другом на употребу рачунара, рачунарских система, рачунарских података и програма ради извршења кривичног дела из чл. 298 до 303 овог законика (19 одговора или 39.58%), прављењем (18 одговора или 37.5%), набављањем (17 одговора или 35.42%), на крају је ту и продајом (15 одговора или 31.25%). И у погледу резултата добијених одговорима на ово питање на прво место се може поставити питање казнене политике и резултата криминалистичких поступања припадника полиције и тужилаштва.

Анкета ПКС

ИСП провајдери

1. Узорак ове анкете у оквиру истраживања твининг-пројекта је чинило 5 испитаника представника интернет сервис провајдера. У одабиру узорка се водило рачуна да буде довољан број испитаника. Узорак су чинили представници привредних друштава која се баве пружањем услуга интернета. Узорак је према свим анализама свеобухватан по свим критеријумима. По многим критеријумима он јесте репрезентативан за популацију.

2. Анализа резултата

Спроведено истраживање о појавним облицима високотехнолошког криминала у Србији, обухватило је, поред анкете намењене општој популацији, и анкету коју су попуњавали представници ИСП-а. Испитивање је било анонимно и временски није било ограничено. Упитници су дисеминирани путем електронске поште, на исти начин су и враћани. Сакупљени подаци су обрађивани статистичком анализом у програмима SPSS и Microsoft Exel.

Да ли сте учествовали у посебним акцијама из области високотехнолошког криминала?

да, у акцији

не

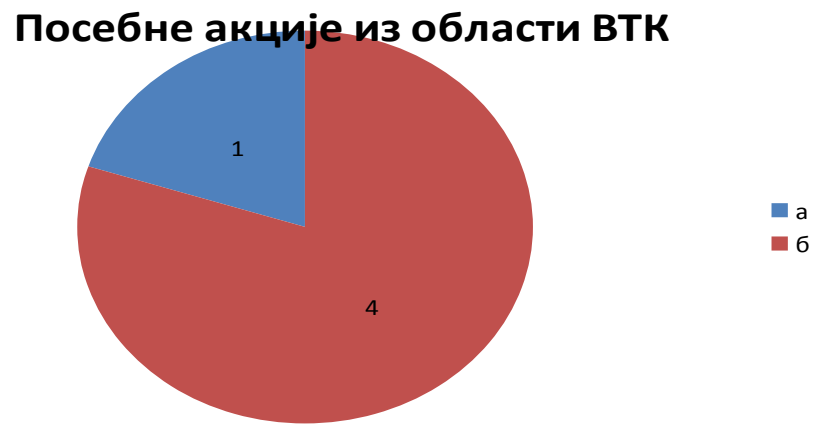


График 68. Учешће у посебним акцијама

У одговорима на ова питања, као што се може приметити, 80% испитаника (ИСП) је изнело да није учествовало ни у једној акцији у области ВТК. Само један од испитаника или 20% је учествовао у некој од акција из области ВТК, и конкретно је и навео да је у питању акција Савета Европе у оквиру пројекта против економског криминала у РС (Council of Europe's Project Against Economic Crime in the Republic of Serbia). Дакле, једна петина испитаних провајдера интернет услуга је учествовала у некој од посебних акција из области ВТК. Као једна од смерница и препорука у овој области могла би се извести потреба да се оваква активност прошири и омасови, с обзиром да је приватно јавно партнерство ИСП и државе у овој области неопходност.

Да ли сте корисницима Ваших услуга блокирали приступ интернет садржајима?

да, којим

не, никада

График 69. Блокирање приступа интеренет садржајима

Наравно, када је у питању демократско друштво и држава очекује да се у области интернет услуга не чине никакве репресалије, посебно када се разуме да је приступ интернету подигнут на ниво основних слобода и права човека према једном делу теорије. Но, с обзиром да је ова област у одређеним државама, које су познате по својим залагањима за примену и неограничавање слобода и права човека и грађанина, регулисана и на начин да се у одређеним случајевима и оваква права и слободе могу ограничити (већ поменути Хадопи закон и СОПА), није немогуће да се и код нас у некој блиској будућности уведе сет ограничења права и слобода у погледу приступа интернету. У нашој анкети сви представници ИСП-а су изнели да никада нису блокирали приступ ником од својих корисника услуга.

Да ли је било случајева пријаве сајтова због нуђења лажних послова у иностранству?

да,

не

График 70. Случајеви пријаве сајтова због нуђења лажних послова у иностранству

У вези са питањем да ли је било случајева пријаве сајтова због нуђења лажних послова у иностранству, очекивано је да се не појаве пријаве у овој области с обзиром да није било неких масовних случајева превара или организованог нуђења послова у иностранству. Међутим, постоје гласине о организованим облицима трговине људима који се рекламирају кроз нуђење различитих садржаја на интернету, које овим путем нису потврђене. Могуће је предвидети и неку накнадну анкету којом би оваква питања била постављена припадницима УКП-а, СБПОК-а или УГП-а у вези са њиховим сазнањима у овој области и поводом оваквих гласина како бисмо проверили ове резултате од стране ИСП-а. Са друге стране је и разумљиво да уколико није било правоснажних пресуда и осуђених извршилаца у оваквим случајевима, ни један ИСП не сме ни да „истрчава“ у категоризацијама у погледу оваквих случајева.

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирaн у овом питању.

Да ли је било случајева пријаве сајтова због посредовања при запошљавању у иностранству?

да,

не

График 71. Случајеви пријаве сајтова због посредовања при запошљавању у иностранству

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирам у овом питању.

Да ли је било случајева пријаве сајтова за услуге посредовања при усвајању деце?

да,

не

График 72. Случајеви пријаве сајтова за услуге посредовања при усвајању деце

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирам у овом питању.

Да ли је било случајева пријаве сајтова због организовања путовања за секс-туризам?

да,

не

График 73. Случајева пријаве сајтова због организовања путовања за секс – туризам

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирана у овом питању.

Да ли је било случајева пријаве сајтова због нуђења сексуалних услуга?

да,

не

График 74. Случајеви пријаве сајтова због нуђења сексуалних услуга

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирана у овом питању.

Да ли је било случајева пријаве сајтова због нуђења незаконитих медицинских услуга?

да,

не

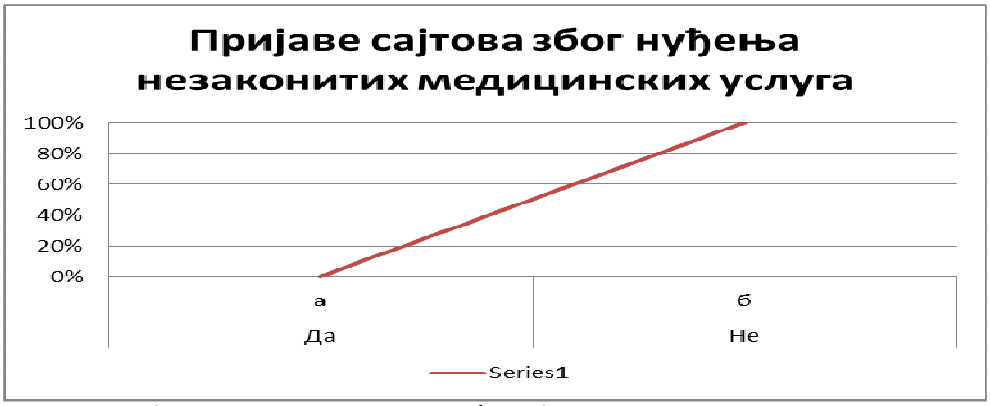


График 75. Случајеви пријаве сајтова због нуђења незаконитих медицинских услуга

У погледу одговора на ово питање као и у свим накнадним видимо константу ИСП–ова да нема посебних пријава веб-сајтова због нуђења незаконитих медицинских услуга. У овом смислу захтевало се од ИСП –ова да наведу како своје тако и пријаве других лица (правних или физичких) у погледу постојања неког основа сумње о садржајима описане врсте. Као што се види није било таквих случајева.

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирана у овом питању.

Да ли је било случајева пријаве сајтова због трговине органима на интернету?

да,

не

График 76. Случајеви пријаве сајтова због трговине људским органима

У погледу одговора на ово питање као и у свим накнадним видимо константу ИСП–ова да нема посебних пријава веб-сајтова због трговине органима на интернету. У овом смислу захтевало се од ИСП–ова да наведу како своје тако и пријаве других лица (правних или физичких) у погледу постојања неког основа сумње о садржајима описане врсте. Као што се види није било таквих случајева.

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирана у овом питању.

Да ли је било случајева пријаве сајтова због трговине органима на интернету?

да,

не

График 77. Случајеви пријаве сајтова организованих криминалних група

У погледу одговора на ово питање као и у свим накнадним видимо константу ИСП–ова да нема посебних пријава веб-сајтова због трговине органима на интернету. У овом смислу захтевало се од ИСП–ова да наведу како своје тако и пријаве других лица (правних или физичких) у погледу постојања неког основа сумње о садржајима описане врсте. Као што се види није било таквих случајева.

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирана у овом питању.

Да ли је било случајева пријаве сајтова организованих криминалних група?
да,
не

График 78. Случајеви пријаве сајтова организованих криминалних група

У погледу одговора на ово питање као и у свим накнадним видимо константу ИСП–ова да нема посебних пријава веб-сајтова због трговине органима на интернету. У овом смислу захтевало се од ИСП–ова да наведу како своје тако и пријаве других лица (правних или физичких) у погледу постојања неког основа сумње о садржајима описане врсте. Као што се види није било таквих случајева.

Ако је било таквих случајева, шта је предузето?

Резултати у одговорима на ово питање су разумљиви, с обзиром да се у претходном није јавио ни један кореспондирајући одговор који би био елаборирaн у овом питању.

3.3 Друштво картичара

3.3.1 Узорак

Узорак ове анкете, у оквиру истраживања твининг-пројекта је чинило 11 испитаника представника Удружења картичара, односно банака. У одабиру узорка се водило рачуна да буде довољан број испитаника. Узорак су чинили представници привредних друштава који се баве пружањем финансијских и банкарских услуга. Узорак је према свим анализама свеобухватан по свим критеријумима. По многим критеријумима он јесте репрезентативан за популацију.

3.3.2 Анализа резултата

Спроведено истраживање о појавним облицима високотехнолошког криминала у Србији, обухватило је, поред анкете намењене општој популацији, и анкету коју су попуњавали представници Удружења картичара, односно банака. Испитивање је било анонимно и временски није било ограничено. Упитници су дисеминирани путем електронске поште, на исти начин су и враћани. Сакупљени подаци су обрађивани статистичком анализом у програмима SPSS и Microsoft Exel.

1. Да ли су Ваши корисници пријављивали злоупотребу платних картица?
   а. да,
   б. не

Табела 74. Питање бр. 1

Да	Не
8	3
72.72727	27.27273

График 79. Пријаве злоупотреба платних картица

2. Ако јесте, каквих?
   а. крађа картица
   б. крађа идентитета у случају остављања података трећим лицима (путем
   телефона или интернета)
   в. фишингом
   г. преузимањем података преко лажних сајтова за online куповину
   д. преузимањем података на сајтовима банака
   ђ. фалсификовањем картица
   е. преко лажних читача на банкоматима и наплатним местима
   ж. друго.

График 80. Облици злоупотребе платних картица

Табела 75. Питање бр.2

Ако јесте, каквих?			
а.	8	72.73	крађа картица
б.	5	45.45	крађа идентитета у случају остављања података трећим лицима (путем телефона или интернета)
в.	3	27.27	фишингом
г.	3	27.27	преузимањем података преко лажних сајтова за он-лајн куповину
д.	1	9.09	преузимањем података на сајтовима банака
ђ.	6	54.55	фалсификовањем картица
е.	7	63.64	преко лажних читача на банкоматима и наплатним местима
ж.	2	18.18	друго

Анализа овог питања доноси нам врло корисне резултате. Можемо видети да се као најзаступљенији облици злоупотреба платних картица јављају следећи начини следећим редоследом: крађа картица у 72.73% случајева, затим преко лажних читача на банкоматима и наплатним местима 63.64%, а потом фалсификовањем картица 54.55%, па крађа идентитета у случају остављања података трећим лицима (путем телефона или интернета) у 45.45% случајева и подједнако 27.27% фишингом и преузимањем података преко лажних сајтова за он-лајн куповину, а најмање пријављених било је преузимањем података на сајтовима банака 9.09%. Оваква дистрибуција је била веома интересантна, посебно у последњем случају, с обзиром да је тешко очекивати да банке признају сопствене пропусте и грешке, а што се ипак у проценту од 9.09% десило у нашој анкети. Као најчешће одређивани облик се јавља крађа картица што је очекивано, односно скиминг као најчешћи следећи, такође очекивани облик и исто фалсификовање картица (беле и златне). Новина у порасту на нашим просторима је крађа идентитета у случају остављања података трећим лицима (путем телефона или интернета) односно фишингом и преузимањем података преко лажних сајтова за он-лајн куповину. Ови облици су облици који су се недавно појавили у свету, а код нас све више узимају маха, па је неопходно предузимати мере којима се овом облику супротстављају у свету. Један од додатно понуђених начина, а који чини 9.09% укупног броја одговора је крађа личне карте и отварање рачуна/добијање картице, на основу украдене личне карте, и још један који подразумева да чланови породице повремено користе картицу без знања њеног власника.

3. Да ли је било пријављених случајева упада у систем банака?
а. да,
б. не

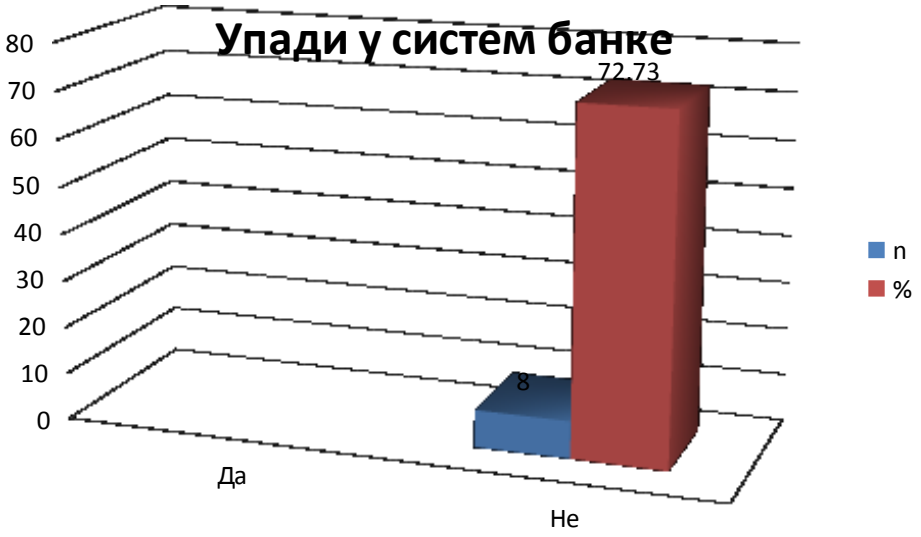


График 81. Упади у информациони систем банака

Анализа трећег питања на које су одговарали банкари (Удружења картичара) донела нам је наравно очекивани резултат по којем је 100% наших испитаника указало да није било упада у системе банака. Очекиваност оваквог одговора је логична, с обзиром да, како интерни прописи банака тако и потреба заштите пословне тајне и приватности пословне политике, захтевају од банака да не откривају овакве информације у било ком смислу јавности док на то нису принуђени. Дакле и да их је било, они их не би признали осим уколико са таквим нечим није упозната шира јавност, па су принуђени да то признају. Разумљиво и са аспекта заштите од нелојалне конкуренције и из комерцијалних разлога.

4. Да ли примењујете страндардизоване процедуре информационе безбедности?

а. да, које
б. не
ц. не знам

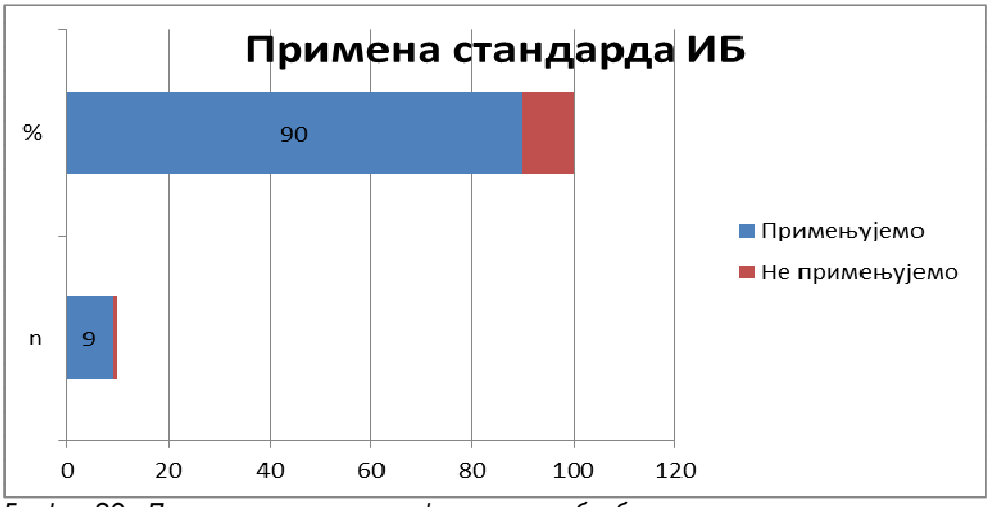


График 82. Примена процедура информационе безбедности

Табела 76. Питање бр. 4

4	Да ли примењујете страндардизоване процедуре информационе безбедности?						
a.	7	63.64	да, које	а. Групни УЦБ стандарди који подлежу ИСО стандардима	Физичке, логичке, управљачке	сви фајлови везани за платне картице се шаљу криптовано преко СФТП конекције; бројеви картица се маскирају у маил коресподенцији;...	ИСО 27001:2005
b.	1	9.09	не				
c.			не знам				

Анализом овог питања и датих одговора можемо утврдити да је постојећа тенденција у 63,64% наших испитаника увођење ИСО стандарда у области информационе безбедности, конкретно 27001:2005, односно Групни УЦБ стандарди који подлежу ИСО стандардима, тј. физичке, логичке, управљачке. Неки од испитаника су наводили и конкретне облике заштите који се на тај начин спроводе, па тако имамо одговор по којем се: сви фајлови везани за платне картице шаљу криптовано преко sftp конекције; бројеви картица се маскирају у маил коресподенцији. Само један испитаник, односно 9.09% је изнео да његова институција не примењује стандардизоване процедуре информационе безбедности. Овакав однос резултата је веома задовољавајући са аспеката како корисника тако и перцепције безбедности на нашем тржишту капитала. У сваком случају сматрамо да је држава та која би морала увести обавезе успостављања стандардизованих процедура информационе безбедности посебно у области платних картица, с обзиром на велике могућности њиховог злоупотребљавања.

Смернице

У погледу смерница у овом одељку свако од питања има на крају и предложене смернице у области која је интересантна за конкретно питање.

ЛИТЕРАТУРА

1. Alvey, R: „Russian hackers for hire: the rise of e-mercenary“, SAD: Janes Intelligence Review, 2001.
2. Athanasopoulos E. et. al: „Antisocial Networks: Turning a Social Network into a Botnet“, Section: Network Security, Lecture Notes In Computer Science, Берлин, Република Немачка, стр. 146–160.
3. Angelopoulou, O. Thomas, P. Xynos, K. and Tryfonas, T. „Online ID theft techniques, investigation and responses“, Int. J. Electronic Security and Digital Forensics,, Велика Британија, 2007.
4. ASIS International Report “Cloud Computing and Software as a Service: An Overview for Security Professionals“, USA, 2010, стр. 43.
5. Abrams M. Podell H. „Information Security: An Integrated Collection of Essays“, Computer Society Press, Los Alamitos, CA USA, 1995,
6. Божидар Бановић, Владимир Урошевић, Звонимир Ивановић „Phishing schemes – typology and analysis in Serbian cyber space“, Policing in Central and Eastern Europe, Social Control of Unconventional Deviance, Conference Proceedings, Faculty of Criminal Justice and Security, University of Maribor, Slovenia, стр. 125–138.
7. Будимлић М. Пухарић П. „Компијутерски криминалитет – криминолошки кривичноправни, криминалистички и сигурносни аспекти“, Факултет за криминалси- тику, криминологију и сигурносне студије, Сарајево, 2009, стр. 10–11.
8. Bidgoli, H. „Handbook of Information Security“, Volume 2, John Wiley & Sons, Inc. Hoboken, NJ 2006.
9. Boroujerdi M. Nazem. S. „Cloud Computing: Changing Cogitation about Computing“, World Academy of Science, Engineering and Technology 58, USA, 2009, стр. 1112– 1116.
10. Војковић, Г. Штамбук-Суњић, М. „Конвенција о кибернетичком криминалу и казнени закон Републике Хрватске“ Зборник радова Правног факултета у Сплиту, broj 1 (81), 2006, стр. 123–136.
11. Вулетић Д. „Кибер ратовање као облик информационог ратовања“, у зборнику радова „ ZITEH2004“, ИТ Вештак, Београд, 2004.
12. Gibson W. “Neuromancer“, Ace, прво издање, САД, 1984. године
13. Gandhi M. et al: „Stealthy click-fraud with unwitting accessories“. Journal of Digital Forensic Practice No. 2, Taylor & Francis, Велика Британија, 2006, 131–142.
14. Герке, М. и др. “Приручник за истрагу кривичних дела у области ВТК“, Савет Европе, 2008.
15. Deutsch, K. W. „The Nerves of Government: Models of Political Communication and Control“, друго издање, 1966, стр. 76.
16. Bidgoli, H. Handbook of Information Security, Volume 2, John Wiley & Sons, Inc. Hoboken, NJ 2006. p.211.
17. Uljanov, S. Urošević, V. Ivanović, Z. Visokotehnološki kriminal iz ugla međunarodne saradnje kriminalističke policije, str.530-541. Zbornik radova Konferencije Internacionalne asocijacije kriminalista, Međunarodna i nacionalna saradnja i koordinacija u suprostavljanju kriminalitetu, na Kelebiji, Banjaluka 2010. Vol. 3. Br.1.
18. Đukanović, D. Ivanović, Z. Uljanov, S. Oblici međunarodne policijske saradnje u uslovima tranzicije na zapadnom Balkanu, Serbian law in transition: changes and challenges, Belgrade Institute of comparative law,
19. Urošević, V. Ivanović, Z. Uljanov, S. Mač u www – u: Izazovi VTK, Beograd: Eternal mix, 2012
20. Жарковић, М. Ивановић, З. Криминалистичка тактика, КПА, Београд, 2014.
21. Ивановић, З. Жарковић, М. научни приступ у изградњи тимова за одузимање дигиталних доказа, стр 399-413 у Тематском зборнику међународног значаја, вол ја, Академија криминалистике и полицијских студија, 2013, ур. Горан Милошевић.

22. Ивановић, З. Жарковић, М. Лајић, О. Криминалистичка разматрања дигиталних доказа, Криминалистичко–форензичка обрада места кривичних догађаја, стр.121-141, Тематски зборник радова, Криминалистичко–полицијска академија, 2013.
23. Ivanović, Z. Žarković, M. Scientific approach in building teams for seizure of digital evidence, pp. 399-413 in Thematic proceedings of international significance, Vol I, Academy of criminalistics and police studies, 2013, Ed. Goran Milošević
24. Ivanović, Z. Vukanić, V. Analiza prava na privatnost u Srbiji kroz primenu normi o nadzoru komunikacija 309-335 u Spoljna politika Srbije i zajednička spoljna i bezbednosna politika EU (Ur. Dragan Đukanović i Miloš Jončić), Beograd 2012.
25. Ivanović, Z. Urošević, V. Uljanov, S. Revija za kriminalistiko in kriminologijo, Ljubljana 64/2013/3, s. 275-286, Interview and Interrogation Tactics and Techniques in Serbia,
26. Ivanovic, Z. Uljanov, S. Chapter 33, pp. 319-327, Serbia Community policing in indigenous communities, eds. Mahesh Nalla, Graeme R. Newman, 2013, CRC Press, Boca Raton, Florida, Taylor and Francis Group, ISBN 978-1-4398-8894-0, HV7936.C83C692 2013, UDK 363.2`3//dc23
27. Ивановић, З. Кесић, Т. Правни статус електронског надзора над обавештајцима у САД, Супротстављање савременом организованом криминалу и тероризму, ИВ ЕДИЦИЈА ΑΣΦΑΛΕΙΑ, Књига В Криминалистичко-полицијска академија, Београд, 2013.
28. Ivanovic, Z. Serbia in the Danube region in the 21st Century, Eds. Jeftić – Šarčević, N. Petrović, D. Proceedings from the International Conference Serbia in the Danube Region in the 21st Century, Kladovo, 16-17 September 2013, Belgrade 24 September, Ivanovic Z. Legislative analysis of some Danube countries in the field of cybercrime, pp.193-208. IIPE Novi Sad – Mala knjiga 2014.
29. Ивановић, З. Практични аспекти примене обавезне инструкције МУП-а о поступању са дигиталним доказима, Зборник радова БИСЕЦ 2014, Конференција о безбедности информација, 18. Јун 2014, Ур. Нецад Мехић,
30. Ивановић, З. Обезбеђење дигиталних трагова, Zloupotreba informacionih tehnologija i zaštita – zbornik, str. 62-75. Izdavač Udruženje sudskih veštaka za informacione tehnologije it veštak Beograd, Danijelova 32, ur. Slobodan R, Petrović
31. Лајић, О. Лукић, Т. Ивановић, З. Специфичности финансијске истраге у Србији, Тематски Зборник радова међународног значаја, Криминалистичко-полицијска академија , Београд 2011. Међународна научна конференција "Арчибалд Рајс дана" пп 369 - 381 .
32. Lajić, O. Kesić, T. Ivanović, Z. Pregled međunarodnih i regionalnih evropskih dokumenata od značaja za istraživanje i oduzimanje imovine stečene kriminalom, str.33-45. Suprotstavljanje savremenom organizovanom kriminalu i terorizmu (Urednik Saša Mijalković) Kriminalističko – policijska akademija, Beograd 2013.
33. Милошевић, М. Ивановић, З. Едукација припадника криминалистичке полиције у сузбијању високотехнолошког криминала у Републици Србији и иностранa искуства са освртом на стратешка опредељења Републике Србије на сузбијању вискотехнолошког криминала, Тематски зборник Полиција, безбедност и високотехнолошки криминал, (ур. Жељко Никач), стр. 81-110. КПА, Београд 2010.
34. Међународна унија за телекомуникације “World Telecommunication Development Report 2003 – Access Indicators for the Information Society“, 2003, страна 8.
35. Morse C. Wang H.: „The Structure of an Instant Messenger Network and its Vulnerability to Malicious Codes“, Department of Computer Science The College of William & Mary, Williamsburg, САД, 2005. стр. 1.
36. Marshall D. A. Podell H. J. „Information Security: An Integrated Collection of Essays“, Computer Society Press, Los Alamitos, CA USA, 1995, стр. 117.
37. Mukkamala S. „Role of Computational Intelligence in Malware Detection and Malicious Code Analysis“, Institute for Complex Additive Systems Analysis, Computational Analysis and Network Enterprise Solutions, New Mexico, 2009. стр. 1.
38. NGSSoftware LTD: „The Phishing Guide Understanding & Preventing Phishing Attacks“, United Kingdom Sutton, 2006.

39. Одбор за банкарство и осигурање-Форум за превенцију злоупотреба платних картица „Платне картице, едукациони материјал за представнике полиције и правосуђа“, Привредна комора Србије, Београд 2007. стр. 40–41.
40. Петровић, С. „Рачунарски криминал“, Министарство унутрашњих послова Републике Србије, Београд, 2000, стр. 42.
41. PACO Serbia-Пројекат за борбу против економског криминала у Републици Србији „Приручник за истрагу кривичних дела у области високотехнолошког криминала“, Савет Европе, 2008. стр. 38.
42. Плескоњић Д. Ђорђевић Б. Мачек Н. Царић М. „Сигурност рачунарских мрежа“, Виша електротехничка школа, Београд, 2006.
43. Uljanov, S. Urošević, V. Ivanović, Z. Visokotehnološki kriminal iz ugla međunarodne saradnje kriminalističke policije, str. 530-541. Zbornik radova Konferencije Internacionalne asocijacije kriminalista, Međunarodna i nacionalna saradnja i koordinacija u suprostavljanju kriminalitetu, na Kelebiji, Banjaluka 2010. Vol. 3. Br.1.
44. Урошевић, V. Ivanović, Z. Уljanov, S. Mač u www–u: Izazovi VTK, Beograd: Eternal mix, 2012.
45. Reljanović, M. Ivanović, Z. Evropska kancelarija za borbu protiv finansijskih prestupa (OLAF), str.111-125, Borba protiv korupcije – iskustva i poređenja, Institut za uporedno pravo, Beograd, 2013. (ur. Jovan Ćirić)

Весна Лукић
Институт друштвених наука – Центар за демографска истраживања

КОРИШЋЕЊЕ ВИСОКИХ ТЕХНОЛОГИЈА И ИРЕГУЛАРНЕ МИГРАЦИЈЕ

Садржај

Табеле

Графици

1. УВОД

Савремене миграције одликује пораст обима и разноврсности миграционих токова. Према процени УН у свету је 2013. било 232 милиона међународних миграната, у поређењу са 154 милиона 1990. године[734]. За велики број ових миграната дестинација су земље чланице Европске уније. Стога се миграцијама, миграционим политикама и јачању капацитета за управљање миграцијама посвећује све већа пажња националних, али и европских институција. Глобални приступ миграцијама и мобилности - GAMM[735], иновиран 2011. године, оквир је спољне миграционе политике ЕУ и основ за сарадњу између земаља Европске уније и других земаља. Заснива се на заједничким интересима и изазовима. Као главни приоритети истичу се: унапређење организације легалних миграција и олакшавање мобилности, превенција и смањивање обима ирегуларних миграција на ефикасан и хуман начин, јачање синергије између миграција и развоја и јачање система међународне заштите и спољашње димензије азила.

У новије време миграције бележе повећану феминизацију и пораст обима ирегуларних, привремених и циркуларних миграционих токова. Међународна организација рада процењује да ирегуларни мигранти чине од 10% до 15% од укупног броја миграната у свету[736]. Кад је реч о Европској унији, најновије процене указују да се, 2008. године[737] број ирегуларних становника у 27 држава чланица ЕУ кретао између 1,9 и 3,8 милиона. У овој популацији најбројнија су лица која су границу прешла легално, али су остала у земљи дестинације након истека визе. Они најчешће раде у сивој економији, заједно са мигрантима који су прешли границу са фалсификованим документима или ван званичних граничних прелаза и лицима којима је одбијен захтев за азилом[738]. Рад у сивој зони ствара ризик од радне експлоатације за ирегуларне мигранте. „Уз ризик радне експлоатације, илегалне мигранте, а посебно девојке, прати ризик и од сексуалне експлоатације"[739]. На спољним границама ЕУ забележено је током 2013. године чак 72.437 илегалних прелазака, од чега 605 уз помоћ крijумчара и то најчешће скривањем у возилима[740]. Сазнања добијена на основу научних истраживања указују да постоји генерални тренд пораста коришћења услуга крijумчара. Границе се у повећаном

734 Trends in International Migrant Stock: The 2013 Revision, Press release, UN http://esa.un.org/unmigration/wallchart2013.htm (приступљено 11.09.2013);

735 Global Approach to Migration and Mobility, European Commission, Home affairs http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/international-affairs/global-approach-to-migration/index_en.htm (приступљено 11.11.2013);

736 International Labour Organisation (2004), Towards a fair deal for migrant workers in the global economy, Report VI, International Labour Conference, 92nd Session, International Labour Office, Geneva. http://www.ilo.org/public/portugue/region/eurpro/lisbon/pdf/rep-vi.pdf (приступљено 16.12.2013);

737 Vogel D. V. Kovacheva, H. Prescott (2011), The Size of the Irregular Migrant Population in the European Union – Counting the Uncountable?, International Migration, 49 (5), 10.

738 Clandestino Project, Final report, (2009),13; http://www.emnbelgium.be/publication/clandestino-project-final-report (приступљено 6.10.2013).

739 Мијаилковић С. и М. Жарковић, (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр.31;

740 Frontex, Annual Risk Analysis, (2013), 12. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013);

обиму прелазе на званичним прелазима, у аутомобилима и камионима или са лажним документима.[741]

Ирегуларне миграције имају транснационални карактер. С обзиром да свака држава надзире улазак и излазак становништва са своје територије, основна веза између ирегуларних миграција и криминала следи из чињенице да је илегалан улазак и боравак на територији неке државе кривично дело. Премда је проучавање популације ирегуларних мигранта значајно са аспекта заштите њихових основних права и обезбеђивања помоћи, потреба за проучавањем и контролом ирегуларних миграција претежно је условљена тиме што оне представљају фактор дестабилизације и претњу националној сигурности. То је последица њихове честе повезаности са терористичким нападима и интернационалним организованим криминалом (кријумчарење дроге, трговина људима, фалсификована документа и друго). Примера ради, у Норвешкој је доказана веза између појединих тражилаца азила и трговине дрогом[742]. Зато се "миграције на Западу све више посматрају кроз призму сигурности"[743]. Европол процењује да се половина нелегалних улазака на простор ЕУ оствари уз помоћ организованих криминалних група, што резултира њиховом зарадом од 12 билиона евра годишње[744]. Осим кријумчара и друга лица и предузећа могу да помажу ирегуларним мигрантима током илегалног преласка границе, било да су то туристичке агенције, као што је забележено у Бугарској или локални возачи и водичи, што је случај Срба и Мађара на Балканској рути ирегуларних миграција[745].

Битан фактор утицаја на пораст обима међународних миграција је глобализација[746]. Комуникациона и саобраћајна револуција делују на смањивање удаљености и олакшавање глобалних веза, које доприносе развоју свести становништва о неједнакостима, али и могућностима које им се пружају на неком другом месту[747]. Очекује се да ће употреба интернета, друштвених мрежа и

741 Futo P., M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2); Jandl M. (2007), Irregular Migration, Human Smuggling, and the Eastern Enlargement of the European Union, International Migration Review, 41 (2);

742 Practical Measures to Reduce Irregular Migration, *European Migration Network, (2012), 45.* http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-stutdies/irregular-migration/00a_emn_synthesis_report_irregular_migration_october_2012_en.pdf. (приступљено 14.12.2013);

743 Munck R. (2008), Globalisation, Governance and Migration: an introduction, Third World Quarterly, 29 (7),1232;

744 Bruggeman W. (2002), *Illegal Immigration and Trafficking in Human Beings Seen as a Security Problem for Europe.* http://www.belgium.iom.int/StopConference/Conference%20Papers/20%20Bruggeman%20Brussels%20IOM.19.09.02.pdf. (приступљено 5.11.2013);

745 Kaizen J., W. Nonneman (2007), Irregular Migration in Belgium and Organized Crime: An Overview, *International Migration,* 45 (2), 123; Frontex, Annual Risk Analysis, (2013), 36; http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013).

746 Лукић В. и Д. Матијевић, (2003), Миграције и глобализација, Регионални развој и демографски токови балканских земаља, Књ. 8, Економски факултет Универзитет у Нишу, Ниш, стр. 224;

747 Koser K. (2008), Dimensions and Dynamics of Contemporary International Migration Paper prepared for the conference on 'Workers without borders: Rethinking economic migration', Maastricht Graduate School of Governance, 18 March 2008;

мобилних телефона допринети јефтинијем илегалном преласку границе[748]. Према извештајима Европола, лица која помажу иregуларним мигрантима и кријумчари, као и у случају других организованих криминалних радњи, у великој мери користе интернет како због контаката тако и због упознавања са правним и законским процедурама држава транзита и дестинације[749]. Бројни аутори, такође, истичу употребу високих технологија од стране кријумчара (мобилни телефони, компјутерска технологија, интернет и друго) за рекламирање угодног живота у земљама које се препоручују за дестинације, комуникацију са иregуларним мигрантима, прелазак границе као и за израду фалсификованих докумената[750]. Осим што поседују савремену технологију кријумчари су се показали као веома флексибилни, мењајући руте и прилагођавајући се променама мера граничне полиције[751]. Употреба високих технологија је у порасту , осим од стране кријумчара и од стране надлежних граничних служби, а за потребе контроле границе и спречавања илегалних прелазака и кријумчарења људи. Примера ради, влада Холандије најавила је нове мере против иregуларних мигранта у земљи, које ће обухватити проверу података на мобилним телефонима и компјутерима без судског налога[752].

И поред свега наведеног, проучавање везе између миграционог процеса и употребе високих технологија релативно је нова област истраживања у оквиру миграција, те недостају истраживања на ову тему. Група аутора која је спровела истраживање о тренутном стању у Европи на тему високих технологија и миграција, наводи да постоји свега неколико студија које су се бавиле питањима сигурности и употребом високих технологија за незаконите активности[753]. Проучавање употребе високих технологија од стране иregуларних мигранта и азиланта представља аспект који није до сада истраживан у домаћој литератури. Нема довољно сазнања

---

http://www.brookings.edu/~/media/research/files/papers/2008/3/14%20migration%20koser/0314_migration_koser (приступљено 18.12.2013);

748 Frontex, Annual Risk Analysis, 2013, 62.

http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013);

749 Bruggeman W. (2002), *Illegal Immigration and Trafficking in Human Beings Seen as a Security Problem for Europe,4.*

http://www.belgium.iom.int/StopConference/Conference%20Papers/20%20Bruggeman%20Brussels%20IOM.19.09.02.pdf. (приступљено 5.11.2013);

750 Futo P., M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2); Kaizen J., W. Nonneman (2007), Irregular Migration in Belgium and Organized Crime: An Overview, *International Migration,* 45 (2); Bilger V., M. Hofmann, M. Jandl (2006), Human Smuggling as a Transnational Service Industry: Evidence from Austria, International Migration*,* 44 (4);

751 Mavris L. (2002), Human smugglers and social networks: transit migration through the states of former Yugoslavia Working Paper, New issues in refugee research,no. 72. UNHCR, 8. http://www.unhcr.org/3e19aa494.pdf (приступљено 23.11.2013); Futo P., M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2);

752 Picum's Main Concerns about the Fundamental Rights of Undocumented Migrants in Europe, 2010, 13.

http://picum.org/en/publications/reports/25189 (приступљено 13.10.2013);

753 Borkert M., P. Cingolani, V. Premazzi (2009), Study on 'The State of the Art of Research in the EU on the Uptake and Use of ICT by Immigrants and Ethnic Minorities (IEM)' IMISCOE Working Paper No. 27, 19, 20.

http://www.imiscoe.org/images/documents/wp27.pdf (приступљено 7.10.2013);

о вези између организованог криминала, ирегуларних миграција и употребе високих технологија, на основу чега би се продубила сазнања о њиховој интеракцији, као предуслову за креирање одговарајућих миграционих и других политика усмерених на доношење релевантних мера.

2. СРБИЈА И ИРЕГУЛАРНЕ МИГРАЦИЈЕ

У домену ирегуларних миграција Република Србија се последњих година суочава са злоупотребом система азила и безвизног режима са земљама ЕУ и повећаним бројем ирегуларних транзитних мигранта из трећих земаља, који покушавају да оду у неку од земаља чланица ЕУ. Споразумом о стабилизацији и придруживању између Европских заједница и њихових држава чланица и Републике Србије, Србија се обавезала на промовисање политике интеграције, поштовање начела забране протеривања и заштите свих права тражилаца азила и избеглица и спречавање и контролу ирегуларне миграције уз усвајање стандарда ЕУ по питању интегрисаног управљања границом.

Закони и миграционе политике генерално имају важну улогу у процесу ирегуларних миграција. У том смислу повећан обим ирегуларних миграционих токова поставља пред Србију нове друштвене и законске изазове. Република Србија је потписница Конвенције Уједињених нација против транснационалног организованог криминала, Протокола за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом и Протокола против кријумчарења мигранта копном, морем и ваздухом.[754] У циљу увођења високих стандарда контроле спољних граница, на које се обавезала потписивањем Споразума о стабилизацији и придруживању ЕУ, Влада Републике Србије је донела Стратегију за интегрисано управљање границом (2006). Ова Стратегија се заснива на европском концепту интегрисаног управљања границом са општим циљем успостављања и дугорочног одржавања границе, отворене за кретање људи и трговину, али безбедне и затворене за све видове прекограничних активности које угрожавају безбедност и стабилност у региону, међу којима су илегалне миграције и трговина људима[755]. Допринос у овој области остварен је и усвајањем новог Закона о заштити границе (2008)[756], усаглашеног са европским стандардима, те Уредбе о ближем уређивању начина обављања полицијских овлашћења полицијских службеника граничне полиције и дужностима лица које прелази државну границу (2011)[757]. Ова Уредба проширује овлашћења граничне полиције у домену питања и доказа о сврси путовања са циљем спречавања злоупотребе безвизног режима са Европском унијом. Главни циљеви Републике Србије у борби против ирегуларних миграција и трговине људима дефинисани су у Стратегији супростављања илегалним

754 Закон о потврђивању Конвенције Уједињених нација против транснационалног организованог криминала и допунских протокола, Службени лист СРЈ — Међународни уговори, бр. 6/01;

755 Стратегија интегрисаног управљања границом у Републици Србији, Службени гласник Републике Србије, бр. 11/06;

756 Закон о заштити државне границе, Службени гласник Републике Србије, бр. 97/08;

757 Уредба о ближем уређивању начина вршења полицијских овлашћења полицијских службеника граничне полиције и дужностима лица које прелази државну границу, Службени гласник Републике Србије, бр. 39/2011;

миграцијама у Републици Србији за период 2009–2014. године (2009),[758] и у Стратегији борбе против трговине људима у Републици Србији (2006)[759] и тичу се унапређења институционалног оквира, побољшања ефективности и ефикасности у супротстављању ирегуларним миграцијама и трговини људима, превенције и помоћи, те заштите и реинтеграције жртава.

Право на азил загарантовано је Уставом Србије. Законом о азилу (2007)[760] дефинисани су услови и поступак добијања и престанка права на боравак и заштиту, као и права и обавезе лица која траже азил и оних којима је признато право на азил у Републици Србији. Промовишу се начела забране протеривања и враћања, недискриминације, јединства породице, родне равноправности, бриге о лицима са посебним потребама и друга. Након успостављања безвизног режима између Србије и земаља шенгенске зоне, крајем 2009. године, билатерални међудржавни споразуми о реадмисији потписани су са Данском, Норвешком, Канадом, Хрватском, Босном и Херцеговином, Македонијом, Албанијом и Молдавијом. Споразумом о реадмисији[761] уређује се враћање и прихватање држављана Србије, који не испуњавају или су престали да испуњавају важеће услове за улазак, боравак или настањење на територији државе чланице ЕУ. Наиме, увођење безвизног режима за путовања између Републике Србије и земаља чланица ЕУ, условило је пораст броја неоснованих захтева за азил на територији ЕУ. По броју уложених захтева за азил у ЕУ држављани Републике Србије 2011. године били су на петом месту[762]. Повратак ирегуларних миграната наведен је као једна од приоритетних активности стратешког одговора ЕУ на миграционе притиске[763]. Током 2012. године забележено је повећање броја враћених држављана у земље које нису чланице ЕУ, па држављани Србије бележе пораст од чак 51% више враћених у односу на претходну годину[764]. Република Србија је 2012. године, на основу Споразума о реадмисији, одобрила 6.581 захтева за реадмисију. Највећи број српских држављана враћен је из Немачке, Шведске и Швајцарске и већином се ради о лицима ромске националности (61,8% 2012 г.)[765].

---

758 Стратегија супростављања илегалним миграцијама у Републици Србији за период 2009–2014. године, Службени гласник Републике Србије, бр. 25/09;

759 Стратегија борбе против трговине људима у Републици Србији, Службени гласник Републике Србије, бр. 111/06;

760 Закон о азилу, Службени гласник Републике Србије, бр. 109/07;

761 Закон о потврђивању споразума између Републике Србије и Европске заједнице о реадмисији лица која незаконито бораве, Службени гласник Републике Србије, бр. 103/07;

762 Eurostat, The number of asylum applicants registered in the EU27, (2011). http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/3-23032012-AP/EN/3-23032012-AP-EN.PDF (приступљено 12.10.2013);

763 Practical Measures to Reduce Irregular Migration, *European Migration Network, (2012), 17.* http://ec.europa.eu/dgs/home-affairs/what-we do/networks/european_migration_network/reports/docs/emn-studies/irregular-migration/00a_emn_synthesis_report_irregular_migration_october_2012_en.pdf. (приступљено 14.12.2013);

764 Frontex, Annual Risk Analysis, (2013), 77. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013);

765 Влада Републике Србије, (2013), Миграциони профил Републике Србије за 2012. годину, 50. http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDMQFjAB&url=http%3A%2F%2Fwww.kirs.gov.rs%2Fdocs%2Fmigracije%2FMigracioni_profil_Republike_Srbije_za_2012.pdf&ei=qhr

Због свог географског положаја Србија је важно транзитно подручје када је реч о ирегуларним миграцијама, али и дроги. Од 35.000 регистрованих илегалних прелазака границе у земљама Западног Балкана 2012. године чак 40% је одлазило на Србију[766]. Такође, сматра се да преко територије земаља бивше Југославије, међу којима је и Србија, стиже чак 80% од укупне количине дроге у Европи, која је пореклом из Авганистана, Пакистана и Ирана[767]. Границе Србије великим делом чине спољне границе са ЕУ, а након прикључења Хрватске Европској унији 1.7.2013. године, дужина спољних граница Србије ка ЕУ још се више повећала. С обзиром да се кријумчари веома брзо прилагођавају променама, мењајући руте кријумчарења, може се очекивати да улазак Хрватске у ЕУ утиче на промену праваца ирегуларних миграција.

Највећи број страних држављана који на недозвољен начин улазе на територију Републике Србије, покушава да оде даље у друге земље Европске уније. Међу ирегуларним мигрантима 2012. године у Србији су најбројнији били држављани Авганистана и Сирије, који су исте године чинили већину популације тражилаца азила у ЕУ. Ово потврђује повезаност система азила и ирегуларне миграције, тј. чињеницу да је подношење захтева за азил често алтернатива за имиграцију[768]. У земљама Западног Балкана забележен је пораст кријумчарења мигранта у возилима, нарочито на граници између Србије и Републике Македоније, са учешћем Авганистанаца од 45% у укупном броју кријумчарених лица у 2012. години[769]. Након проласка кроз Турску и Грчку секундарно кретање Авганистанаца, који чине највећи удео ирегуларних миграционих токова западнобалканске руте, прелази преко Македоније, Србије и Мађарске ка ЕУ. Међутим, током 2013. године, у структури ирегуларних миграционих токова у Србији, дошло је до смањења броја ирегуларних мигранта пореклом из Авганистана, уз преовлађујуће учешће лица из Сирије, Сомалије и Еритреје.

Ирегуларна миграција најчешће се остварује у фазама за које су задужене различите мање криминалне организације које сарађују транснационално[770]. Према савету кријумчара, ирегуларни мигранти, у случају хапшења, подносе захтев за азилом. Такође, кријумчари их често остављају у близини центара за азил, одакле они поново крећу на пут након неког времена. Ови центри, тако, постају део

---

sUsLDJMKjtAak_YHwBA&usg=AFQjCNFWyt7JvwZfh8QEXc_E40jqfussKA&sig2=AaePO2V_uotKeWFFIIeJhg (приступљено 29.10.2013);

766 Frontex, Annual Risk Analysis, (2013), 33.
http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013);

767 Mavris L. (2002), Human smugglers and social networks: transit migration through the states of former Yugoslavia Working Paper, New issues in refugee research, no. 72, UNHCR, 1.
http://www.unhcr.org/3e19aa494.pdf (приступљено 23.11.2013);

768 Hysmans J. (2006), The Politics of Insecurity. Fear, Migration and Asylum in the EU, London, Routledge; Kraler A., M. Rogoz (2011), Irregular migration in the European Union since the turn of the millennium –development, economic background and discussion, Database on Irregular Migration, Working paper 11/2011. http://irregular-migration.net/ (приступљено 12.12.2013));

769 Frontex, Annual Risk Analysis, (2013), 27.
http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (9.11.2013);

770 Frontex, Europol, 2007 Determination of High Risk Routes Regarding Illegal Migration in the Western Balkan Countries,10.
http://www.bing.com/search?q=Frontex,+Europol,+2007+Determination+of+High+Risk+Routes+Regarding+Illegal+Migration+in+the+Western+Balkan+Countries&src=IE-TopResult&FORM=IE11TR&conversationid= (приступљено 26.12.2013);

планске руте ирегуларних миграната[771]. С обзиром да путују на већим раздаљинама, ирегуларним мигрантима центри за азиланте у Србији најчешће служе као место за одмор. Они остају извесно време на територији Републике Србије, у прихватним центрима (Бања Ковиљача и Боговађа), подносећи захтев за азил. Лица која траже међународну заштиту у Србији најчешће изражавају намеру да траже азил пред полицијским службеницима на граници или након што уђу на територију земље. Док траје поступак азила[772], након извршеног здравственог прегледа, ова лица смештају се у центар за азиланте. Међутим, већина ових лица злоупотребљава право на азил и не дочека решавање захтева, те поступци бивају обустављени[773]. Од укупно 2.723 лица која су 2012. године изразила намеру за азилом у Србији, свега 12% је поднело захтев за азил, односно 8% у 2011. години[774]. Неки од ирегуларних миграната који су у Србији поднели захтев за азил и који су смештени у азилантске центре, откривени су у возовима ка Мађарској, покушавајући да стигну у ЕУ[775]. На феномен нестајања тражилаца азила током процедуре разматрања њиховог захтева указују и други аутори. Пораст злоупотребе система азила и центара за азил забележен је и у бројним земљама чланицама ЕУ (Мађарска, Пољска, Словачка, Словенија)[776]. Од 13.000 лица која су поднела захтев за азилом у Словенији 2000. године, чак 12.600 је напустило земљу за време разматрања њиховог захтева[777].

Немогућност утврђивања идентита ирегуларних миграната – тражилаца азила, с обзиром да највећи број њих нема никаква документа, веома је велики проблем. Ово је значајно како са аспекта праћења саме појаве, тако и из безбедоносних разлога. Поједини аутори истичу да су центри за азиланте средство миграционе контроле популације тражилаца азила, док су мигранти у земљи. Проучавање центара за азил у Чешкој указује да тражиоци азила приликом пријема у ове установе морају надлежним властима, за време боравка, да предају "средства за комуникацију" (мобилне телефоне) како би се спречило њихово бекство. Такође, сигурносна служба регрутује доушнике међу тражиоцима азила[778],

---

771 Futo P., M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2). Bilger V., M. Hofmann, M. Jandl (2006), Human Smuggling as a Transnational Service Industry: Evidence from Austria, International Migration, 44 (4);

772 До доношења одлуке може да прође најдуже шездесет дана;

773 Лукич В. (2013), Миграционные тенденции в Сербии, 279, Сербские научные исследования 2012. Сборник научных статей. – М.: Экон-информ, Москва, составитель А.Н. Новик,1-481;

774 Влада Републике Србије, (2013), Миграциони профил Републике Србије за 2012. годину, 42. http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDMQFjAB&url=http%3A%2F%2Fwww.kirs.gov.rs%2Fdocs%2Fmigracije%2FMigracioni_profil_Republike_Srbije_za_2012.pdf&ei=qhrsUsLDJMKjtAak_YHwBA&usg=AFQjCNFWyt7JvwZfh8QEXc_E4OjqfussKA&sig2=AaePO2V_uotKeWFFIIeJhg (приступљено 29.10.2013;

775 Frontex, Annual Risk Analysis, 2013, 35. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (приступљено 9.11.2013);

776 Jandl M. (2004), Research Note ''The Relationship between Human Smuggling and the Asylum System in Austria.'' Journal of Ethnic and Migration Studies, 30 (4); Futo P., M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2);

777 Požun B. J. (2001), "Just passing through: illegal immigrants find new back door to Europe in Slovenia," Central Europe Review, 3 (4). http://www.ce-review.org/01/4/pozun4.html (приступљено 10.12.2013);

778 Szczepanikova A. (2012), Between Control and Assistance: The Problem of European Accommodation Centres for Asylum Seekers, International Migration, 51 (4),133,134;

јер и сами тражиоци азила признају да имају сазнања како одређени број њих наменски жели да остане дуже смештен у центрима за азил. Ова лица делују као посредници између кријумчара и тражилаца азила смештених у центру, обезбеђујући им контакт и информације о месту и времену међусобног сусрета или одласка[779].

3. МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

За потребе овог проучавања обављена су 53 интервјуа са тражиоцима азила у центру за азил у Бањи Ковиљачи и 45 интервјуа са ирегуларним мигрантима. Категорија ирегуларних миграната обухватила је повратнике по основу Споразума о реадмисији, лица ухапшена приликом илегалног преласка границе, контроле саобраћајница, преноћишта, аутобуских и железничких станица, лица са фалсификованим документима, лица у Центру за смештај малолетних страних држављана без родитељске или старатељске пратње при Заводу за образовање деце и омладине "Васа Стајић" у Београду, лица у прихватилишту за странце у Падинској Скели у Београду и лица у поступку азила која још нису смештена у центре за азиланте. Разговори су обављени током јуна 2013. године од стране лица запослених у наведеним установама и припадника полиције и граничне полиције. Поред интервјуа обављених са тражиоцима азила и ирегуларним мигрантима, као допуна истраживању спроведена је анкета међу лицима запосленим у државним институцијама и невладиним организацијама, коју су током јуна 2013. године испунила 92 лица. Прикупљени подаци су обрађивани статистичком анализом у програмима Microsoft Excel и SPSS. Циљ анкете био је продубљивање сазнања о вези између ирегуларних миграција и коришћења савремених технологија, заснованих на конкретним случајевима у пракси. На корисност праксе укрштања података добијених од ирегуларних миграната и полицијских службеника, како би се додатно проверила стечена сазнања, указују и аутори финалног извештаја Clandestino пројекта[780].

Истраживање је обухватило и анкету спроведену међу шест туристичких агенција, чланица Националне асоцијације туристичких агенција Србије - YUTA, која је садржала питања о запажањима и сазнањима запослених о вези између путовања и ирегуларних миграција.

Проучавање популације ирегуларних миграната прате бројне потешкоће с обзиром да многи од њих немају документа или дају неистините податке. Стога, иако ово истраживање није репрезентативно, с обзиром на мали узорак, емпиријски резултати послужили су да се укаже у којој су мери ирегуларне миграције у Србији у вези са организованим криминалом, уз нагласак на употреби високих технологија у процесу миграције.

779 Bilger V. M. Hofmann, M. Jandl (2006), Human Smuggling as a Transnational Service Industry: Evidence from Austria, International Migration, 44 (4), 77;

780 Clandestino Project, Final report, (2009), 9
http://www.emnbelgium.be/publication/clandestino-project-final-report (приступљено 6.10.2013);

4. АНАЛИЗА РЕЗУЛТАТА

4.1. Тражиоци азила

Испитивану популацију тражилаца азила чинила су 53 лица смештена у центру за азиланте у Бањи Ковиљачи. Највећи број испитаника пореклом је из Сирије (20,8%) и Алжира (11,3%). Реч је о мушкој популацији (90,6%), старости 19-34 године (64,2%) из градских насеља (92,5%), која је претежно у браку (67,9%). Средње образовање има највећи број испитаника (69,8%), а од лица за која је позната област образовања чак 60% је стекло образовање у техничко-технолошкој области. С обзиром да је већина њих незапослена (98,1%), претежно су се изјаснили да свој економски статус сматрају веома лошим (47,2%). На економске разлоге миграције указује и старосно-полна структура испитиване групе тражилаца азила, с обзиром да популацију избеглица најчешће чине читаве породице[781]. Од 69,8% испитаника, који говоре један или више страних језика, највећи број њих говори енглески језик (37,7%). Већина испитаника познаје некога ко је већ боравио у Србији (73,6%), што упућује на путовање познатим рутама. Потврда деловања миграционих мрежа је и чињеница да чак 75,5% тражилаца азила има родбину и пријатеље у некој европској земљи.

Посебна пажња приликом интервјуисања тражилаца азила у Србији посвећена је коришћењу савремених технологија, како би се испитао њихов утицај на процес миграције. Велики број испитаника има мобилни телефон (47 лица или 88,7% испитаника), док знатно мањи број поседује рачунар (35 лица или 66,0%). Важно је напоменути да од тражилаца азила, који су се изјаснили да поседују рачунар, чак 60% има лаптоп/ноутбук.

Укупно 44 испитаника (83%) знају да користе рачунар и у том погледу запажен је статистички значај када је реч о вези између коришћења рачунара/интернета и школске спреме тражилаца азила, односно лица са вишим степеном образовања боље познају рад на рачунару и више користе интернет. Такође, постоји корелација између коришћења интернета и познавања страног језика, чиме је доказано да лица која користе интернет најчешће говоре неки страни језик (76,5%).

Иако 44 тражиоца азила тврде да знају да користе рачунар, чак 46 (86,8%) њих користи друштвене мреже, а 47 (88,7%) зна да приступи интернету, што указује на неискреност испитаника приликом давања одговора. Само седам тражилаца азила (13,2%) нема профил ни на једној друштвеној мрежи. Многи испитаници користе више друштвених мрежа, а најчешће коришћене друштвене мреже су *Facebook*, *Google+* и *Twitter*.

Упркос великом обиму коришћења рачунара, друштвених мрежа и телефона, 18 тражилаца азила (33,9%) сматра да им ова средства нису помогла у доношењу одлуке да мигрирају из земље порекла, 20 испитаника (37,7%) сматра да су им ови уређаји веома мало олакшали доношење одлуке, док само 15 лица (28,3%) сматра

781 Lukić V. V. Nikitović (2004), Refugees from Bosnia and Herzegovina in Serbia: A Study of Refugee Selectivity, International Migration, 42 (4), 95.; Nikitović V., V. Lukić (2010), Could Refugees Have a Significant Impact on the Future Demographic Change of Serbia?, International Migration, 48 (1), 6;

да им је коришћење рачунара или мобилних телефона доста помогло при доношењу одлуке о миграцији.

Укупно 23 тражиоца азила (43,4%) сматрају да им коришћење рачунара или мобилног телефона није помогло у одређивању земље дестинације, док је код 30 азиланата или 56,6%, коришћење рачунара или мобилног телефона било од користи приликом одређивања земље дестинације (15 лица или 28,3% испитаника сматра да им је помогло веома мало, док исти број мисли да им је то доста олакшало). Познавање страног језика има утицаја на коришћење рачунара/мобилног телефона приликом одређивања земље дестинације ($p<0,05$), тј. испитаницима који познају неки страни језик више је помогло коришћење мобилних телефона/рачунара у одређивању земље дестинације.

Када је реч о коришћењу рачунара или мобилног телефона приликом одређивања руте кретања, мишљења испитаника су прилично подељена. Укупно 17 испитаника (32,1%) сматра да им то није помогло приликом миграције, исти број тражилаца азила мисли да им је веома мало помогло, док 19 лица (35,8%) истиче да им је коришћење рачунара или мобилног телефона доста олакшало доношење одлуке о рути кретања. Постоје статистички значајне разлике ($p<0,05$) у помоћи ових уређаја приликом одређивања руте кретања у односу на пол испитаника, односно највећем броју жена (80,0%) коришћење мобилних телефона или рачунара није помогло у одређивању земље дестинације, док само 27,1% мушкараца дели исто мишљење.

Питање "да ли је коришћење рачунара или мобилног телефона утицало на одређивање ваше руте кретања?" укрштено је са питањима "колико вам је коришћење рачунара/мобилних телефона помогло у доношењу одлуке о миграцији/одређивању дестинације миграције?", чиме је потврђена висока, статистички значајна разлика ($p<0,001$), односно већини лица којима коришћење рачунара/мобилних телефона није помогло у доношењу одлуке о миграцији/одређивању земље дестинације, коришћење мобилних телефона или рачунара није помогло ни приликом одређивања руте кретања.

Коришћење рачунара или мобилног телефона је доста помогло 21 тражиоцу азила (39,6%) да самостално мигрира, без помоћи других лица; 15 лица (28,3%) сматра да им је коришћење савремене технологије веома мало помогло приликом миграције; док се 17 испитаника (32,1%) изјаснило да им то није било од помоћи. Постоје статистички значајне разлике ($p<0,05$) у односу на пол, па већини жена (80,0%) коришћење мобилних телефона или рачунара није помогло да самостално мигрирају, без помоћи других лица, док чак 43,7% мушкараца сматра да им је коришћење мобилних телефона или рачунара доста помогло да самостално мигрирају.

Постоје разлике приликом коришћења рачунара/мобилног телефона за самосталну миграцију и у односу на државу порекла тражилаца азила ($p<0,05$). Коришћење мобилних телефона или рачунара је највише помогло испитаницима из Алжира (23,8%), Сирије (19,1%) и Авганистана (14,3%) да самостално мигрирају, без помоћи других лица.

Разлике у коришћењу рачунара или мобилних телефона, као помоћи тражиоцима азила да самостално мигрирају, у односу на познавање страног језика су изузетно статистички значајне ($p<0,005$). Испитаницима који познају неки страни језик коришћење мобилних телефона или рачунара је више помогло да самостално мигрирају.

Висока статистичка значајност ($p<0,001$) потврђена је приликом укрштања питања „да ли је коришћење рачунара/мобилних телефона помогло тражиоцима азила да самостално мигрирају?“ са питањем „колико је коришћење рачунара/мобилних телефона помогло азилантима приликом одређивања земље дестинације и руте кретања?“. У оба случаја је потврђено да већина испитаника, којима коришћење савремене технологије није помогло да самостално мигрирају, није имала користи од рачунара/мобилног телефона приликом одређивања земље дестинације или руте кретања.

Коришћење рачунара или мобилног телефона помогло је чак у случају 34 тражиоца азила (64,2%) да ступе у контакт са другим мигрантима – кријумчарима, док њих 11 сматра да им је то веома мало помогло, а њих 23 (43,4%) каже да им је то пружило велику помоћ у остварењу контаката. Само 19 испитаника (35,9%) сматра да им коришћење рачунара или мобилног телефона није помогло да ступе у контакт са другим мигрантима – кријумчарима.

Постоје значајне разлике у односу на познавање страног језика ($p<0,005$), тј. испитаници који знају страни језик више су користили мобилне телефоне или рачунаре како би ступили у контакт са другим мигрантима или кријумчарима.

Питање коришћења мобилног телефона или рачунара како би ступили у везу са осталим мигрантима или кријумчарима, укрштено је са питањима о коришћењу рачунара или мобилног телефона при доношењу одлуке о дестинацији, рути кретања или самосталном кретању миграната, и у свим случајевима је потврђена позитивна корелација.

Прилично је уједначен број тражилаца азила који су уз помоћ рачунара или телефона комуницирали са мигрантима-кријумчарима приликом миграције (26 или 49,1%) и оних који нису комуницирали са мигрантима или кријумчарима за време остваривања миграције (27 или 50,9%).

Највећи број испитаника (32 особе или 60,4%) мисле да би успели да дођу у Србију и без помоћи рачунара/мобилног телефона, а само њих 7 (13,2%) сматра да без коришћења савремене технологије не би успели да мигрирају.

Само 12 мигранта (22,6%) би другим, потенцијалним мигрантима, препоручили да се самостално или уз помоћ рачунара-мобилног телефона пребаце из земље порекла у земљу дестинације, док 24 испитаника (45,3%) не би то препоручило. Остали испитаници (17 или 32,1%) нису одлучни по овом питању.

4.2. Ирегуларни мигранти

Популацију ирегуларних мигранта у овом истраживању чинило је 45 ирегуларних мигранта, од којих је највећи број интервјуисан у Београду (51,1% испитаника) и Прешеву (11,1%). Већина испитаника пореклом је из Србије (28,9%), Авганистана (15,6%) и из АП Косова и Метохије (11,1%). Реч је о мушкој популацији (82,2%), претежне старости 19-33 године (73,3%), већином из градских насеља (91,1%) и ромске националности (40%). Основно образовање има највећи број испитаника (28,9%). С обзиром да је већина њих незапослена (97,8%), претежно су се изјаснили да свој економски статус сматрају лошим (46,7%). Највећи број испитаника не говори ниједан страни језик (55,6%).

Посебна пажња у истраживању ирегуларних мигранта посвећена је коришћењу савремених технологија и њихове помоћи у остваривању процеса

миграције – кријумчарења. Највећи број ирегуларних мигранта поседује мобилни телефон (42 особе или 93,3%), док рачунар поседује свега 14 испитаника или 31,1%. Па ипак, више од половине ирегуларних мигранта (24 лица или 54,5% од броја лица која су дала одговор на ово питање) зна да користи рачунар. Запажа се логична веза између степена образовања и познавања рада на рачунару. Сва лица са средњом или вишом/високом школском спремом познају рад на рачунару, у односу на лица без образовања или са непотпуном основном школом, од којих већина не зна да користи рачунар (63,6% односно, 87,5%).

Највећи број ирегуларних мигранта не користи интернет (27 лица или 60,0% испитаника). Ако посматрамо коришћење интернета у односу на школску спрему ирегуларних мигранта, можемо закључити, као и код коришћења рачунара, да лица која користе интернет најчешће имају вишу школску спрему. Познавање страног језика, такође, има утицаја на коришћење интернета ($p<0,005$). Од укупног броја лица који говоре неки страни језик, 65% користи интернет, док од укупног броја ирегуларних мигранта који не говоре страни језик, само 20% користи интернет.

Премда се 18 испитаника изјаснила да користи интернет, 20 лица је навело да користи друштвене мреже, што упућује на неистинитост приликом давања одговора. Више од половине ирегуларних мигранта не користи друштвене мреже (25 особа или 55,6% испитаника). Најчешће коришћена друштвена мрежа је *Facebook* коју користи 13 испитаника. Постоји статистичка значајност ($p<0,05$) када је реч о коришћењу друштвених мрежа и школској спреми ирегуларних мигранта, тј. лица која имају виши степен образовања чешће користе друштвене мреже.

Највећи број ирегуларних мигранта сматра да им коришћење рачунара или мобилних телефона није помогло да донесу одлуку о мигрирању из земље порекла, затим приликом одређивања земље дестинације и руте кретања. Удео лица која су на претходна питања одговорила да им је употреба мобилног телефона или рачунара доста помогла, креће се од 13% до 20%. Постоји корелација између коришћења рачунара или мобилних телефона како би се одредила рута кретања/донела одлука о земљи дестинације и школске спреме ирегуларних мигранта. Ирегуларни мигранти који су без образовања, немају завршену основну школу или имају само основно образовање су лица која су се изјаснила да им коришћење савремене технологије није помогло приликом одређивања земље дестинације и руте кретања.

На одређивање руте кретања и земље дестинације утицај има и познавање страног језика. Већини ирегуларних мигранта, који говоре неки страни језик, коришћење савремене технологије је помогло у одређивању земље дестинације или руте кретања (70% или 65%), док највећем броју ирегуларних мигранта, који не говоре страни језик, није помогло (64 или 84%).

Од укупног броја ирегуларних мигранта њих 16 (35,6%) сматра да им коришћење мобилних телефона или рачунара није помогло да самостално мигрирају без ичије помоћи, 24 ирегуларна мигранта (53,3%) сматрају да им је помогло веома мало, а само 5 испитаника (11,1%) сматра да им је доста помогло. Међутим, 26 ирегуларних мигранта (57,8%) сматра да им је коришћење мобилног телефона или рачунара помогло да ступе у контакт са другим ирегуларним мигрантима или кријумчарима (12 лица мисли да им је помогло веома мало, а 14 да им је доста помогло). За 19 испитаника (42,2%) коришћење савремене

технологије није помогло у контактима са другим ирегуларним мигрантима или кријумчарима.

Школска спрема ирегуларних миграната има утицаја на коришћење мобилних телефона или рачунара као помоћ ирегуларним мигрантима да самостално мигрирају ($p<0,01$). Испитаницима са вишом или високом школском спремом коришћење савремене технологије је доста помогло да самостално мигрирају, док је ирегуларним мигрантима са нижом школском спремом коришћење савремене технологије мало помогло или није уопште помогло да самостално мигрирају. Статистичка значајност постоји и у корелацији питања о самосталној миграцији уз помоћ технологије и питања о познавању страног језика. Ирегуларним мигрантима који познају неки страни језик више је помогло коришћење савремене технологије да мигрирају без ичије помоћи. За 20% лица која познају неки страни језик коришћење савремене технологије није помогло у самосталној миграцији, док је то 48% у случају лица која не познају ниједан страни језик. Познавање језика показало се као значајно и у контактима са другим мигрантима или кријумчарима. Употреба рачунара/мобилног телефона доста је помогла ирегуларним мигрантима у контакту са другим мигрантима или кријумчарима, за 50% лица која говоре неки страни језик и свега 16% испитаника који не познају ниједан страни језик.

Ирегуларни мигранати углавном нису комуницирали са другим ирегуларним мигрантима или кријумчарима током миграције (33 особа или 73,3% испитаника), док је само 12 миграната (26,7%) користило савремену технологију у ове сврхе. У поређењу са питањем „да ли је коришћење рачунара или телефона помогло ирегуларним мигрантима да ступе у контакт са другим мигрантима или кријумчарима?“ потврђене су разлике које су статистички високо значајне ($p<0,001$). Чак 83,3% ирегуларних миграната који користили мобилне телефоне или рачунаре за комуникацију током трајања миграције, сматра да им је коришћење савремене технологије доста помогло у контактима са другим ирегуларним мигрантима или кријумчарима.

Да би успели да мигрирају и без помоћи рачунара или мобилних телефона сматра мање од половине ирегуларних миграната (21 или 46,7%), док само шест ирегуларних миграната (13,3%) сматра да не би успели да мигрирају без помоћи савремене технологије. Остали испитаници нису сигурни да ли им је била неопходна помоћ савремене технологије током миграције.

Тестирано је да ли постоји разлика у броју ирегуларних миграната који не би успели да мигрирају без коришћења мобилних телефона или рачунара и лица којима су ови уређаји помогли у контактима са другим ирегуларним мигрантима или кријумчарима, чиме је потврђено да постоји статистички значајна разлика ($p<0,01$). Већина ирегуларних миграната, која сматра да би успели да мигрирају без коришћења средстава савремене технологије, изјавила је да им коришћење телефона или рачунара није помогло у остваривању контаката са другим ирегуларним мигрантима или кријумчарима и обрнуто.

Само 4 ирегуларна мигранта (8,9%) би другим, потенцијалним мигрантима, препоручили да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације, 24 (53,3%) им не би препоручило да самостално мигрирају, док би 17 ирегуларних миграната (37,8%) можда препоручило другим потенцијалним мигрантима да самостално мигрирају, уз помоћ мобилних телефона или рачунара.

4.3. Иregуларни мигранти – оперативна сазнања

Анкетом спроведеном са циљем продубљивања сазнања о вези између високих технологија и иregуларних миграција, на основу случајева у пракси, обухваћена су 92 испитаника запослена у државним институцијама и невладиним организацијама, од којих највећи број ради у државном сектору (90 или 97,8%). Уједначен је број испитаника који поступају превентивно, репресивно или хуманитарно према иregуларним мигрантима (34,8%, испитаника поступа превентивно, 32,9%, репресивно, а 32,3% хуманитарно), премда већина поступа истовремено и превентивно и репресивно. Највећи број испитаника (54 или 59,3%) има сазнања да су иregуларни мигранти, са чијим су се случајевима сусретали, током миграције користили интернет. Са друге стране, прилично је уједначен број испитаника који имају сазнања да су иregуларни мигранти током миграција користили друштвене мреже (45 испитаника или 49,4% од лица која су се изјаснила по овом питању) и оних који ова сазнања немају. Најчешће коришћена друштвена мрежа од стране иregуларних мигранта била је *Facebook* (12 или 27,3%), а затим следе *Twitter* и *Google+.*

Већина испитаника (74 или 82,2% од лица која су се изјаснила по овом питању) има сазнања да су иregуларни мигранти током илегалног преласка/боравка користили мобилни телефон или рачунар, док се 16 лица (17,8%) изјаснило да нема оваквих сазнања. Међутим, само 25 испитаника (27,8% од лица која су се изјаснила по овом питању) има сазнања да су иregуларни мигранти користили посебне апликације на мобилним телефонима или рачунарима (ГПС) како би одредили руту кретања. Нешто више од половине испитаника (52 или 57,1%) има искуство да су иregуларни мигранти користили рачунаре или мобилне телефоне за контакт са породицом, док само 8 испитаника (8,8%) сматра да иregуларни мигранти нису овим путем контактирали са породицом за време миграције. Остала лица изјаснила су се да немају сазнања о овој појави (31 или 34,1% од лица која су се изјаснила по овом питању).

Да је коришћење рачунара или мобилног телефона доста помогло иregуларном мигранту да самостално, без помоћи других лица, дође у Србију сматра већина испитаника (42 или 45,7%). Сазнања у вези ове теме нема 30 лица или 33,3%, док 17 (18,9%) испитаника сматра да је коришћење мобилног телефона или рачунара веома мало помогло иregуларном мигранту у процесу миграције. Већина испитаника има сазнања да је коришћење мобилног телефона или рачунара помогло иregуларним мигрантима да ступе у контакт са другим иregуларним мигрантима или кријумчарима. Чак 50 лица или 56,8% сматра да им је то доста помогло приликом миграције, док 16 лица или 18,2% испитаника мисли да им је коришћење мобилног телефона или рачунара веома мало помогло да ступе у контакт са другим иregуларним мигрантима или кријумчарима. Остали испитаници (22 или 25%) су се изјаснили да немају сазнања на ову тему.

Да иregуларни мигранти не би успели да постигну досадашњи ток на путу иregуларних миграција без помоћи рачунара или мобилног телефона сматра 37 испитаника (42% од укупног броја испитаника који су се изјаснили по овом питању), док је 40 лица (45,5%) на ово питање одговорило са "можда". Само 11 испитаника (12,5%) сматра да би иregуларни мигранти ипак успели да пређу пут којим су дошли и без помоћи савремене технологије. Највећем броју лица (47 или 53,4%) није познато да ли су иregуларни мигранти користили мобилне телефоне/рачунаре на

јавним местима, у циљу самосталног организовања и креирања даље руте кретања (интернет-кафе, парк, шопинг-центар, трг или друго јавно место), 27 лица (30,7%) одговорило је позитивно, док се 14 испитаника (15,9%) изјаснило да није имало случајеве да су ирегуларни мигранти користили мобилне телефоне/рачунаре на јавним местима.

4.4. Туристичке агенције

Када је реч о анкети спроведеној међу туристичким агенцијама, на питања "да ли је било случајева фалсификованих докумената код путника?", "да ли је нека туристичка агенција изгубила лиценцу због везе са трговином људима?", "да ли је нека туристичка агенција изгубила лиценцу због ирегуларних миграција?", "да ли је неко лице запослено у туристичкој агенцији кажњено за трговину људима?", "да ли је неко лице запослено у туристичкој агенцији кажњено због ирегуларних миграција?", "да ли је било случајева организовања путовања у иностранство ради тзв. Секс- туризма?", "да ли је било случајева да је организован превоз малолетних лица ради криминалних радњи?", "да ли је било случајева путовања у иностранство због нуђења незаконитих медицинских услуга?" све агенције су одговориле негативно. Један потврдан одговор је дат само на питање "да ли је било случајева да су поједини путници остали ван земље приликом путовања?", уз образложење да немају податке али да су чули да је било доста таквих случајева.

5. УПОРЕДНА АНАЛИЗА КОРИШЋЕЊА САВРЕМЕНИХ ТЕХНОЛОГИЈА У ОСТВАРИВАЊУ ПРОЦЕСА МИГРАЦИЈЕ/КРИЈУМЧАРЕЊА (ТРАЖИОЦИ АЗИЛА, ИРЕГУЛАРНИ МИГРАНТИ, ИРЕГУЛАРНИ МИГРАНТИ-ОПЕРАТИВНА САЗНАЊА)

Мобилни телефон у великој мери поседују и тражиоци азила (88,7%) и ирегуларни мигранати (93,3%). Међутим, важно сазнање је да тражиоци азила у већој мери поседују лаптоп и ноутбук рачунаре и рачунаре уопште, у односу на ирегуларне мигранте.

Табела 1. Тражиоци азила и ирегуларни мигранти према поседовању мобилних телефона

Поседовање мобилног телефона		Тражиоци азила	Ирегуларни мигранти
да	број	47	42
	%	88,7	93,3
не	број	6	3
	%	11,3	6,7

Табела 2. Тражиоци азила и ирегуларни мигранти према поседовању рачунара

Поседовање рачунара	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
да, десктоп	14	26,4	10	22,2
да, лаптоп	21	39,6	4	8,9
не	18	33,9	31	68,9
укупно	53	100,0	45	100,0

Утврђена је статистички значајна разлика ($p<0,01$) у познавању рада на рачунару између тражилаца азила и ирегуларних мигранта, односно ирегуларни мигранти мање знају да користе рачунар (53,3%), у односу на тражиоце азила, од којих чак 83% зна да користи рачунар.

Табела 3. Тражиоци азила и ирегуларни мигранти према познавању рада на рачунару

Познавање рада на рачунару	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
да	44	83,0	24	53,3
не	9	17,0	20	44,4
није унето	-	-	1	2,2
укупно	53	100,0	45	100,0

У оквиру истраживања тестирано је да ли у процесу ирегуларних миграција постоје статистички значајне разлике у коришћењу интернета између популација тражилаца азила, ирегуларних мигранта и кријумчара. Резултати анализе указују да азиланти више користе интернет (88,7%), у односу на ирегуларне мигранте (40%) и ирегуларне мигранте – оперативна сазнања (58,7%), те да је ова разлика изузетно статистички значајна. Према оперативним сазнањима, више од половине кријумчара (52,8%), такође, користи интернет.

Табела 4. Коришћење интернета у процесу ирегуларних миграција

Да ли испитаници користе интернет?	Тражиоци азила	Ирегуларни мигранти	Ирегуларни мигранти (оперативна искуства)	Кријумчари (оперативна искуства)	Укупно
да	47	18	54	46	165
не	6	27	37	41	111
није унето	-	-	1	1	2
укупно	53	45	92	88	278

Ирегуларни мигранти - ирегуларни мигранти (оперативна искуства): (χ^2=4.52, df=1, p<0.05)

Ирегуларни мигранти – тражиоци азила: (χ^2=54.08, df=1, p<0.001)

Ирегуларни мигранти (оперативна искуства) – тражиоци азила: (χ^2=13.81, df=1, p<0.001)

Ирегуларни мигранти - ирегуларни мигранти (оперативна искуства) – тражиоци азила: (χ^2=25.72, df=4, p<0.01)

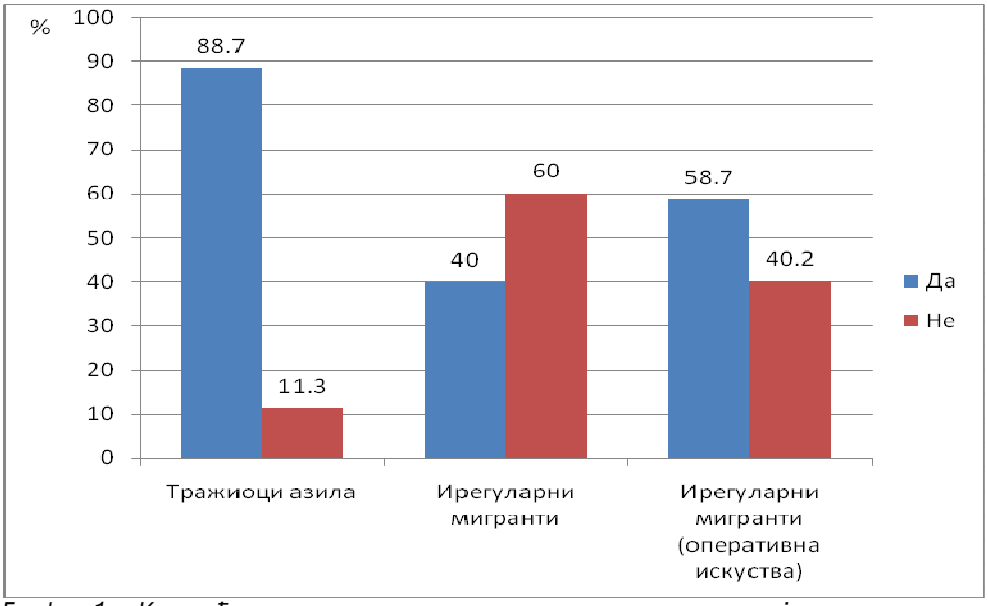


График 1. Коришћење интернета у процесу ирегуларних миграција

Као и код коришћење интернета, тако и код коришћења друштвених мрежа постоје разлике између тражилаца азила, ирегуларних мигранта и ирегуларних мигранта (оперативна искуства), које су статистички изузетно високог значаја. У структури посматраних популација чак 86,8% тражилаца азила користи друштвене мреже, односно 48,9% према оперативним сазнањима о ирегуларним мигрантима и 48,3% у случају кријумчара. Ирегуларни мигранти најмање користе друштвене мреже у процесу ирегуларних миграција (44,4%).

Табела 5. Коришћење друштвених мрежа у процесу ирегуларних миграција

Да ли испитаници користе друштвене мреже?	Тражиоци азила	Ирегуларни мигранти	Ирегуларни мигранти (оперативна искуства)	Кријумчари (оперативна искуства)	Укупно
да	46	20	45	42	153
не	7	25	46	45	123
није унето	-	-	1	1	2
укупно	53	45	92	88	278

Ирегуларни мигранти - ирегуларни мигранти (оперативна искуства): (χ^2=0.28, df=1, p>0.05)

Ирегуларни мигранти – тражиоци азила: (χ^2=13.88, df=1, p<0.001)

Ирегуларни мигранти (оперативна искуства) – тражиоци азила: (χ^2=13.35, df=1, p<0.001)

Ирегуларни мигранти - Ирегуларни мигранти (оперативна искуства) – Тражиоци азила: (χ^2=16.13, df=4, p<0.001)

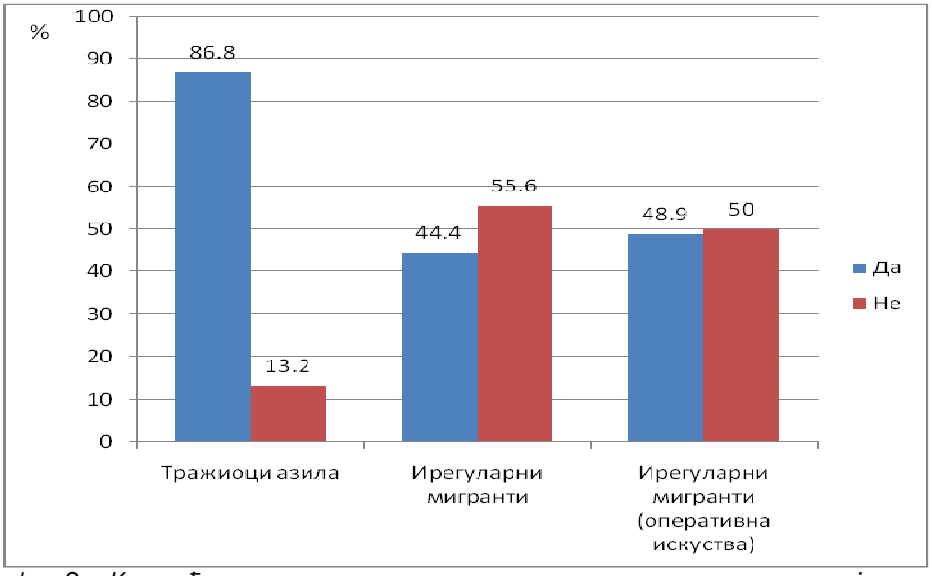


График 2. Коришћење друштвених мрежа у процесу ирегуларних миграција

Многи испитаници навели су да користе више од једне друштвене мреже. Најчешће коришћене друштвене мреже су *Facebook,* коју користи 79,2% тражилаца азила, 44,2% ирегуларних мигранта, 43,5% ирегуларних мигранта (оперативна искуства) и 46,6% кријумчара, затим *Twitter, Google+, Foursquare* и друге.

Табела 6. Најчешће коришћене друштвене мреже у процесу ирегуларних миграција

Да ли користите друштвене мреже?	Тражиоци азила	Ирегуларни мигранти	Ирегуларни мигранти (оперативна искуства)	Кријумчари (оперативна искуства)
Facebook	42	19	37	41
Google+	42	6	16	12
Twitter	31	2	21	14
Foursquare	1	1	-	0
LinkedIn	-	-	4	3
друге	21	1	7	2
нема налог	5	24	41	7

Да им је коришћење мобилних телефона или рачунара доста помогло да донесу одлуку да мигрирају сматра 28,3% тражилаца азила и 20% ирегуларних мигранта, 37,8% испитаника обеју група сматра да им је помогло веома мало, док су 33,9% тражилаца азила и чак 42,2% ирегуларних мигранта мишљења да им коришћење савремене технологије није помогло при доношењу одлуке о миграцији.

Табела 7. Коришћење мобилних телефона или рачунара

Коришћење мобилних телефона или рачунара при доношењу одлуке да мигрирају	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
није ми помогло	18	33,9	19	42,2
веома мало	20	37,7	17	37,8
доста ми је помогло	15	28,3	9	20,0
укупно	53	100,0	45	100,0

Иако нису доказане статистички значајне разлике између тражилаца азила и ирегуларних мигранта у одређивању земље дестинације, помоћу коришћења рачунара или мобилних телефона, ипак се уочава да је у популацији тражилаца азила већи проценат лица којим су ови уређају помогли приликом миграције.

Табела 8. Коришћење рачунара или мобилних телефона

Коришћење рачунара и мобилних телефона при одређивању земље дестинације	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
није ми помогло	23	43,4	22	48,9
веома мало	15	28,3	17	37,8
доста ми је помогло	15	28,3	6	13,3
укупно	53	100,0	45	100,0

Разлика између популација тражилаца азила и ирегуларних миграната, у томе колико им је коришћење мобилних телефона или рачунара помогло при одређивању руте кретања, статистички је значајна ($p<0,05$), тј. коришћење мобилних телефона или рачунара је више помогло тражиоцима азила него ирегуларним мигрантима при одређивању руте кретања.

Табела 9. Коришћење рачунара/мобилних телефона

Коришћење рачунара и телефона при одређивању руте кретања	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
није ми помогло	17	32,1	28	62,2
веома мало	17	32,1	8	17,8
доста ми је помогло	19	35,8	9	20,0
укупно	53	100,0	45	100,0

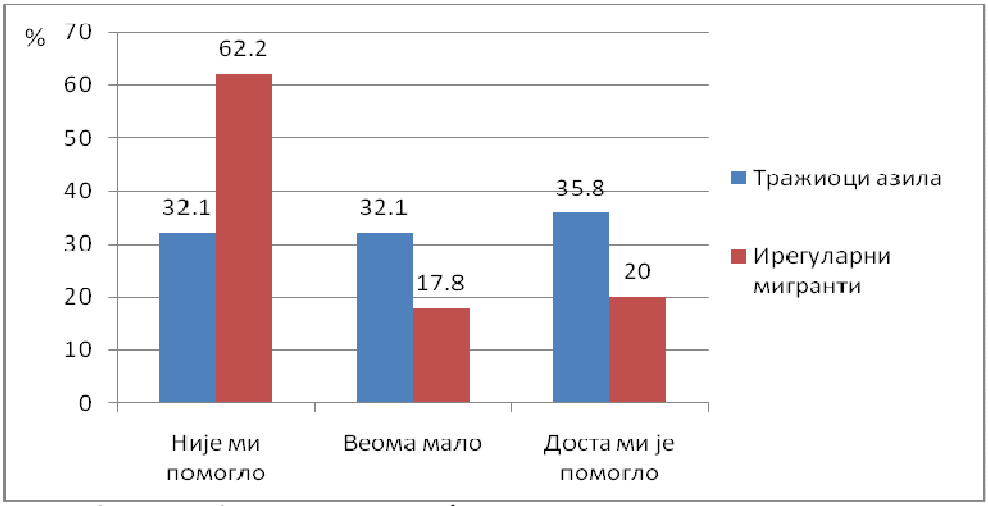


График 3. Коришћење рачунара/мобилних телефона

Већина испитаника има оперативна сазнања да су ирегуларни мигранти и кријумчари користили мобилне телефоне или рачунаре (82% ирегуларних миграната и 85% кријумчара) у процесу миграције.

Табела 10. Коришћење мобилних телефона или рачунара током илегалног преласка границе

Коришћење мобилног телефона или рачунара		Ирегуларни мигранти (оперативна искуства)	Кријумчари (оперативна искуства)
да	број	74	74
	%	82,2	85,1%
не	број	16	13
	%	17,8	14,9

Међутим, према оперативним сазнањима, највећи број ирегуларних мигранта (70,6%) и кријумчара (77,3%) није користио посебне апликације (ГПС) на мобилним телефонима или рачунарима приликом одређивања руте кретања, у процесу ирегуларних миграција.

Табела 11. Коришћење посебних апликација (ГПС) на мобилном телефону

Коришћење посебних апликација (ГПС) на мобилном телефону или рачунару у процесу ирегуларних миграција	Ирегуларни мигранти (оперативна искуства)		Кријумчари (оперативна искуства)	
	Број	%	Број	%
да	25	27,2	17	19,3
не	65	70,6	68	77,3
непознато	2	2,2	3	3,4

Између свих посматраних група – тражиоци азила, ирегуларни мигранти и ирегуларни мигранти (оперативна искуства) - постоје изузетно велике разлике у односу на то колико им је коришћење мобилног телефона или рачунара помогло да самостално мигрирају. Највећем броју ирегуларних мигранта је коришћење савремене технологије веома мало помогло да мигрирају без ичије помоћи, док је већини тражилаца азила као и ирегуларним мигрантима, према оперативним искуствима, доста помогло коришћење савремене технологије. Можемо закључити да је коришћење савремене технологије помогло при миграцији 64,4% ирегуларних мигранта, 98,3% ирегуларних мигранта (оперативна искуства) и 67,9% тражилаца азила.

Табела 12. Коришћење мобилних телефона/рачунара као помоћ испитаницима да самостално без помоћи других лица спроведу процес миграције

Колико вам је рачунар/мобилни телефон помогао да самостално, без помоћи других лица пређете до овог места?	Тражиоци азила		Ирегуларни мигранти		Ирегуларни мигранти (оперативна сазнања)		Укупно
	Број	%	Број	%	Број	%	Број
није му помогло	17	32,1	16	35,5	1	1,7	34
веома мало	15	28,3	24	53,3	17	28,3	56
доста је помогло	21	39,6	5	11,1	42	70,0	68
укупно	53	100,0	45	100,0	60[782]	100,0	158

782 Да немају сазнања на ову тему изјаснило се 30 испитаника, док за још два испитаника нема података;

Ирегуларни мигранти - ирегуларни мигранти (оперативна искуства): (χ^2=42.28, df=4, p<0.001)

Ирегуларни мигранти – тражиоци азила: (χ^2=11.38, df=4, p<0.001)

Ирегуларни мигранти (оперативна искуства) – тражиоци азила: (χ^2=20.99, df=4, p<0.001)

Ирегуларни мигранти - ирегуларни мигранти (оперативна искуства) – тражиоци азила: (χ^2=57.90, df=6, p<0.001)

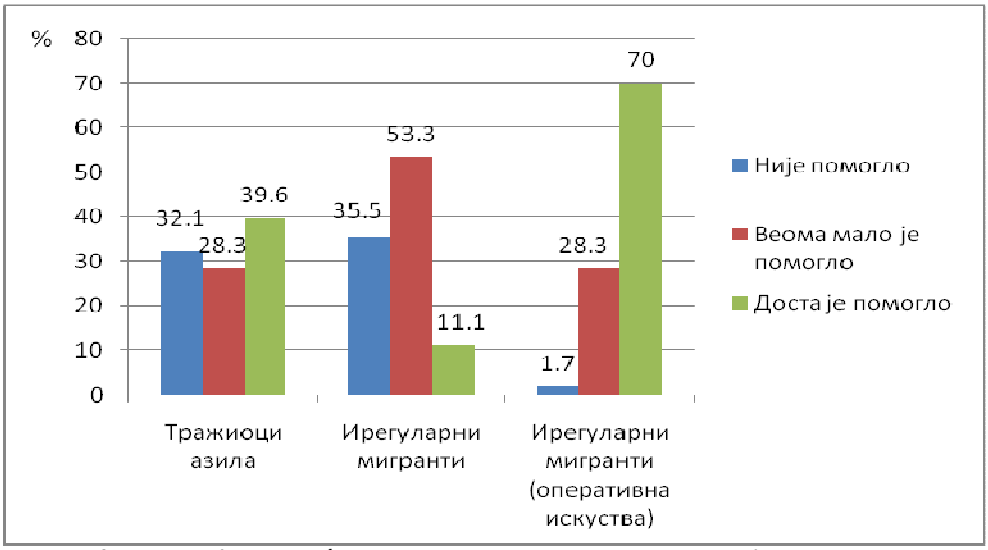


График 4. Коришћење мобилних телефона/рачунара као помоћ испитаницима да самостално без помоћи других лица спроведу процес миграције

Тестирана је хипотеза да ли постоје статистички значајне разлике између истраживаних популација у погледу коришћењу мобилних телефона и рачунара како би ступили у контакт са другим мигрантима или кријумчарима, и потврђено је да постоје високо статистички значајне разлике (p<0.001). Већини ирегуларних миграната (75,8%), према оперативним сазнањима, коришћење мобилних телефона или рачунара је доста помогло у контакту са другим мигрантима или кријумчарима, док 43,4% тражилаца азила и 31,1% ирегуларних миграната има исто мишљење. У популацији ирегуларних миграната највећи је удео лица (42,2%) која су се изјаснила да сматрају да им није помогло коришћење савремене технологије у контактима са другим ирегуларним мигрантима или кријумчарима, док 35,8% тражилаца азила дели исто мишљење. Међутим, ниједан испитаник из групе ирегуларни мигранти (оперативна искуства), који има сазнања о овој појави, не сматра да ирегуларним мигрантима није помогло коришћење мобилних телефона или рачунара ради остваривања контакта са другим мигрантима/кријумчарем, барем у одређеној мери. Такође, према оперативним сазнањима великом броју кријумчара (70%) је коришћење мобилних телефона или рачунара доста помогло у контакту са другим кријумчарима и ирегуларним мигрантима.

Табела 13. Коришћење рачунара/мобилних телефона при остваривању контакта са другим мигрантима/кријумчарима

Колико вам је рачунар/мобилни телефон помогао у контактима са другим мигрантима – кријумчарима?	Тражиоци азила		Ирегуларни мигранти		Ирегуларни мигранти (оперативна искуства)		Кријумчари (оперативна искуства)	
	Број	%	Број	%	Број	%	Број	%
није ми помогло	19	35,8	19	42,2	0	0,0	2	2,3
веома мало	11	20,7	12	26,7	16	24,2	2	2,3
доста је помогло	23	43,4	14	31,1	50	75,8	62	70,5
укупно	53	100,0	45	100,0	66[783]	100,0	66	100,0

Већина ирегуларних миграната није комуницирала са другим ирегуларним мигрантима или кријумчарима током миграције (33 особа или 73,3% испитаника), док је само 12 ирегуларних миграната (26,7%) користило савремену технологију током миграција. У случају тражилаца азила подједнак број испитаника је одговорио потврдно и одрично на питање о комуникацији са мигрантима/кријумчарима током миграције.

Табела 14. Коришћење рачунара/мобилних телефона за комуницирање са ирегуларним мигрантима/ријумчарима за време остваривања миграције/кријумчарења

Да ли су испитаници комуницирали са мигрантима/кријумчарима током миграције?	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
Да	26	49,1	12	26,7
Не	27	50,9	33	73,3
Укупно	53	100,0	45	100,0

Постоје статистички значајне разлике између ирегуларних миграната и тражилаца азила у контактирању путем мобилних телефона или рачунара током миграције са другим ирегуларним мигрантима или кријумчарима, које указују да су тражиоци азила више комуницирали са кријумчарима у односу на ирегуларне мигранте.

Према оперативним сазнањима, већина кријумчара и знатан број ирегуларних миграната не би успео на путу ирегуларних миграција или кријумчарења без помоћи мобилних телефона или рачунара. Међутим, у популацији тражилаца азила и ирегуларних миграната преовладава мишљење да би ипак успели да остваре процес миграције и без помоћи високих технологија. Међутим, оперативна сазнања указују да ирегуларни мигранти, ипак, у већој мери не би успели да дођу у Србију без помоћи мобилних телефона или рачунара.

783 Двадесет два испитаника су се изјаснила да им није познато да ли су ирегуларни мигранти или кријумчари користили рачунаре/мобилне телефоне за контакт са другим мигрантима или кријумчарима током миграције, док подаци за остала лица нису унети.

Табела 15. Остваривање процеса миграције-кријумчарења без помоћи рачунара-мобилног телефона

Да ли бисте успели да дођете у Србију без помоћи рачунара/мобилног телефона?	Тражиоци азила		Ирегуларни мигранти		Ирегуларни мигранти (оперативна искуства)		Кријумчари (оперативна искуства)	
	Број	%	Број	%	Број	%	Број	%
да	32	60,4	21	46,7	11	12,5	6	6,8
не	7	13,2	6	13,3	37	42,0	54	61,4
можда	14	26,4	18	40,0	40	45,5	28	31,8
укупно	53	100,0	45	100,0	88[784]	100,0	88	100,0

У упитницима за ирегуларне мигранте и кријумчаре (оперативна искуства) постављено је и питање да ли имају сазнања да су ова лица користила мобилне телефоне или рачунаре на јавним местима у циљу организовања и креирања даље руте кријумчарења ирегуларних миграната (интернет-кафе, парк, шопинг-центар, трг или друго јавно место). Већина испитаника (која су унела одговор на то питање) нема ту информацију, док око трећине испитаника (30% ирегуларних миграната и око 35% кријумчара) има сазнања да су посматране групе користиле мобилне телефоне или рачунаре на јавним местима.

Табела 16. Коришћење мобилних телефона/рачунара на јавним местима, у циљу организовања и креирања даље руте кријумчарења ирегуларних миграната

Коришћење мобилних телефона/рачунара на јавним местима мигранта	Ирегуларни мигранти		Кријумчари	
	Број	%	Број	%
да	27	30,6	31	35,2
не	14	15,9	11	12,5
непознато	47	53,4	46	52,3
није унето	4	4,5	-	-
укупно	92	100,0	88	100,0

Веома мали број испитаника се изјаснио да би другим, потенцијалним мигрантима препоручили да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације. Премда не постоје статистички значајне разлике између ирегуларних миграната и тражилаца азила, по овом питању, подаци указују да би то у већој мери учинили тражиоци азила.

784 За четири испитаника нису унети подаци.

Табела 17. Препорука потенцијалним мигрантима да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације

Да ли бисте другим, потенцијалним мигрантима препоручили да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације?	Тражиоци азила		Ирегуларни мигранти	
	Број	%	Број	%
да	12	22,6	4	8,9
не	24	45,3	24	53,3
можда	17	32,1	17	37,8
укупно	53	100,0	45	100,0

6. ЗАКЉУЧЦИ И ПРЕПОРУКЕ

Резултати истраживања указују на постојање везе између ирегуларних миграција и употребе високих технологија. Популација тражилаца азила више користи високе технологије у процесу миграција у односу на ирегуларне мигранте. Оно што је заједничко за обе популације јесте чињеница да је коришћење рачунара/мобилног телефона у већој мери коришћено за комуникацију са другим мигрантима или кријумчарима него за самостално путовање. Такође, степен употребе високих технологија зависи од демографских и социоекономских карактеристика испитаника, те мушкарци, лица са вишим степеном образовања и они који говоре неки од страних језика више користе високе технологије у процесу ирегуларне миграције.

Приметна је значајна веза између ирегуларних миграција и употребе високих технологија и од стране испитаника запослених у државним и невладиним организацијама, међу којима су и припадници полицијских установа широм Србије и припадници граничне полиције, стечено кроз оперативна искуства. Међутим, како би исти могли да делују превентивно, потребна је много боља техничка опремљеност њихових јединица. Транснационални карактер ирегуларних миграција, те висок удео секундарних кретања у структури токова тражилаца азила према територијалном пореклу, намећу потребу за даљом и бољом међународном сарадњом по питању ирегуларних миграција.

ЛИТЕРАТУРА

1. Bilger V. M. Hofmann, M. Jandl (2006), Human Smuggling as a Transnational Service Industry: Evidence from Austria, International Migration, 44 (4), 59-93.
2. Borkert M. P. Cingolani, V. Premazzi (2009), Study on 'The State of the Art of Research in the EU on the Uptake and Use of ICT by Immigrants and Ethnic Minorities (IEM)' IMISCOE Working Paper No. 27, 1-68.
3. Bruggeman W. (2002), Illegal Immigration and Trafficking in Human Beings Seen as a Security Problem for Europe
4. Drbohlav D., P. Stych, D. Dzurov (2013), Smuggled Versus Not Smuggled Across the Czech Border, International Migration Review, 47(1), 207–238.
5. European Commission, Clandestino project, 2009, Policy brief: Size and Development of Irregular Migration to the EU, 1-8.
6. European Commission, Clandestino Project, Final report, (2009), 1-190.
7. European Commission, Home affairs, Global Approach to Migration and Mobility,
8. European Migration Network, Practical Measures to Reduce Irregular Migration, 2012, 1-69.
9. Eurostat, The number of asylum applicants registered in the EU27, 2011. http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/3-23032012-AP/EN/3-23032012-AP-EN.PDF (12.10.2013)
10. Frontex, Annual Risk Analysis, 2013, 1-84.
11. Frontex, Europol, 2007 Determination of High Risk Routes Regarding Illegal Migration in the Western Balkan Countries, 1-24.
12. Futo P. M. Jandl, L. Karasakova (2005), Illegal Migration and Human Smuggling in Central and Eastern Europe, Migracijske i etničke teme, 21 (1-2), 35–54.
13. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-studies/irregular-migration/00a_emn_synthesis_report_irregular_migration_october_2012_en.pdf. (14.12.2013)
14. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/international-affairs/global-approach-to-migration/index_en.htm (11.11.2013)
15. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf. (9.11.2013).
16. http://irregular-migration.net/ (12.12.2013)
17. http://picum.org/en/publications/reports/25189 (13.10.2013)
18. http://www.bing.com/search?q=Clandestino+project,+2009,+Policy+brief%3A+Size+and+Development+of+Irregular+Migration+to+the+EU%3A+7&src=IE-TopResult&FORM=IE11TR&conversationid= (24.11.2013)
19. http://www.bing.com/search?q=Frontex,+Europol,+2007+Determination+of+High+Risk+Routes+Regarding+Illegal+Migration+in+the+Western+Balkan+Countries&src=IE-TopResult&FORM=IE11TR&conversationid= (26.12.2013)
20. http://www.brookings.edu/~/media/research/files/papers/2008/3/14%20migration%20koser/0314_migration_koser (18.12.2013)
21. http://www.ce-review.org/01/4/pozun4.html (10.12.2013).
22. http://www.emnbelgium.be/publication/clandestino-project-final-report (6.10.2013).
23. http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDMQFjAB&url=http%3A%2F%2Fwww.kirs.gov.rs%2Fdocs%2Fmigracije%2FMigracioni_profil_Republike_Srbije_za_2012.pdf&ei=qhrsUsLDJMKjtAak_YHwBA&usg=AFQjCNFWyt7JvwZfh8QEXc_E4OjqfussKA&sig2=AaeP02V_uotKeWFFIleJhg (29.10.2013)
24. http://www.iehei.org/bibliotheque/ imigration.htm. (5.11.2013)
25. http://www.ilo.org/public/portugue/region/eurpro/lisbon/pdf/rep-vi.pdf (16.12.2013)
26. http://www.imiscoe.org/images/documents/wp27.pdf (7.10.2013)
27. http://www.unhcr.org/3e19aa494.pdf (23.11.2013)

28. Hysmans J. (2006), The Politics of Insecurity. Fear, Migration and Asylum in the EU, London, Routledge.
29. International Labour Organisation (2004), Towards a fair deal for migrant workers in the global economy, Report VI, International Labour Conference, 92nd Session, International Labour Office, Geneva.
30. Jandl M. (2004), Research Note ''The Relationship between Human Smuggling and the Asylum System in Austria.'' Journal of Ethnic and Migration Studies, 30 (4), 799–806.
31. Jandl M. (2007), Irregular Migration, Human Smuggling, and the Eastern Enlargement of the European Union, International Migration Review, 41 (2), 291–315.
32. Kaizen J. W. Nonneman (2007), Irregular Migration in Belgium and Organized Crime: An Overview, *International Migration,* 45 (2), 121-146.
33. Koser K. (2008), Dimensions and Dynamics of Contemporary International Migration Paper prepared for the conference on 'Workers without borders: Rethinking economic migration', Maastricht Graduate School of Governance.
34. Kraler A., M. Rogoz (2011), Irregular migration in the European Union since the turn of the millennium –development, economic background and discussion, Database on Irregular Migration, Working paper 11/2011.
35. Lukić V. V. Nikitović (2004), Refugees from Bosnia and Herzegovina in Serbia: A Study of Refugee Selectivity, International Migration, 42 (4), 85-110.
36. Mavris L. (2002), Human smugglers and social networks: transit migration through the states of former Yugoslavia - Working Paper, New issues in refugee research, no. 72, UNHCR, 1-14.
37. Munck R. (2008), Globalisation, Governance and Migration: an introduction, Third World Quarterly, 29 (7), 1227–1246.
38. Nikitović V. V. Lukić (2010), Could Refugees Have a Significant Impact on the Future Demographic Change of Serbia?, International Migration, 48 (1),106-128.
39. Picum, Picum's Main Concerns about the Fundamental Rights of Undocumented Migrants in Europe, 2010, 1-84.
40. Požun B. J. (2001), "Just passing through: illegal immigrants find new back door to Europe in Slovenia," Central Europe Review, 3 (4).
41. Szczepanikova A. (2012), Between Control and Assistance: The Problem of European Accommodation Centres for Asylum Seekers, International Migration, 51 (4),130-143.
42. UN, Trends in International Migrant Stock: The 2013 Revision, Press release, http://esa.un.org/unmigration/wallchart2013.htm (11.09.2013)
43. Vogel D., V. Kovacheva, H. Prescott (2011), The Size of the Irregular Migrant Population in the European Union – Counting the Uncountable?, International Migration, 49 (5), 78-96.
44. Влада Републике Србије, (2013), Миграциони профил Републике Србије за 2012. годину, 1-85.
45. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.
46. Закон о заштити државне границе, Службени гласник Републике Србије, бр. 97/08.
47. Закон о потврђивању Конвенције Уједињених нација против транснационалног организованог криминала и допунских протокола, Службени лист СРЈ — Међународни уговори", број 6/01.
48. Закон о потврђивању Споразума између Републике Србије и Европске заједнице о реадмисији лица која незаконито бораве, Службени гласник Републике Србије, бр. 103/07.
49. Лукић В. Д. Матијевић (2003), Миграције и глобализација, Зборник са скупа "Регионални развој и демографски токови балканских земаља", Књ. 8, Економски факултет Универзитета у Нишу, Ниш, 223-229.
50. Лукич В. (2013), Миграционные тенденции в Сербии, 277-286, Сербские научные исследования 2012. Сборник научных статей. – М.: Экон-информ, Москва, составитель А.Н. Новик с. 1-481.
51. Мијаилковић С. М. Жарковић (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд.

52. Стратегија борбе против трговине људима у Републици Србији, Службени гласник Републике Србије, бр. 111/06.
53. Стратегија интегрисаног управљања границом у Републици Србији, Службени гласник Републике Србије, бр. 11/06.
54. Стратегија супростављања илегалним миграцијама у Републици Србији за период 2009–2014. године, Службени гласник Републике Србије, бр. 25/09.
55. Уредба о ближем уређивању начина вршења полицијских овлашћења полицијских службеника граничне полиције и дужностима лица које прелази државну границу, Службени гласник Републике Србије, бр. 39/2011.

Ана Батрићевић
Институт за криминолошка и социолошка истраживања

ЗЛОУПОТРЕБА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА У СВРХУ ТРГОВИНЕ ЉУДИМА – ПОДАЦИ О ЖРТВАМА –

Садржај

1. УВОД

Трговина људима, а посебно женама и децом, представља глобални феномен, који у истој мери погађа земље које се налазе у такозваном пост-конфликтном периоду, односно периоду економске и друштвене транзиције, као и индустријски развијене земље. Као и све друге активности, које су испреплетане са организованим криминалом, трговина људима по правилу није ограничена на територију само једне земље, већ најчешће има транснационални карактер[785]. Не постоје поуздани и свеобухватни подаци о размерама проблема трговине људима, али процене које дају међународне организације и неке националне агенције могу послужити као добар показатељ. Према проценама Уједињених нација, 700.000 деце, жена и мушкараца сваке године постају жртве трговине људима. Амерички Стејт Департмент ову бројку процењује на 900.000, од чега је 20.000 жртава експлоатисано на територији САД-а. У Извештају Међународне организације рада за 2005. годину наводи се да је 2,45 милиона људи у сваком тренутку само радно експлоатисано. Уницеф процењује да 1,2 милиона деце сваке године постану жртве трговине људима. Такође, трговина људима се сматра једном од три најпрофитабилније криминалне активности, уз трговину дрогом и илегалну трговину оружјем. О њој се најчешће говори као о високо профитабилном и ниско ризичном криминалу, јер се процењује да се зараде трговаца људима крећу у распону од неколико милијарди до 60 или чак 500 милијарди долара годишње, а статистички посматрано, веома мали број њих заврши на суду и буде осуђено на високе затворске казне.[786]

Трговина људима је вишеслојан, комплексан и динамичан социјални феномен који захтева свеобухватни (правни и друштвени) приступ, односно примену ефикасних мера на плану превенције, сузбијања, кажњавања учинилаца и заштите жртава, уз обавезну међусобну сарадњу држава. Трговина људима дефинисана је у члану 4 Конвенције Савета Европе о борби против трговине људима[787], односно у члану 3 Протокола за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојеног у Палерму, децембра 2000. године[788]. У складу са овим међународним документима, трговина људима значи вербовање, превоз, премештање, скривање или прихват лица, уз примену претње или силе или других облика принуде, отмице, преваре, обмане, злоупотребе овлашћења или стања угрожености, или давање или примање новчаних средстава или друге користи ради добијања пристанка лица које има

---

785 Видети: Јовашевић, Д. Батрићевић, А. (2013), Organized Crime As a Threat to Security Systems – Serbian Experience, *Studia Securitatis (Security Studies),* 7 (2), стр. 86-102;

786 Анђелковић, М. Бешировић, В. Вукасовић, Т. Глигорић, М. Николић, Д. Оташевић, О. Радовић, И. Wijers, М. (2011), Трговина људима у Републици Србији, Извештај за период 2000–2010, АСТРА – Акција против трговине људима, Београд, стр. 48;

787 Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009;

788 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001;

контролу над другим лицем у циљу експлоатације.[789] Експлоатација обухвата, као минимум, експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа.[790] Пристанак жртве трговине људским бићима на намеравану експлоатацију је без значаја у случајевима у којима је коришћена било која наведених мера. Врбовање, превожење, пребацивање, скривање или примање детета за сврхе експлоатације сматра се "трговином људским бићима" чак и ако не обухвата било које од набројаних средстава.

2. ВИДОВИ И ОБЛИЦИ ТРГОВИНЕ ЉУДИМА

У теорији се разликује неколико облика и видова трговине људима. Ова подела је условна и има само теоријски значај будући да у пракси појавни облици трговине људима нису увек тако строго издиференцирани. Честа је појава да се поједини облици и видови трговине људима преклапају, те да једна иста жртва буде истовремено подвргнута различитим видовима трговине људима. Као критеријуми за класификацију облика трговине људима, могу се јавити: степен друштвене опасности, просторни критеријум, биофизиолошке одлике жртве, став жртве према сопственом положају и облик експлоатације жртве.

Према *степену друштвене опасности* коју представљају, могу се разликовати обичајна трговина људима и криминална трговина људима. Случајеви обичајне трговине људима (традиционалне, „неправе“) немају за циљ никакву експлоатацију лица, већ су део веровања и обичаја народа. Такви обичаји, који су заправо рудиментирани облици трговине људима, индикатор су положаја жене у традиционалним и патријархалним друштвима. Криминална трговина људима обухвата све остале облике, изражене на националном и међународном нивоу. Њихово основно обележје је противправност, односно правна забрањеност. Манифестују се кроз следеће облике: обичајно–криминалне, који представљају комбинацију обичајних и криминалних облика трговине људима, појединачне, које одликује свесна и намерна „купопродаја“ лица, с циљем стицања противправног профита: „продавца“ од продаје лица, „купца“ од накнадне експлоатације, које одликује висок степен организованости, континуираност криминалне делатности, масовност трговаца и жртава, мултиманифестност експлоатације жртава и висок степен друштвене опасности.

Према *просторном критеријуму*, трговина људима се може реализовати на националном *(унутрашња трговина)* и на међународном нивоу. Трговина људима *на националном нивоу* подразумева да жртве у процесу трговине не прелазе државну границу своје земље, при чему извршиоци, укључени у криминалну активност, могу

789 Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009. члан 4 и Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001. члан 3;

790 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала *усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001;*

бити држављани више држава. Овај облик трговине људима може се одвијати на *локалном*, *регионалном* и на тзв. *централном националном нивоу*. Посебан облик прекограничне трговине људима је тзв. једнодневна или викенд трговина људима (*„one – day“* или *„weekend“ trafficking*), при чему се најчешће жене или деца, периодично транспортују преко државне границе ради њихове једнодневне или викенд сексуалне експлоатације, а потом враћају у земљу порекла, односно привремене дестинације.

Према *биофизиолошким одликама жртава* (пол и узраст), трговина људима се може манифестовати као *трговина мушкарцима*, *трговина женама* и *трговина децом* (мушког и женског пола). Ову класификацију, зависно од конкретних законских решења неких земаља, допуњује и критеријум животног (старосног) доба лица. Тако је могуће разликовати бебе, децу, одрасла лица, односно различите категорије лица са одређеним годинама живота.[791] Трговина мушкарцима, иако препозната од стране већине стручњака који изучавају ову проблематику, још увек се налази на маргини истраживачког и друштвеног интересовања. Управо је последица таквог занемаривња постојање мало систематичних података о карактеристикама, природи и распрострањености трговине мушкарцима, али и постојање тешкоћа везаних за идентификовање жртава и разумевање потреба жртава мушког пола[792]. Међународна организација за миграције, на основу 9376 регистрованих жртава унутрашње (34%) и међународне (66%) трговине људима, на крају 2006. године процењује да су мушкарци жртве у 18%, док жене чине 82% идентификованих жртава. У поменутом извештају, а на основу података Међународне организације рада и Уницефа, наводи се да 2% оних који су идентификовани као жртве трговине у циљу комерцијалне сексуалне експлоатације управо јесу мушкарци и дечаци, али се упозорава да је тај удео много већи.[793] Трговина мушкарцима присутна је и у Србији. У случајевима трговине пунолетним мушкарцима доминира трговина у циљу радне експлоатације. Са друге стране, у случајевима трговине дечацима, примарно место заузима трговина у циљу просјачења, затим, трговина у циљу вршења кривичних дела, па трговина у циљу сексуалне експлоатације и трговина у циљу радне експлоатације.[794] Ипак, највећи број расположивих података у свету и код нас се односи на трговину женама ради сексуалне експлоатације, јер је овај облик најчешћи и најуочљивији.[795]

С обзиром *на лични однос и став жртве према положају у којем се налази*, постоје тзв. добровољна и присилна трговина људима. *Добровољна* трговина људима подразумева сагласност (одобравање) жртве да буде објект трговине, односно експлоатације. Од тога треба разликовати случајеве у којима су лица преваром и обманом, да ће се бавити неким послом или проституцијом, доведена у

791 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 78;

792 Николић-Ристановић, В. (2009), Трговина мушкарцима у Србији, Виктимолошко друштво Србије, Београд, стр. 19;

793 Николић-Ристановић, В. (2009), Трговина мушкарцима у Србији, Виктимолошко друштво Србије, Београд, стр. 20-21;

794 Николић-Ристановић, В. (2009), Трговина мушкарцима у Србији, Виктимолошко друштво Србије, Београд, стр. 75-76;

795 Николић-Ристановић, В. Ћопић, С. Миливојевић, С. Симеуновић-Патић, Б. Михић, Б. (2004), Трговина људима у Србији, Виктимолошко друштво Србије, Организација за европску безбедност и сарадњу, Београд, стр. 25;

ропски положај и експлоатисана. *Присилна* трговина људима подразумева одсуство сагласности жртве да буде предмет трговине и експлоатације, односно употребу разних облика принуде и преваре према жртви. Добровољност жртве може да значи да у конкретном случају није реч о трговини људима, већ о неком другом кривичном делу (нпр. о посредовању у проституцији). С друге стране, то је понекад индикатор да су код жртве наступили извесни душевни поремећаји, те је равнодушна услед непостојања свести о томе шта јој се догађа.

С обзиром на *вид експлоатације којем је жртва изложена*, трговина људима се може манифестовати у више облика, и то као: сексуално ропство, радно ропство, илегално усвојење, принудни брак, одузимање људских органа или делова тела, принудно вршење криминалних радњи, принудно учешће у оружаним сукобима и као „препродаја људи“ без излагања другим видовима експлоатације од стране „препродавца“. О појединим облицима експлоатације биће речи приликом излагања о фази експлоатације, као најважнијој, кључној фази трговине људима.

3. ФАЗЕ ТРГОВИНЕ ЉУДИМА

Фазе трговине људима могу укључивати:

- фазу порекла,
- фазу транзита,
- фазу дестинације и
- фазу елиминације.

Фаза порекла је прва фаза кријумчарења мигранта и трговине људима која се одвија на међународном нивоу. Одвија се у земљи порекла и неретко је одликује деловање организоване криминалне групе са адекватном структуром, стварање злочиначког плана и регрутовање мигранта, односно жртава трговине људима.[796] Регрутовање жртава трговине људима обухвата скуп метода, поступака и средстава чијом се појединачном или комбинованом применом неко лице „увлачи“ у мрежу кријумчарења или трговине људима.[797] Врбовање је појава чији су обим и садржај ужи од појма регрутовање и његова је поткатегорија. То је акт придобијања сагласности, воље потенцијалне жртве са легендираном понудом регрутера и манифестује се као обмана жртве апсолутним неистинама или полуистинама. Гледано кроз кривичноправну призму „врбовање подразумева наговарање неког лица да предузме неке делатности, односно да се стави у одређени положај и овај облик радње се најчешће може односити на вршење криминалних активности, проституцију, просјачење и друго.[798]

У последње време је све присутније врбовање жртава преко *интернета* (тзв. *кибертрафикинг*), сервирањем лажних понуда за запослење, лажним представљањем, злоупотребом интернет-причаоница (*chat rooms*) у којима

796 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 81;

797 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 86;

798 Лазаревић, Љ. (2011), *Коментар Кривичног законика Републике Србије*, Савремена администрација, Београд, стр. 1123;

потенцијалне жртве дају податке о себи и подлежу понудама регрутера. Осим тога, интернет је корисно средство комуникације између трговаца људима, односно трговаца људима и потенцијалних конзумената услуга жртава трговине људима, као и за рекламирање таквих активности, односно за растурање порнографског материјала насталог експлоатацијом жртава.[799]

Начини, средства и методе које трговци људима користе за вербовање жртава трговине људима као и за одржавање контаката са њима и спровођење контроле над њима током трајања периода експлоатације су бројни и међусобно веома различити. Захваљујући брзом развоју и ширењу различитих информационо-комуникационих технологија, све је чешћа употреба односно злоупотреба интернета, посебно друштвених мрежа и специјализованих сајтова за огласе, у сврху вербовања и одржавања контаката са жртвама трговине људима.

Употреба интернета се шири великом брзином, и познато је да се овај облик информационо-комуникационих технологија у свету користи како за вербовање жртава трговине људима тако и за рекламирање услуга које оне пружају. Такође је распрострањена појава да се састанци између жртава трговине људима и њихових клијената, односно лица која користе њихове услуге, организују преко специјализованих веб-сајтова[800]. Примећено је да је велики број жртава трговине људима регрутован у земљама свог порекла управо захваљујући томе што су се јавиле на лажне огласе за запошљавање. Констатовано је да у свету трговци људима све више користе интернет и друге електронске медије да на тај начин регрутују и вербују жртве.[801] Такође, у намери да избегну откривање, трговци људима често пребацују жртве у друге земље и користе анонимност интернета као дискретан метод за регрутовање нових жртава[802]. Све наведено показује да се информационо-комуникационе технологије и у случају трговине људима користе не само за вербовање и за одржавање контакта са њима већ и за њихово илегално пребацивање на територије других земаља, што се сматра илегалним миграцијама.

Фаза транзита жртава трговине људима је друга фаза у процесу трговине људима и подразумева транспортовање жртава до места њихове дестинације, а када је реч о међународној трговини људима одвија се у тзв. земљама порекла, транзита и/или земљама дестинације жртава и обухвата планирање и организовање транспорта и логистичке подршке, транспортовање лица и прелажење државне границе. Ова фаза може да подразумева не само

799 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 88;

800 Trafficking in Human Beings in the European Union, OC Networks in the South-East European Sphere, Analysis and Knowledge, The Hague, 1 September 2011, https://www.europol.europa.eu/sites/default/files/publications/trafficking_in_human_beings_in_the_european_union_2011.pdf, 01.11.2013;

801 Situational Overview on Trafficking in Human Beings, European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Warsaw, June 2011, http://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Situational_Overview_on_Trafficking_in_Human_Beings.pdf, 01.11.2013;

802 Strategic Project on Eurojust's action against trafficking in human beings, Final report and action plan, The European Union's Judicial Cooperation Unit (EUROJUST), October, 2012, http://eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Eurojust%20action%20against%20trafficking%20in%20human%20beings%20%28October%202012%29/THB-report-2012-10-18-EN.pdf, 01.11.2013;

пребацивање са једног места на друго, већ и скривање жртве и озбиљно кршење људских права (кроз нехумане услове транспорта и сакривања, физичко и психичко злостављање).[803]

Фаза дестинације је трећа фаза кријумчарења мигранта и трговине људима која се одвија у земљи дестинације. Судбина прокријумчарених мигранта и жртава трговине људима у овој фази је различита. Над *жртвама трговине људима* заснива се ропски однос и оне су сурово експлоатисане. Смештају их у одређене објекте из којих не могу својевољно да оду (високе ограде, постављене камере, физичко обезбеђење и слично) или их контролишу на други начин. Жртве тзв. добровољне трговине људима добијају фалсификоване идентификационе исправе (путне исправе, личне карте, пријаве боравка и слично) или задржавају лична документа и укључују се у процес експлоатације.[804]

Као што је истакнуто, експлоатација обухвата, као минимум, експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа. Експлоатација жртава је кључни моменат трговине људима: то је основно средство за остваривање енормно високог противправног профита, што је и њен главни узрок. Операционализацијом датих дефиниција и уважавањем видова и облика намераване, односно извршене експлоатација који њима нису предвиђени, могу се идентификовати следећи *доминантни видови експлоатације жртава трговине људима*: продаја жртве другом лицу, тзв. „препродаја људи"; радна експлоатација; сексуална експлоатација; илегално усвојење деце; принудно склапање бракова; трговина људским органима или деловима тела; принудно учешће у оружаним сукобима; принудно вршење одређњних криминалних радњи и остали, неспецифични облици експлоатације.[805]

Продаја жртава другоме, односно „препродаја људи" је доминантни вид експлоатације жртава. Наиме, жртву може да експлоатише појединац или криминална група која ју је регрутовала, али она може да буде продата другом лицу или групи који ће је даље експлоатисати. У другом случају, даља продаја жртве представља облик њене експлоатације, односно зараду трговаца људима на разлици прихода од продаје жртве и трошкова њеног регрутовања, транспортовања и издржавања.[806] Осим тога, жртва може да буде продата и пошто је неко време била експлоатисана. Због тога се овај вид експлоатације назива трговина људима у ужем смислу, јер представља „трговину ради даље трговине".[807]

Сексуална експлоатација (*sex trafficking*) је најзаступљенији облик експлоатације жртава трговине људима. То је експлоатација њиховог тела, полног и сексуалног идентитета и интегритета. Реч је о виду експлоатације жртава оба пола,

---

803 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 91;

804 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 92-93;

805 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 153-154;

806 Голубовић, С. и Голубовић, Н. (2011), Примена теорије рационалног избора у анализи трговине људима, *Наука, безбедност, полиција,* 16 (2), стр. 87–100;

807 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 97;

различитог узрасног доба, који се манифестује као некомерецијална и комерцијална сексуална експлоатација. Некомерцијална је сексуална експлоатација жртава трговине људима од стране лица које их је „купило“ ради задовољења личних или/и сексуалних прохтева њему блиских лица, без намере да таквом експлоатацијом остварује противправни приход. Комерцијална је сексуална експлоатација жртава трговине људима ради задовољења сексуалних прохтева, нагонских и патолошких потреба неодређеног броја „власнику“ познатих и непознатих лица, при чему се остварује извесна противправна корист. Принудна проституција је један од најзаступљенијих појавних облика експлоатације жртава трговине људима.[808] Под проституцијом се подразумева сексуални однос који карактерише плаћање (најчешће у новцу), екстреман промискуитет и емоционална равнодушност према партнеру и самом сексуалном чину. Битне одлике проституције су: повезивање сваког сексуалног односа са новцем или каквом другом користи; екстреман сексуални промискуитет, односно везаност за велики број различитих, али и непознатих партнера и емотивна равнодушност не само према сексуалном задовољству већ и према партнеру.[809]

Пороногрфија се одређује као приказ еротског понашања (у виду визуелних садржаја или у писаној форми) који има за циљ изазивање сексуалног узбуђења. При овом виду експлоатације *принудне* сексуалне активности у којима жртва учествује бележе се у аудио-визуелном облику (фотографија или тонфилмско снимање), а потом репродукују или дистрибуирају[810]. Други облик подразумева принуду жртве на извођење представа са порнографским садржајем.

Радна експлоатација је тип експлоатације који подразумева принудни рад жртве. Принудни рад је дефинисан Конвенцијом број 29 о присилном раду Међународне организације рада из 1930. године[811] и Конвенцијом број 105 о укидању принудног рада из 1957. године. Принудни рад се односи на било који рад или службу који су изнуђени од стране неког лица под претњом било какве казне и за које се то лице није добровољно пријавило. Услови принудног рада укључују употребу физичког или сексуалног насиља, претњу насиљем, дужничко ропство, обустављање исплате примања или неплаћање, ограничење слободе кретања, задржавање пасоша и личних исправа и претњу пријавом властима. Радна експлоатација може укључивати: експлоатацију у пољопривредном сектору и шумарству, експлоатацију у индустријском сектору, експлоатацију у услужном сектору, експлоатацију у домаћинству (тзв. кућно ропство) и комбиновану експлоатацију.[812]

---

808 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 158-159;

809 Јефтовић, М. и Милашиновић, С. (2002), *Самоугрожавање друштва – социјално-патолошке девијације*, Синекс, Београд, стр. 143;

810 Упоредити: Батрићевић, А. (2008), Грађанско-правна одговорност због повреде права на сопствену слику, Бранич, 121 (1-2), стр. 117-127;

811 Convention (No. 29) concerning Forced Labor, Adopted on 28 June 1930 by the General Conference of the International Labor Organization at its 14th session, at: Human Rights - A Compilation of International Instruments Volume I, Universal Instruments, United Nations, New York and Geneva, 1994;

812 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 156-157;

Принуда на закључење брака је тип експлоатације при коме се жртва експлоатише улогом брачног партнера у браку који је склопљен принудно. У оваквим ситуацијама жртва се експлоатише кроз наметнуту улогу брачног друга – супружника, јер брак није закључен сагласном изјавом воља обе особе, већ само једне. Може имати следеће облике: с обзиром на пол брачних партнера - принудни хетеросексуални брак и принудни хомосексуални брак; с обзиром на пол и узраст жртве - принудни брак са женом, принудни брак са дететом, принуђени дечји брак, принудни брак са мушкарцем; с обзиром на број жртава које су експлоатисане - принудни моногамни брак, принудни полигамни брак, принудни моноандни или полиандни брак.[813]

Принудно вршење криминалних радњи је још један вид експлоатације. Према степену друштвене опасности ових незаконитих радњи, може се разликовати принудно вршење прекршаја и принудно вршење кривичних дела.[814] Принуда на вршење кривичних дела је тип експлоатације при коме се жртве приморавају на вршење одређених противправних радњи, а са циљем прибављања противправне имовинске користи за лице које примењује принуду. Таква је нпр. принуда на просјачење. Просјачење је дефинисано 2004. године, када је Међународна организација рада усвојила дефиницију просјачења које се утврђује као „низ активности којима појединац тражи новац од непознате особе, а на основу свог сиромаштва или у потрази за добротворним донацијама, позивајући се на здравствене или верске разлоге. Просјаци исто тако могу продавати мање предмете, као што су крпе за чишћење или цвеће, заузврат тражећи новац чији износ није утемељен вредношћу предмета који се продаје.“[815] Принуда на просјачење представља облик принуде на вршење прекршаја. Просјачење може бити индивдуално или у оквиру организоване мреже за просјачење, на локацијама са великом фреквенцијом људи.[816] Принудно учешће у оружаним сукобима подразумева да се жртве приморавају да непосредно или посредно учествују у ратним, терористичким, диверзантским, герилским и сличним акцијама.[817]

Принуда подразумева навођење неког лица силом или претњом да нешто учини, не учини или да трпи. Сила подразумева употребу физичке, механичке или друге снаге са циљем сламања отпора неког лица, као и примену хипнозе или омамљујућих средстава како би се оно довело у несвесно стање и принудило на одређено понашање. Сила може бити примењена као апсолутна или компулзивна, посредно или непосредно, али у интензитету који је подобан да утиче на вољу пасивног субјекта. Претња је зло које се ставља у изглед пасивном субјекту или њему блиском лицу ако не поступе по захтеву лица које врши принуду.[818] Заблуда је

813 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 167;

814 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 172;

815 Save the Children (2011), Регионални извјештај о просјачењу дјеце, распрострањеност, превенција и сузбијање дјечјег просјачења, Save the Children, Сарајево, стр. 12;

816 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 172;

817 Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 173;

818 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 518;

непостојање представе о некој околности или постојање погрешне или непотпуне представе о некој околности.[819] Довођење у заблуду је стварање погрешне или непотпуне представе код другог лица. Та се радња може извршити на два начина: лажним приказивањем чињеница и прикривањем чињеница. Лажно приказивање је тврђење да постоји нека чињеница која у стварности не постоји и обрнуто. Прикривање чињеница је прећуткивање чињеница од лица које је дужно да их саопшти или стварње неке ситуације да неко лице не може само да сазна за одређене чињенице. Одржавање у заблуди је активна радња, активно одржавање погрешне или непотпуне представе код другог лица која код њега већ постоји. [820]

Трговина децом ради усвојења је вид експлоатације који се успоставља над дететом и може се манифестовати као неправо и право. Неправо експлоатисање илегалним усвојењем детета постоји у случајевима када је усвојење извршено на незаконит начин, након чега дете живи са новим родитељима без икаквих додатних облика експлоатације. Сам положај жртве, због начина на који је у њега доведена, сматра се експлоатацијом. Право експлоатисање илегално усвојеног детета постоји у случајевима када је, поред тога што је неправо усвојено, дете и додатно експлоатисано другим видовима и облицима: сексуално, радно, приморавањем на вршење одређених криминалних радњи или трговином људима у ужем смислу.

Трговина органима или *одузимање људских органа и делова тела* је вид експлоатације где су жртве експлоатисане на тај начин што им је узет орган из организма, или део тела. У овом случају може постојати неколико облика експлоатације. С обзиром на врсту људског ткива које се узима: узимање људских органа и узимање делова људских тела; у односу на то да ли постоји сагласност даваоца органа, односно дела тела: добровољно давање људских органа или делова тела и насилно узимање људских органа или делова тела; с обзиром на то да ли је лице од кога се орган узима живо или не: узимање органа или делова тела од живог лица, узимање органа или делова тела од „свеже умрлог" лица и узимање органа или делова тела од давно мртвог лица; с обзиром на циљ, односно сврху одузимања органа или дела тела: узимање органа или делова тела ради задовољења здравствених потреба лица и узимање органа или делова тела у научно–истраживачке сврхе.[821]

4. ЖРТВЕ ТРГОВИНЕ ЉУДИМА И ТРГОВЦИ ЉУДИМА

Појам жртве најшире је одређен у Декларацији о основним принципима правде за жртве злочина и злоупотребе власти из 1985. године. Према овом међународном документу, *жртва је лице које је појединачно или колективно претрпело штету, укључујући физичко или ментално повређивање, емотивну патњу, материјални губитак или груб напад на своја основна права, услед чињења или нечињења која представљају кршење кривичних закона држава, што се односи и на законе који забрањују злоупотребу власти.* Жртвом се може сматрати свако ко

819 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 733;

820 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 502;

821 Мијалковић, С. (2005), Облици и видови трговине људима. *Темида*, 8(1), стр. 41;

испуњава наведене услове, без обзира на то да ли је учинилац дела идентификован или није, да ли је ухапшен, да ли се против њега води судски поступак, да ли је проглашен кривим и без обзира на степен његовог сродства са жртвом. Термин „жртва“ обухвата по потреби и блиску породицу и лица која жртва директно издржава, као и лица која су претрпела штету помажући жртвама које су се нашле у невољи.[822] Жртве трговине људима, али и њима блиска лица потпадају под овако дефинисан појам жртве.[823] Према Стратегији борбе против трговине људима у Републици Србији, жртва трговине људима је свако физичко лице подвргнуто трговини људима.[824]

Као што је истакнуто, жртве трговине људима могу бити лица оба пола, с тим што постојећа истраживања показују да су међу њима ипак знатно заступљеније жене. Идентификоване су три групе фактора које утичу на виктимизацију жена на једној страни и вршење кривичног дела од стране како мушкараца тако и жена, на другој страни. Као макросоцијални фактори наводе се: тржиште и ратна економија, експанзија секс-индустрије, економске промене у свакодневном животу људи и промене везане за рат, повећавање разлика између богатих и сиромашних земаља и повећано присуство војске. Од психолошких и психосоцијалних фактора се истичу: повећана изложеност жена виктимизацији услед психолошког стања изазваног насиљем у породици и сексуалним насиљем, бескућништво, породични проблеми, миграције изазване ратом, економски и слични проблеми, ниско самопоштовање, незапосленост, друштвена изолованост и маргинализованост, наркоманија, затим, незапосленост и сиромаштво као фактори који утичу на укључивање мушкараца и жена у ланац трговине људима на страни извршилаца и њихових помагача, као и културни фактори и родна социјализација.[825]

Трговци људима су сва лица која су укључена у процес трговања људима (учествују у врбовању жртава, њиховом спровођењу, превожењу, чувању, обезбеђењу смештаја, контролисању или експлоатацији).[826] То су особе које су регрутовањем (врбовањем), спровођењем, превожењем, чувањем, обезбеђењем смештаја, контролисањем или експлоатицијом људи укључене у процес трговања њима. Према дефиницији Уједињених нација, сви трафикери се могу класификовати као регрутери или врбовници (*recruiters)*, превозници (*transporters*), контролори жртава (*controlers*), они који врше трансфер и/или одржавају лица у експлоататорском положају, они који су умешани у криминал у вези с тим и они који профитирају од трговине људима, од појединих њених облика или сродних прекршаја[827], било директно било индиректно, Кријумчари људи су особе које

822 *Декларација о основним принципима правде за жртве злочина и злоупотребе власти*, усвојена Резолуцијом Генералне скупштине Уједињених нација број 40/34 од 29. новембра 1985. године.

823 Упоредити:Батрићевић, А. (2013), Еколошка кривична дела – злочини без жртве?, *Темида,* 16 (1), стр. 113-132.

824 Стратегија борбе против трговине људима у Републици Србији, „Службени гласник РС“, бр. 111/2006.

825 Николић Ристановић, В., Ћопић, С., Миливојевић, С., Симеуновић-Патић, Б., Михић, Б. (2004), Трговина људима у Србији, Виктимолошко друштво Србије, Организација за европску безбедност и сарадњу, Београд, стр. 29-30.

826 Мијалковић, С., Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 133.

827 Смерница 2, *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, United Nations High Commisissioner for Human Rights to the Economic and Social Council, E/2002/68/Add.1, New York, 2002;

свесно (из користољубља) другом лицу омогуће неовлашћени прелазак државне границе, као и оне које странцу омогуће неовлашћени транзит или боравак.

5. МЕЂУНАРОДНИ НОРМАТИВНИ ОКВИР ЗА БОРБУ ПРОТИВ ТРГОВИНЕ ЉУДИМА

Нормативни оквир за борбу против трговине људима чине међународни и национални правни акти, који садрже одредбе од директног или индиректног значаја за превенцију, сузбијање и санкционисање трговина људима.

Међународноправни акти који садрже одредбе релевантне за дефинисање кривичних дела трговине људима и кријумчарења миграната јесу: Универзална декларација Уједињених нација о људским правима (1948); Конвенција о спречавању трговине људима и експлоатације проституције других (1949); Конвенција за заштиту људских права и основних слобода (1950); Међународни пакт о грађанским и политичким правима (1966); Конвенција о елиминисању свих облика дискриминације жена (1977); Генерална препорука Комитета за елиминисање дискриминације према женама број 19 (1992); Пекиншка Платформа за акцију IV светске конференције о женама (1995); Хашка министарска декларација о европским смерницама за ефикасне мере у сузбијању трговине женама с циљем сексуалне експлоатације; Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом која допуњава Конвенцију Уједињених нација против транснационалног организованог криминала (2000); Протокол против кријумчарења миграната копном, морем и ваздухом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала (2000); Препорука Савета Европе 1325 о трговини женама и присилној проституцији у државама чланицама Савета Европе; Препорука Комитета министара број R (2000) о акцији против трговине људским бићима у сврху сексуалне експлоатације; Предлог оквирне одлуке Комисије Европске уније о борби против трговине људским бићима бр. 201/0024 (2001).

Регулатива Уједињених нација у погледу заштите људских права жртава трговине људима и кријумчарених миграната: Међународни споразум за успешну заштиту од криминалне трговине познате под именом Трговина белим робљем (1904); Међународна конвенција за сузбијање трговине женама и децом (1921); Конвенција о ропству (1926) са Протоколом (1953); Конвенција о забрани свих облика праксе сличне ропству (1926); Међународна конвенција о сузбијању трговине пунолетним женама (1933); Међународна конвенција о сузбијању трговине белим робљем (1949); Конвенција за сузбијање и укидање трговине лицима и експлоатације проституисања других (1950); Допунска конвенција о укидању ропства, трговине робљем и установа и праксе сличних ропству са Завршним актом (1956); Конвенција о правима детета (1989)[828]; Декларација о елиминацији насиља према женама – DEVAW (1993); Пекиншка Платформа за

828 Упоредити: Батрићевић, А. (2010) Међународни стандарди у превенцији насилничког криминалитета код малолетника, (Ур. Лепосава Крон) *Насилнички криминал:етиологија, феноменологија превенција*, Инситутут за криминолошка и социолошка истраживања, Београд, стр.321-338.

акцију IV светске конференције о женама (1995); Хашка министарска декларација о европским смерницама за ефикасне мере у сузбијању трговине женама с циљем сексуалне експлоатације; Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала (2000); Протокол против кријумчарења миграната копном, морем и ваздухом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала (2000); Правило број 2001/4 о забрани трговине људима на Косову (2001); Факултативни протокол о продаји деце, дечјој проституцији и дечјој порнографији, уз Конвенцију о правима детета (2002); Факултативни протокол о учешћу деце у оружаним сукобима, уз Конвенцију о правима детета (2002); Препорука принципа и смерница о људским правима и трговини људима (2002).

Међународни документи и препоруке Савета Европе (СОЕ): Конвенција о заштити људских права и основних слобода (1950); Европска конвенција о екстрадицији (1957); Европска конвенција о сарадњи у кривичним стварима (1959); Европска социјална повеља (1966); Конвенција о компензацији жртвама насиља (1983); Препорука о положају жртава у кривичном праву и кривичном поступку (1985); Препорука о помоћи жртвама и превенцији виктимизације (1987); Препорука о криминалној политици у Европи (1996); Препорука која се односи на положај сведока у односу на окривљениково право одбране (1997); Препорука о мерама против организатора трговине (1997); План за акцију борбе против насиља над женама (1997); Препорука о акцији против трговине људима ради сексуалне експлоатације (2000); Препорука о сексуалној експлоатацији, порнографији и проституцији и трговини децом и млађим пунолетницима; Препорука Rec (2001)16 о заштити деце од сексуалног експлоатисања; Европски кодекс полицијске етике (2001); Проглас Савета Европе о трговини женама (2002); Конвенција Савета Европе о борби против трговине људима (2005).

Документи Европске уније: Резолуција о експлоатацији проститутки и трговини људским бићима (1989); Резолуција о трговини женама (1993); Резолуција о трговини људским бићима (1996); Оквирна одлука Комисије Министарског савета и Европског парламента о трговини женама, нарочито с циљем сексуалне експлоатације (1996); Резолуција о трговини женама и одговарајућа Оквирна одлука Комисије о трговини женама, посебно с циљем сексуалне експлоатације (1997); Акциони план о спречавању трговине и сексуалне експлоатације деце (1997); Министарска декларација о европским упутствима за ефективне мере на превенцији и спречавању трговине женама с циљем сексуалне експлоатације (1997); Оквирна одлука Комисије Министарског савета и Европског парламента са предлогом даљих акција против трговине женама (1998); Резолуција о трговини женама (2000); Одлука о борби против дечје порнографије на интернету (2000); Оквирна одлука Савета Европске уније о положају жртава у кривичном поступку (2001); Оквирна одлука Савета Европске уније о борби против трговине људима (2002); Оквирна одлука о борби против сексуалне експлоатације деце и дечје порнографије (2003) и друга.

Документи Организације за европску безбедност и сарадњу: Санкт–Петербуршка декларација Парламентарне скупштине ОЕБС–а о трговини женама и

децом (1999); Декларације Парламентарне скупштине ОЕБС–а из Букурешта (2000); Одлука Министарског савета о оснаживању напора ОЕБС–а за борбу против трговине људима (2000); Декларација о трговини људима из Порта (2002).

Документи Пакта за стабилност Југоисточне Европе*:* Министарска Декларација пакта за стабилност Југоисточне Европе о борби против трговине људима (2000).

6. ПРОПИСИ РЕПУБЛИКЕ СРБИЈЕ ОД ЗНАЧАЈА ЗА БОРБУ ПРОТИВ ТРГОВИНЕ ЉУДИМА

Устав Републике Србије, као највиши правни акт, садржи прокламацију којом се изричито забрањују неке од активности које спадају и у тговину људима. Њиме је изричито наглашена *забрана ропства, положаја сличног ропству и принудног рада*: нико не може да буде држан у ропству или у положају сличном ропству;сваки облик трговине људима је забрањен; забрањен је принудни рад. Сексуално или економско искоришћавање лица које је у неповољном положају сматра се принудним радом. Принудним радом се не сматрају рад или служба лица на издржавању казне лишења слободе, ако је њихов рад заснован на принципу добровољности, уз новчану надокнаду, рад или служба лица на војној служби, као ни рад или служба за време ратног или ванредног стања у складу са мерама прописаним приликом проглашења ратног или ванредног стања (члан 26). Поред ових, Устав је преузео и многе одредбе Универзалне декларације о људским правима и других међународних аката од значаја за супротстављање трговини људима. [829]

Осим Устава као највишег правног акта и Кривичног законика и Законика о кривичном поступку, као најважнијих извора кривичног права, за сузбијање трговине људима релевантни су и други правни акти. *Законом о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела*[830] уређује се образовање, организација, надлежност и овлашћења државних органа и посебних организационих јединица државних органа, ради откривања, кривичног гоњења и суђења за кривична дела одређена овим законом. *Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала*[831] уређује се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела из области високотехнолошког криминала. Високотехнолошки криминал представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику (чл. 1 и 2).

829 Устав Републике Србије, Службени гласник РС, бр. 98/2006;

830 Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела, Службени гласник РС, бр. 42/2002, 27/2003, 39 /2003, 67/2003, 29/2004, 45/2005 и 72/2009;

831 Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, број 61/2005 и 104/2009;

Законом о полицији[832] прецизирају се, између осталог, полицијски послови, организација полиције, полицијска овлашћења, контрола рада полиције, облици сарадње са другим субјектима безбедности и овлашћења за доношење подзаконских прописа. Ове одредбе су свакако значајне за дефинисање организације и функције овог субјеката безбедности у супротстављању многим безбедносним проблемима, па и трговини људима и кријумчарењу мигранта.

Законом о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица[833] дефинишу се одредбе које се примењују према малолетним учиниоцима кривичних дела, а односе се на материјално-кривично право, органе који га примењују, кривични поступак и извршење кривичних санкција према овим учиниоцима кривичних дела. За супротстављање трговини људима посебно су значајне одредбе овог закона о заштити деце и малолетника као оштећених у кривичном поступку (члан 1). ЗОМУКД садржи посебне одредбе о заштити деце и малолетника (малолетних лица) као оштећених у кривичном поступку. То значи да се и на малолетне жртве трговине људима примењују посебне одредбе овог закона, систематизоване у оквиру његовог З. дела под насловом „Посебне одредбе о заштити малолетних лица као оштећених у кривичном поступку“. Примена ових одредби има за циљ да се током кривичног поступка, који се води према учиниоцу тог кривичног дела, малолетним жртвама обезбеди посебна, додатна заштита како би се спречила, односно умањила њихова секундарна виктимизација.

Законом о програму заштите учесника у кривичном поступку[834] уређују се услови и поступак за пружање заштите и помоћи лицима која су, услед давања исказа или обавештења без којих би било знатно отежано или онемогућено доказивање у кривичном поступку за дела организованог криминала, изложени опасности по живот, здравље, физички интегритет, слободу или имовину (члан 1). Примена овог закона изузетно је важна за заштиту, помоћ и подршку жртвама, али и за ефикасно сузбијање трговине људима и кријумчарења мигранта засновано на активном учешћу и помоћи жртава.

Република Србија је израдила и *Стратегију борбе против трговине људима*. Овај документ је израђен према Смерницама за националне планове акције Пакта стабилности[835] и у складу са Програмом за израду и реализацију свеобухватног националног одговора на проблем трговине људима и најбоље праксе у региону, припремљеног од стране Међународног центра за развој миграционе политике (*ICMPD*). Стратегија Републике Србије састоји се од низа мера и активности које треба предузети у циљу правовременог и свеобухватног одговора на проблем трговине људима у земљи, са посебним нагласком на заштиту људских права жртава. Израдом Стратегије успостављени су јасни стратешки циљеви који треба да буду реализовани кроз различите активности државних институција, невладиних и међународних организација. Ове активности ће бити посебно представљене и у Националном плану акције за борбу против трговине људима, који ће бити донет по усвајању Стратегије. Стратегија је одраз националне политике наше земље у

832 Закон о полицији, Службени гласник РС, бр. 101/2005, 63/2009 и 92/2011;
833 Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица, Службени гласник РС, бр. 85/2005;
834 Закон о програму заштите учесника у кривичном поступку, Службени гласник *РС*, бр. 85/2005;
835 http://www.stabilitypact.org/trafficking/default.asp, 31.10.2013;

области борбе против трговине људима и првенствено се базира на заштити људских права жртава.[836]

7. ИНКРИМИНАЦИЈА ТРГОВИНЕ ЉУДИМА У КРИВИЧНОМ ПРАВУ РЕПУБЛИКЕ СРБИЈЕ

Трговина људима, као и одређене активности које су повезане са том криминалном активношћу инкриминисане су у оквиру 34. главе Кривичног законика Републике Србије, која је посвећена кривичним делима против човечности и других добара заштићених међународним правом. Као најзначајнија за ову проблематику међу њима се могу издвојити следећа кривична дела: трговина људима (члан 388), трговина малолетним лицима ради усвојења (члан 389) и заснивање ропског односа и превоз лица у ропском односу (члан 390).

Кривично дело трговине људима је дефинисано у члану 388 Кривичног законика Републике Србије[837], као и у Стратегији борбе против трговине људима у Републици Србији[838]. Ово дело чини лице које силом или претњом, довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи, врбује, превози, пребацује, предаје, продаје, купује, посредује у продаји, сакрива или држи друго лице, а у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима, казниће се затвором од 3 до 12 година (члан 388 став 1). За дело из става 1 овог члана, учињено према малолетном лицу, учинилац ће се казнити казном прописаном за то дело и кад није употребио силу, претњу или неки други од наведених начина извршења (члан 388 став 2). Ако је дело из става 1 овог члана учињено према малолетном лицу, учинилац ће се казнити затвором најмање 5 година (члан 388 став 3). Ако је услед дела из ст. 1 и 2 овог члана наступила тешка телесна повреда неког лица, учинилац ће се казнити затвором од 5 до 15 година, а ако је наступила тешка телесна повреда малолетног лица услед дела из става 3 овог члана, учинилац ће се казнити затвором најмање 5 година (члан 388 став 4). Ако је услед дела из ст. 1 и 3 овог члана наступила смрт једног или више лица, учинилац ће се казнити затвором најмање 10 година (члан 388 став 5). Ко се бави вршењем кривичног дела из ст. 1 до 3 овог члана или је дело извршено од стране групе, казниће се затвором најмање пет година (члан 388 став 6). Ако је дело из ст. 1 до 3 овог члана извршено од стране организоване криминалне групе, учинилац ће се казнити затвором најмање 10 година (члан 388 став 7). Ко зна или је могао знати да је лице жртва трговине људима, па искористи њен положај или другоме омогући искоришћавање

836 Стратегија борбе против трговине људима у Републици Србији, Службени гласник РС, бр. 111/2006;

837 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005,72/2009, 111/2009 и 121/2012;

838 Стратегија борбе против трговине људима у Републици Србији, Службени гласник РС, бр. 111/2006;

њеног положаја ради експлоатације предвиђене ставом 1 овог члана, казниће се затвором од 6 месеци до 5 година (члан 388 став 8). Ако је дело из става 8 овог члана учињено према лицу за које је учинилац знао или је могао знати да је малолетно, учинилац ће се казнити казном затвора од 1 до 8 година (члан 388 став 9). Пристанак лица на експлоатацију или на успостављање ропског или њему сличног односа из става 1 овог члана не утиче на постојање кривичног дела из ст. 1, 2 и 6 овог члана (члан 388 став 10).[839]

Радња извршења овог кривичног дела одређена је алтернативно и може обухватати једну или више, у законском тексту, набројаних активности. Радња извршења јесте врбовање, превоз, пребацивање, предаја, продаја, куповина, посредовање у продаји, сакривање или држање другог лица.[840] За постојање овог кривичнох дела, потребно је да радња буде предузета на неки од следећих начина: силом или претњом, довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи. За постојање кривичног дела неопходна је и одређена усмереност. Ради се о циљним делатностима, тј. оне су повезане са постизањем одређеног циља у односу на лице које је предмет трговине, тј. у вези са пасивним субјектом. Потребно је да се те радње чине у циљу експлоатације његовог рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа ради одузимања органа или дела тела или ради коришћења у оружаним сукобима.[841] Пасивни субјект може бити било које лице, али због природе овог кривичног дела најчешће ће се радити о женама и деци. Дело има умишљајни карактер. Спорно је да ли се као посебни субјективни елемент захтева и намера учиниоца која би била управљена на постизање неког од наведених циљева или је реч о томе да је довољно знање извршиоца да ће пасивни субјект бити искоришћен у неку од наведених сврха и то од стране било ког лица. Чини се да је други став више у складу са интенцијом Протокола за превенцију, сузбијање и кажњавање трговине људским бићима да се пружи што шира заштита жртвама трговине.[842]

Осим основног облика, ово кривично дело има и теже облике. Облик из става 2, иако није запрећен тежом казном, у суштини је квалификовани облик јер се, с обзиром на одређену околност, а то је својство пасивног субјекта, инкриминише оно што иначе не би представљало ово кривично дело. Наиме, уколико је радња предузета према малолетном лицу (тј. лицу млађем од 18 година[843]), кривично дело ће постојати и кад учинилац није употребио силу, претњу или неки други од наведених начина извршења, тј. и онда када радња није предзета на начин који јој даје карактер радње извршења овог кривичног дела. У односу на ову околност мора постојати умишљај учиниоца. Тежи облик (став 3) постоји у случају да је дело из става 1 учињено према малолетном лицу. У односу на ову квалификаторну околност

839 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005,72/2009, 111/2009 и 121/2012, члан 388;

840 Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд, стр. 810:

841 Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд, стр. 811;

842 Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд, стр. 811;

843 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009 и 121/2012, члан 112. став 10;

мора постојати умишљај учиниоца. Прописана су и два облика квалификована тежом последицом. У првом случају реч је о тешкој телесној повреди неког лица (став 4), а у другом о смрти (став 5). Иако се у законском опису говори о смрти „неког лица“, то као тежа последица основног облика долази у обзир само када се ради о пасивном субјекту, а не о било ком лицу. У односу на тежу последицу, у складу са општим правилима, мора постојати нехат. Тежи облик (став 6) постоји и у случају да је остварена једна од две квалификаторне околности. Једна је вршење кривичних дела из става 1 до 3, тј. вишекратно понављање радње извршења, а друга вршење кривичног дела од стране најмање 3 лица која су се у том циљу удружила.[844]

Кривично дело трговина малолетним лицима ради усвојења из члана 389 став 1 чини лице које одузме лице које није навршило 16 година ради његовог усвојења противно важећим прописима или ко усвоји такво лице или посредује у таквом усвојењу или ко у том циљу купи, прода или преда друго лице које није навршило шеснаест година или га превози, обезбеђује му смештај или га прикрива. За овај, основни облик тог кривичног дела прописана је казна затвора у трајању од 1 до 5 година. Ако се неко лице бави делатношћу које чине основни облик кривичног дела трговине малолетним лицима ради усвојења или уколико је то дело извршено од стране групе, учинилац се може казнити затвором у трајању од најмање 3 године (члан 389 став 2). Ако је основни облик овог кривичног дела извршен од стране организоване криминалне групе, учинилац ће се казнити затвором у трајању од најмање 5 година.[845] Ова инкриминација је унета у Кривични законик с обзиром на то да кривично дело трговине људима из члана 388 не обухвата трговину децом ради усвојења. Кривично дело (став 1) може бити извршено на више начина. У првом случају радња извршења је одузимање лица које није навршило четрнаест година у циљу његовог усвојења, а противно важећим прописима. Одузиамње значи да се то лице, тј. дете, одузима од лица која по закону имају обавезу и право да се о њему старају (родитељи, старалац и други). То се може учинити силом, претњом, обманом, односно неком преварном радњом. Треба приметити да је услов да се то чини противно важећим прописима – када се ради о одузимању сувишан, јер одузимање ради усвојења не може бити у складу са прописима. Кривично дело чини и онај ко усвоји дете које је одузето ради усвојења, као и оно лице које у томе посредује. Даље, радња извршења је и куповина, продаја, предаја, превожење, обезбеђивање смештаја или прикривање лица које није навршило четрнаест година у истом циљу, тј. ради усвојења. Спорно је да ли и у том случају треба да се ради о одузетом детету. На основу језичког и телеолошког тумачења могло би се закључити да то није нужно, да је довољно да се те радње предузимају ради усвојења које је противно важећим прописима. Заузимање таквог става би значило да ово кривично дело у одређеним случајевима могу да изврше и родитељи детета (на пример, ако продају дете ради усвојења, што је самим тим противно и важећим прописима). Субјективни елемент кривичног дела јесте умишљај који обухвата и свест да се радња извршења предузима ради усвојења детета противно прописима. Ово дело добија тежи вид (став 2) у случају да је остварена једна од две квалификаторне околности. Једна је бављење трговином

844 Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд, стр. 812;

845 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009 и 121/2012, члан 389;

децом ради усвојења, а друга је када је дело извршено организовано од стране више лица. [846]

Кривично дело заснивање ропског односа и превоз лица у ропском односу, прописано чланом 390 Кривичног законика Републике Србије чини лице које, кршећи правила међународног права, стави другог у ропски или њему сличан однос или га држи у таквом односу, купи, прода, преда другом лицу или посредује у куповини, продаји или предаји оваквог лица или подстиче другог да прода своју слободу или слободу лица које издржава или о којем се стара. За ово кривично дело прописана је казна затвора од 1 до 10 година. Лице које превози лица која се налазе у ропском или њему сличном односу из једне земље у другу, казниће се затвором од 6 месеци до 5 година (члан 390 став 2). Уколико је кривично дело заснивања ропског односа и превоза лица у ропском односу учињено према малолетном лицу, учинилаца ће се казнити затвором у трајању од 5 до 15 година (члан 390 став 3).[847]

Дело из овог члана (став 1) има више радњи извршења: а) стављање другог у ропски или њему сличан однос; б) држање другог у таквом односу; в) куповина, продаја или предаја лица које се ставља у ропски или њему сличан однос; г) посредовање у тој куповини продаји или предаји; д) подстицање другог да прода своју слободу или слободу лица које издржава или се о њему стара. С обзиром на то да се и код кривичног дела трговине људима (члан 388) може радити о делатностима које су усмерене на успостављање ропског или њему сличног односа, у неким случајевима се јавља проблем разграничења ова два кривична дела. Превоз лица која се налазе у ропском или њему сличном односу представља лакши облик (став 2). Неопходно је да се превоз чини из једне земље у другу.

За ово кривично дело карактеристично је постојање ропства или њему сличног односа. Према конвенцијама из 1926. (члан 1) и 1956. године, ропством се сматра стање или положај лица над којим се врше сва или нека овлашћења везана за право својине. Поред ропства, обухваћене су и институције и пракса сличне ропству. Ту, пре свега, спадају тзв. ропство због дуга, кметство, продаја женског лица од стране породице ради удаје, продаја или уступање без накнаде малолетног лица од стране родитеља или старалаца ради његовог експлоатисања, као и још неки облици слични ропству предвиђени у члану 1 Допунске конвенције о укидању ропства, трговине робљем и установа и праксе сличне ропству од 1956. године. Квалификовани облик (став 3) постоји када се нека од ових радњи основног или лакшег облика (ст. 1 и 2) изврши према малолетном лицу. Дело из става 1 може се извршити само са директним умишљајем, а дело из става 2 и са евентуалним умишљајем. Постојање свести да се крше правила међународног права, као и код других кривичних дела из ове главе, није потребно.

846 Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд, стр. 812-813;

847 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005, 72/2009, 111/2009 и 121/2012, члан 390;

8. АНАЛИЗА ПОДАТАКА ПРИКУПЉЕНИХ НА ОСНОВУ ИНТЕРВЈУА СА ЖРТВАМА ТРГОВИНЕ ЉУДИМА

Анализа се односи на податке добијене на основу интервјуа који је спроведен у периоду од 24.4.2013. године до 20.6.2013. године на узорку од 50 испитаника, жртава трговине људима. Подаци су обрађени у програмима *Microsoft Office Excel* и *Statistical Package for the Social Sciences (SPSS).*

Жртве трговине људима интервјуисане су у укупно 18 места у Републици Србији: Београду, Новом Саду, Смедереву, Алексинцу, Сомбору, Лесковцу, Бечеју, Крагујевцу, Краљеву, Панчеву, Бољевцу, Инђији, Крушевцу, Лазаревцу, Нишу, Сремској Митровици, Старој Пазови и Тителу. Највећи број жртава интервјуисан је у Београду (14), Новом Саду (6) и Смедереву (5). Укупно 45 жртава интервјуисали су запослени у Центру за заштиту жртва трговине људима. Једну жртву интервјуисали су запослени у Одељењу за јавни ред и мир Полицијске управе за град Београд. За 4 жртве нису унети подаци о организацији која их је интервјуисала.

Женског пола је 46 испитаника, односно 92% узорка, а 4 испитаника, односно 8% узорка су мушког пола.

Укупно 6 испитаника (12%) је узраста од 6 до 14 година, 5 испитаника (10%) има између 15 и 16 година, 10 испитаника (20%) има између 17 и 18 година, 24 испитаника (48%) имају између 19 и 33 година, 4 испитаника (8%) имају између 34 и 49 година и 1 испитаник (2%) има између 50 и 65 година. Заступљеност пунолетних лица у узорку нешто је већа од малолетних, а најзаступљенији су они између 19 и 33 година.

Као државу свог рођења, 20 испитаника (40%) навело је СФРЈ, 25 испитаника (50%) навело је СРЈ, 1 је навео Републику Србију(2%), 1 (2%) Србију и Црну Гору, 1 (2%) Немачку, 1 (2%) Молдавију, а 1 није унео податак о држави свог рођења. Из одговора произлази да је велика већина испитаника са ових простора, те да су само у 2 случаја у питању била лица пореклом из иностранства – Молдавије и Немачке. Од испитаника рођених у Републици Србији, највише је рођено у Београду (7), Новом Саду (6) и Панчеву (4). По 3 испитаника су рођена у Алексинцу, Бечеју, Лесковцу, Смедереву и Сомбору, по 2 у Вршцу и Прокупљу, а по 1 у Аранђеловцу, Бабушници, Гњилану, Зајечару, Инђији, Крагујевцу, Краљеву, Крушевцу, Пироту, Сремској Митровици и Тителу. Укупно 3 испитаника навели су као државу свог рођења државу која није Република Србија. 1 испитаник је навео Македонију, 1 Молдавију, а 1 Немачку.

Скоро половина испитаника, 24 односно 48% је српске националности, али је међу испитаницима значајан број припадника ромске националности - 22, односно 44%. Остале националности заступљене су у малом проценту – само 2% и то: мађарска (1), словачка (1) и молдавска (1). Међу малолетним лицима било највише припадника ромске националности (12), затим српске (8) и на крају словачке (1). Међу пунолетним испитаницима било је више оних који припадају српској националности. Међу испитаницима старости од 19 до 33 године, било је 14 припадника српске националности, 7 ромске, 1 припадник молдавске и 1 припадник мађарске националности. Међу лицима старости од 34 до 49 година била су три припадника ромске и 1 припадник српске националности, док је 1 испитаник из категорије од 50 до 65 година био српске националности. Дакле, од

пунолетних жртава, њих укупно 16 било је српске националности, њих 10 ромске, док је 1 испитаник био молдавске а 1 мађарске националности.

Од 50 испитаника, њих 38 тренутно борави у урбаном подручју у Републици Србији, док њих 12 борави у руралном подручју. Наведени подаци показују да се већина испитаника, након ослобађања из ланца трговине људима, населила у урбаном подручју, што је и логично, будући да је већина њих и пореклом из урбаног подручја, тако да то може указивати да нису мењали животно окружење.

Од укупно 50 испитаника, њих 35 (70%) није у браку, њих 6 (12%) су ожењени/удате, 3 (6%) су разведени/разведене, 2 (4%) су у ванбрачној заједници, док 4 испитаника није унело податак о свом брачном статусу. Анализирани подаци показују да је међу жртвама трговине људима, које су испитане у оквиру овог истраживања, највише неудатих, односно неожењених лица. Од 35 испитаника који су се изјаснили као неожењени/неудате њих 18 је српске националности, њих 14 је ромске, 1 је словачке, а 1 молдавске националности. Од 6 испитаника који су се изјаснили као ожењени/удате, њих 4 су српске, а 2 ромске националности. Од 3 испитаника који су се изјаснили као разведени/разведене, 1 је српске, 1 ромске и 1 мађарске националности. 2 испитаника, који су навели да живе у ванбрачној заједници, су ромске националности.

Од укупно 35 испитаника који су се изјаснили као неожењен/неудата, њих 6 је узраста од 6 до 14 година, њих 4 је узраста од 15 до 16 година, њих 8 је узраста од 17 до 18 година, а њих 17 узраста од 19 до 33 године. Такође, из наведених података се види да ниједан од малолетних испитаника (узраста од 15 до 16 и од 17 до 18 година) није ожењен/удата, као и да је највећи проценат испитаника од 19 до 33 година неудат/неожењен. Када су у питању испитаници који су се изјаснили као ожењени/удате, од укупно 6 испитаника, 2 имају између 19 и 33 године, 3 имају између 34 и 49 година, а 1 има између 50 и 65 година. Сва 3 испитаника који су се изјаснили као разведени/разведене имају између 19 и 33 година. Од 2 испитаника који су у ванбрачној заједници, 1 има између 17 и 18, а 1 између 19 и 33 година.

Садашњи услови становања испитаника, дакле, место њиховог смештаја након изласка из ланца трговине људима, показују на који начин се жртва „снашла“ по изласку из ланца трговине људима, као и да ли на страни државних институција и организација, односно невладиних организација, које се баве заштитом жртава трговине људима, постоји спремност да им обезбеде прихват и смештај. Поред тога, подаци о месту живота, односно о условима становања жртава могу показати колику су оне подршку добиле од своје породице и шире заједнице где су живеле пре виктимизације. Тако би, на пример, чињеница да се жртва вратила у своју породицу након изласка из ланца трговине људима могла показати да је, са једне стране породица за њу „сигурно место“, те да у том случају није представљала извор опасности, као и да је жртва наишла на подршку и разумевање породице, што је важно за успешан опоравак од траума изазваних тим обликом виктимизације. Са друге стане, смештај жртве у просторијама које јој је обезбедила Република Србија може значити да је подршка и помоћ породице у конкретном случају изостала, било да је то због тога што породица није спремна, не жели или не може да пружи смештај жртви, било због тога што је управо неко од чланова породице био тај који је укључио жртву у токове трговине људима и подвргао је неком облику експлоатације. Ово друго посебно је важно када су у питању деца и малолетна лица, која су жртве трговине децом ради усвојења, односно ради принуђавања на просјачење или на вршење кривичних дела, али и на сексуалне и радне

експлоатације и то управо од стране чланова породице. Коначно, број жртава трговине људима смештених у просторијама обезбеђеним од стране Републике Србије показује и спремност наше земље да изађе у сусрет овим лицима, пружајући им различите видове помоћи, подршке и оснаживања, како би наставиле са нормалним животним активностима након престанка експлоатације.

Наведени подаци показују да 19 испитаника живи код родитеља, да је њих 10 смештено у привременом боравишту одређеном од стране Републике Србије, да њих 12 борави у изнајмљеном стану, а њих 4 у сопственом стану. Укупно 5 испитаника није унело податке о свом садашњем смештају. Од 12 испитаника који живе у изнајмљеном стану, њих 10 има између 19 и 33 године, 1 између 34 и 49, а 1 између 50 и 65 година. То значи да су сви испитаници који су смештени у изнајмљеном стану пунолетни. Од 19 испитаника који живе код родитеља, њих 12 је малолетно, док је 7 испитаника пунолетно и спада у категорију од 19 до 33 године. Од 10 испитаника који се налазе на привременом смештају обезбеђеном од стране Владе Републике Србије, њих 7 су малолетни, а 3 су пунолетна и спадају у категорију између 19 и 33 година. Од 4 испитаника који су се изјаснили да живе у свом стану, 1 је малолетан и има између 17 и 18 година, док су 3 пунолетна и имају између 34 и 49 година. Приликом анализирања одговора малолетника да живи у свом стану требало би имати у виду да је, с обзиром на узраст испитаника, већа вероватноћа да је под појмом „свој стан“ подразумевао стан својих родитеља, односно старатеља, односно породични стан или кућу, будући да је мала вероватноћа да лице од 17 година поседује сопствену непокретност.

Од испитаника који живе код родитеља, њих 17 су самци, док је 1 у браку. Од 10 испитаника који се налазе на привременом смештају, обезбеђеном од стране Владе Републике Србије, њих 9 су неожењени/неудате, а 1 је у ванбрачној заједници. Од испитаника који живе у изнајмљеном стану, њих 5 су неожењени/неудате, 2 су ожењени/удате, 3 су разведени, а 1 је у ванбрачној заједници. Од укупно 4 испитаника који су навели да живе у свом стану, 3 испитаниак су ожењени/удате.

Од 19 испитаника који бораве код родитеља, њих 12 живи у урбаној, а њих 7 у руралној средини. Испитаници који се налазе на привременом смештају, који им је обезбедила Влада Републике Србије (њих 10), бораве у урбаној средини. Од 12 испитаника који живе у изнајмљеном стану, њих 9 борави у урбаној, а 3 у руралној средини. Од 4 испитаника који бораве у свом стану, њих 3 се налази у урбаној, а 1 у руралној средини.

Од 19 испитаника који су смештени код родитеља, њих 17 су незапослени, 1 је запослен, а 1 је привремено запослен. Свих 10 испитаника на привременом смештају који им је обезбедила Влада Републике Србије су незапослени. Од 12 испитаника који бораве у изнајмљеном стану, 8 је незапослено, 1 је запослен на привременим, а 1 на повременим пословима. Сва 4 испитаника који живе у свом стану су незапослени.

Од укупно 50 испитаника, њих 6 (12%) нема основно образовање, њих 17 (34%) је уписало, али није завршило основну школу, 14 испитаника (28%) има завршену основну школу, 6 испитаника (12%) је уписало, али није завршило средњу школу или гимназију, њих 6 (12%) има завршену средњу школу, а 1 испитаник (2%) је уписао, али није завршио факултет. Из наведеног следи да 23 од укупно 50 испитаника нема основно образовање – или нису ни похађали наставу или су уписали основну школу, али је нису завршили. Њих 20 има завршену само основну

школу, док њих 7 има завршену средњу школу. То показује да је образовање испитаника, који чине овај узорак, на веома ниском нивоу.

У том смислу, могло би се поставити питање ниског нивоа образовања као фактора виктимизације у случају кривичног дела трговине људима. Наиме, низак ниво образовања и непоседовање адекватних професионалних квалификација отежава проналажење регуларног запослења, те је особа на неки начин „принуђена" да пронађе извор прихода и обезбеди себи егзистенцију на неки други начин. Ипак, треба имати у виду да је у питању мали узорак, ограничен на жртве испитане у одређеном временском периоду, што не допушта да се из њега изведе генерални закључак о томе да су жртве трговине људима у нашој земљи по правилу ниског степена образовања.

Од укупно 6 испитаника који уопште нису похађали школу, 1 лице је узраста између 6 и 14 година, 1 лице је узраста између 15 и 16 година, 2 испитаника су узраста између 17 и 18 година, 1 има између 19 и 33 година, а 1 између 34 и 49 година. Од укупно 17 испитаника који су уписали, али нису завршили основну школу, њих 5 има између 6 и 14 година, 2 имају између 15 и 16 година, 2 између 17 и 18, њих 7 има између 19 и 33 године, а 1 испитаник има између 34 и 49 година.

Будући да је уобичајено да лица заврше основну школу са навршеном 14 годином живота, за 5 испитаника који имају између 6 и 14 година, сасвим је логично да још увек нису завршили основну школу. За 2 испитаника узраста између 15 и 16, па чак и за 2 испитаника узраста између 17 и 18 година, може се претпоставити или да су понављали неки од разреда или да су напустили школовање пре завршетка основне школе. Са друге стране, у погледу 7 испитаника старости између 19 и 33 година, као и за 1 који има између 34 и 49 година, јасно је да су напустили основну школу без намере да се врае у редован образовни систем.

Чињеница да међу пунолетним испитаницима (којих има укупно 29) има 10 лица која нису завршила основну школу (2 испитаника нису ни похађала школу, док 8 испитаника јесте уписало, али није завршило основну школу) и 13 лица која су завршила само основну школу (њих 10 је завршило основну, а њих 3 су након основне уписали али нису завршили средњу школу односно гимназују), те да је само 7 пунолетних испитаника завршило средњу школу (1 од њих је након завршене средње школе уписао факултет, али га није завршио), показује низак ниво образовања жртава трговине људима.

Област образовања испитана је са циљем да се стекне што детаљнији увид у образовни профил жртава трговине људима, како би се могла створити слика о њиховом социјалном, културном, економском миљеу, условима живота, интересовањима и навикама. Дакле, његова природа је квалитативна и у овом истраживању има вредност само у комбинацији са осталим факторима попут степена образовања, економског статуса, запослења итд. Такође, приликом анализирања овог фактора, треба имати на уму да велики број испитаника објективно и није био у могућности да се изјасни о области свог образовања, те због тога од 50 испитаника чак њих 36 (72%) није у упитнике унело податак о области образовања. Наиме, већ је наглашено да укупно 23 испитаника немају ни основно образовање (што је у погледу неких и логично због узраста), а да њих 14 има завршену само основну школу. Од испитаника који су се изјаснили о области свог образовања, 2 су се определила за медицинско-биолошко, 4 за природно-математичко, од њих 8, који су се определили за опцију „остало".

Сврха утврђивања садашњег радног статуса испитаника јесте да се стекне увид у то да ли је, на који начин и у којој мери жртва трговине људима успела да се по изласку из експлоатације врати у нормалне животне токове. Такође, подаци о радном статусу показују и да ли је жртва у стању да по изласку из ланца трговине људима самостално и независно остварује приходе, те да, захваљујући својој економској независности, избегне евентуалну поновну експлоатацију. Веома велика већина испитаника – од 43 од 50 (дакле 86%) изјаснило се да су незапослени, док су само 2 испитаника стално запослена, 2 имају привремено запослење, а 3 обављају повремене послове. Чињеница да је чак 86% жртава трговине људима незапослено показује у којој мери је тај облик виктимизације негативно утицао на њихове животне активности од којих их је у потпуности удаљио, као и на тешкоћу изналажења запослења по изласку из ланца трговине. Незапослености испитаника свакако доприноси и чињеница да међу њима има и малолетних лица и деце, који још увек похађају основну школу, да скоро ¼ узорка чине лица која се налазе на привременом смештају обезбеђеном од стране Владе Републике Србије, те да они, објективно и нису у могућности да имају запослење. У том смислу, незапосленост, прекид континуитета у раду и отежан повратак на тржиште рада и у раније радно окружење, могли би сматрати додатним негативним ефектима и последицама изложености експлоатацији. Анализирани подаци о радном статусу жртава трговине људима који су обухваћено узорком овог истраживања, показују да су међу њима најзаступљенија незапослена лица.

Испитаници који нису незапослени, односно који су запослени (4), који обављају привремене послове (2) и који обављају повремене послове (3) навели су своје садашње запослење. Тако је 1 испитаник навео да ради у бутику и кладионици, 1 у кафани, 1 у грађевинарској струци, 1 се бави чувањем деце, 1 ради као продавац сладоледа, 1 ради у продавници, а 1 на фарми. Дакле, може се констатовати да 3 испитаника раде у малопродајним објектима, док се остали баве пољопривредним, односно услужним делатностима, с тим што 1 поред тога ради у кладионици. Место запослења жртве трговине људима, како пре виктимизације, тако и након изласка из ланца трговине, представља значајан податак, с обзиром на то да се врбовање жртава често дешава управо на радном месту, те да су се на основу искустава из праксе поједина радна места показала као посебно „опасна“, односно подобна да доведу особу у ситуацију у којој постоји повишен ризик од тог облика виктимизације. Као једно од таквих радних места наводи се управо кладионица, премда и угоститељски објекти (кафићи, барови, кафане, клубови и слично) такође спадају у ризична места

Начин на који испитаник види свој садашњи економски статус показује колико је он у економском смислу оштећен због тога што је био жртва трговине људима, да ли је и у којој мери могао да се врати у нормалне животне токове по прекиду експлоатације и у којој мери му је пружена материјална подршка од стране породице, заједнице или државе. Такође, лоша економска ситуација може указивати на то да постоји ризик од поновне експлоатације. При томе треба имати на уму да није у питању објективна процена економске ситуације испитаника, већ субјективна, односно да одговор на ово питање заправо показује како испитаник перципира сопствену економску ситуацију. То не значи да се процена испитаника неће поклапати са његовим реалним и објективним економским стањем.

Укупно 6 (12%) испитаника је оценило свој економски статус као добар, њих 8 (16%) као осредњи, њих 22 (44%) као лош, њих 13 (26%) као веома лош, док 1

испитаник (2%) није желео да се изјасни о томе. Дакле, највећи проценат испитаника оцењује свој садашњи економски статус као лош (44%), док су на другом месту по бројности они који свој економски статус оцењују као веома лош (26%). Такве оцене сопственог економског статуса су у складу су са чињеницом да су у питању лица која су била у једном временском периоду потпуно отргнута из својих редовних животних токова. Такође, оцена сопственог економског статуса као лошег, односно веома лошег, одговара околности да је велики број жртава незапослен, те да је слабог образовања. Као једна од понуђених опција било је наведено и „веома добар“, међутим, ниједан од испитаника се није определио за њу. Анализирани подаци о процени сопственог економског статуса жртава трговине људима показују да постоји одређена статистичка значајност перцепције сопственог економског статуса као лошег, односно веома лошег и виктимизације, али она није велика, бар када је овај узорак у питању.

Највећи број испитаника који су свој статус оценили као лош (њих 10) спада у категорију између 19 и 33 године и највећи број испитаника који су свој статус оценили као веома лош (њих 7) такође спада у категорију између 19 и 33 године. Такође, највећи број испитаника који су свој економски статус оценили као лош (18) и веома лош (11) живи у урбаној средини. Од 6 испитаника који су свој економски статус оценили као добар, 1 испитаник је уписао, али није завршио основну школу, 1 је уписао, али није завршио средњу школу, а 4 су завршили средњу школу. Од 8 испитаника који су свој економски статус оценили као осредњи, 2 су без школе, 1 има уписану, али незавршену основну школу, 4 имају завршену основну школу, а 1 завршену средњу школу. Од 22 испитаника који су свој економски статус описали као лош, њих 10 има уписану, али незавршену основну пколу, њих 7 има завршену основну школу, 3 имају уписану, а незавршену средњу школу, 1 завршену средњу школу и 1 има уписан, а незавршен факултет. Од 13 испитаника који су свој економски статус оценили као веома лош, њих 4 је без школе, 4 су уписали, али нису завршили основну школу, 3 имају завршену основну школу, 1 има уписану, а незавршену средњу школу, а 1 има завршену средњу школу. Само 1 испитаник који нема основно образовање оценио је свој економски статус као добар, 3 су оценили као осредњи, 10 као лош, а 8 као веома лош. Само 1 испитаник који има основно образовање оценио је свој економски статус као добар, 5 су га оценили као осредњи, 10 као лош и 4 као веома лош. Од испитаника који имају средње образовање, 4 су свој економски статус оценили као добар, ниједан од њих није свој економски статус оценио као осредњи, 2 су га оценили као лош, а само 1 као веома лош. Из наведеног следи да су испитаници, који нису завршили основну школу или имају само основно образовање, били склонији да свој економски статус оцене негативно него они који имају средње образовање.

За потребе овог истраживања, податак о познавању страних језика од стране жртава трговине људима важан је за процену њихове способности да употребљавају информационо-комуникационе технологије, као и за процену њихове могућности да информационо-комуникационе технологије употребљавају на правилан начин и у правилне сврхе, да препознају опсаности и да се од њих заштите. Наиме, познато је де је највећи број садржаја на интернету на енглеском језику, као и да је макар основно знање енглеског језика практично предуслов за коришћење друштвених мрежа, чак и ако се у конкретном случају комуникација између корисника одвија на неком другом језику. Од 50 испитаника, 7 је навело да говори неки страни језик, 42 су одговорила да не говоре ни један страни језик, а у 1 случају је у питању био

погрешан унос. Ови подаци показују да већина испитаника (84%) не говори ни један страни језик. Као страни језик који говоре, 2 испитаника навела су енглески, 1 мађарски, 1 руски, а 1 српски језик.

Анализирани статистички подаци показују да је заступљеност лица која не говоре ниједан страни језик међу жртвама тровине људима знатно већа од оних који говоре неки страни језик. Ту околност требало би имати у виду, пре свега као ограничавајући фактор када је у питању приступ жртвама трговине људима савременим информационо-комуникационим технологијама, будући да је велика количина садржаја на интернету (како на сајтовима, тако и на друштвеним мрежама) на енглеском језику, као и да је за коришћење ових средстава комуникације потребно барем базично знање енглеског језика. Ипак не треба занемарити чињеницу да постоји велики број интернет сајтова преко којих се могу врбовати жртве трговине људима, чији је садржај искључиво на српском језику, те да се исто односи и на огласе објављене на интернету, као и на профиле трговаца људима и регрутера или других лица који им помажу на друштвеним мрежама. То значи да би непознавање страних језика практично ограничило жртву само када је у питању непосредно ступање у контакт и директно комуницирање са иностраним трафикерима и регрутерима који не знају српски језик, или директно пријављивање на огласе или сајтове за врбовање чија је садржина на страном језику. Чак ни тада, непознавање страног језика не би било препрека да се жртва укључи у међународни ланац трговине људима, уколико би у томе посредовао трафикер или регрутер који говори српски језик.

Највећи број испитаника који говоре неки страни језик су пунолетни. Када су у питању испитаници који не говоре ни један страни језик, њих 19 спада у категорију између 19 и 33 година, 4 има између 34 и 49, 6 између 6 и 14, а 4 између 15 и16. Од 7 испитаника који говоре неки страни језик 1 има уписану а незавршену основну школу, 3 имају завршену основну школу а 2 завршену средњу школу. Од 42 испитаника који не говоре ни један страни језик, 6 је без школе, 15 има уписану, а незавршену основну школу, 11 има завршену основну школу, 6 уписану, а незавршену сресњу школу, а 4 завршену средњу школу.

Знање да се користи рачунар представља предуслов да се појединац уопште нађе у ситуацији да буде врбован за трговину људима путем друштвених мрежа, односно да трговац људима са њиме одржава контакт током експлоатације на тај начин. Од укупно 50 испитаника, њих 27 (55%) изјавило је да зна да користи рачунар, док су 22 испитаника (45%) навела да не знају да користе рачунар. Од 27 испитаника који знају да користе рачунар, 1 има између 6 и 14 година, 4 између 15 и 16 година, 6 између 17 и 18 година, 14 између 19 и 33 година, а 2 између 34 и 49 година. Од 22 испитаника који не знају да користе рачунар, њих 5 има између 6 и 14 година, 4 између 17 и 18 година, 9 између 19 и 33 године, 2 између 34 и 49 и 1 између 50 и 65 година. Од 27 испитаника који знају да користе рачунар, највећи број њих има завршену основну школу (9), али по 6 испитаника има уписану, али незавршену основну школу, уписану, али незавршену средњу средњу школу и завршену средњу школу. Од 22 испитаника који не знају да користе рачунар, њих 4 су без школе, 11 има уписану, а незавршену основну школу, 5 има завршену основну школу, а 1 уписан, али незавршен факултет.

Подаци показују да највећи проценат испитаника који не знају да користе рачунар спада у категорију лица која су уписала, али која нису завршила основну школу, те да лица која немају основно образовање (њих 11 који су уписали, али

нису завршили основну школу и њих 4 који нису ни похађали основну школу) заједно чине највећи проценат оних који не знају да користе рачунар. Затим следе лица која имају само завршену основну школу, којих има укупно 5. То показује да је, бар на овом узорку степен образовања директно пропорционалан са знањем коришћења рачунара, односно да они испитаници који су вишег степена образовања у већем броју случајева и знају да користе рачунар. Изузетак представља испитаник који је уписао, али није завршио факултет (што значи да је морао имати барем средње образовање), а који не зна да користи рачунар. Међутим, треба напоменути да је у питању лице које има између 50 и 65 година, те да, с обзиром на чињеницу да у нашој земљи велики број припадника средовечне и старије популације не користи рачунар, такав одговор није неуобичајен.

Од 49 жртава трговине људима које су одговориле на питање о знању употребе рачунара, њих 27 одговорило је потврдно, а 22 су одговориле одрично. Од 44 ирегуларна мигранта, 24 је одговорило да зна да користи рачунар, а 20 да не зна. Од 53 азиланта, њих 44 је одговорило да зна да користи рачунар, а њих 9 да не зна.

Из наведеног се може уочити да је најмањи број оних који не знају да користе рачунар присутан код азиланата, док је број жртава трговине људима и ирегуларних миграната који знају да користе рачунар знатно мањи, како у апсолутном износу (27 жртава и 24 мигранта), тако и у односу на укупан број припадника тих категорија (нешто више од 50%). Такав однос између ове три категорије показује да је код азиланата највећа вероватноћа да ће злоупотребити информационо-комуникационе технологије у сврху илегалних миграција него што је то код ирегуларних миграната, односно у случају жртава трговине људима – вероватноћа да ће бити врбоване или експлоатисане злоупотребом информационо-комуникационих технологија од стране трговца људима.

За разлику од знања коришења рачунара, које је предуслов да се овај облик информационо-комуникационих технологија уопште употребљава од стране жртве, те да жртва буде изложена виктимизацији услед злоупотребе ИКТ-а од стране трговца људима, поседовање рачунара није нужан предуслов за то. Ипак, чињеница је да доступност рачунара, било да је у питању десктоп рачунар који жртва може користити у свом дому или лаптоп тј. Ноутбук, може у знатној мери олакшати приступ овом облику информационо-комуникационих технологија, а самим тим и приступ друштвеним мрежама и другим каналима комуникације путем којих се може остварити и одржавати контакт између жртве и трафикера. На питање да ли поседујете рачунар, било је могуће заокружити више оговора. 14 испитаника је одговорило да поседује рачунар код куће, а 2 су одговорила да поседују лаптоп или ноутбук, што значи да укупно њих 16 поседује неки рачунар. Укупно 34 испитаника је одговорило да не поседује рачунар.

Као и у случају рачунара, поседовање мобилног телефона од стране жртве практично представља предуслов да она буде виктимизирана на начин који подразумева овај облик информационо-комуникационих технологија, односно да трговац људима путем мобилног телефона са њом успостави контакт, да је врбује, као и да одржава контакт током периода експлоатације – да је контролише и проверава, да јој даје инструкције итд. Од 50 испитаника, 41 испитаник (82%) поседује мобилни телефон, а њих 9 (18%) га не поседује, што значи да су међу жртвама трговине људима, које су ушле у овај узорак, била заступљенија лица која поседују мобилни телефон у односу на она која га не поседују.

Слично, као и у вези са поседовањем и коришћењем рачунара, односно мобилног телефона, коришћење интернета од стране испитаника може се сматрати предусловом да он уопште дође у ситуацију да буде у ризику од виктимизације путем злоупотребе овог облика информационо-комуникационих технологија од стране трговца људима. Коришћење интернета је предуслов за приступ друштвеним мрежама, комуницирање путем чета, мејла, приступ сајтовима и огласима путем којих се врбују жртве трговине људима итд. Од 50 испитаника, њих 27 (54%) изјавило је да користи интернет, док је њих 23 (46%) изјавило да не користи интернет. Пошто је укупно 27 испитаника од 50 изјавило да зна да користи рачунар, може се претпоставити да истих 27 испитаника користи и интернет.

Од 27 испитаника који користе интернет, највећи број њих, тачније 14 (58,33%) спада у категорију између 19 и 33 година, 7 спада у категорију од 17 до 18 година, 4 има између 15 и 16 година, 1 има између 6 и 14 година и 1 између 34 и 49 година. Испитаници старости од 19 до 33 године који користе интернет, бројнији су од свих осталих категорија заједно. Од 23 испитаника који не користе интернет, њих 5 има између 6 и 14 година, 1 има између 15 и 16 година, 3 има између 17 и 18 година, 10 има између 19 и 33 година, 3 има између 34 и 49 година и 1 има између 50 и 65 година.

Од 27 испитаника који користе интернет њих 25 (92,59%) има мобилни телефон, а 2 испитаника (9,52%) немају мобилни телефон. Од 22 испитаника који не користе интернет 2 испитаника имају мобилни телефон, а 19 испитаника који не користе интернет (90,48%) нема ни мобилни телефон. То показује да већина ипитаника који користе интернет истовремено поседује и мобилни телефон, док они испитаници који не користе интернет немају ни мобилни телефон и обрнуто. Дакле, већина испитаника користити обе информационо-комуникационе технологије, док се само мали број њих определио само за интернет (2), односно само за мобилни телефон (2).

Анализирани подаци показују да су међу испитаницима који користе интернет најзаступљенији они који поседују мобилни телефон, док су код испитаника који не користе интернет знатно заступљенији они који не поседују ни мобилни телефон. Најмање су заступљени они испитаници који поседују мобилни телефон, а не користе интернет и они који користе интернет, а не поседују мобилни телефон. Таква заступљеност показује да жртве трговине људима које су укључене у овај узорак у већини случајева не користе мобилни телефон као замену за интернет и обрнуто, интернет као замену за мобилни телефон приликом комуникације, већ да је знатно учесталија појава да користе обе од наведених информационо-комуникационих технологија, дакле, и мобилни телефон и интернет заједно.

Од 50 испитаника, њих 27 користи интернет, а њих 23 не користи интернет, од 91 испитаника ирегуларних миграната, њих 54 користи интернет а њих 37 не користи интернет, од 53 испитаника – азиланта, њих 47 користи интернет а њих 6 не користи интернет. Највећи проценат испитаника који користе интернет налази се међу азилантима – чак 47 азиланата од 53, односно 88,68% испитаних азиланата користи интернет док га њих 6 (11,32%) не користи. На другом месту су ирегуларни мигранти – од 91 испитаника њих 54 (59,34%) користи интернет, а њих 37 (40,66%) га не користи. На крају, најмањи број испитаника који користе интернет налази се међу жртвама трговине људима – њих 27 користи интернет (54%), а њих 23 га не користи (46%).

У сваком случају, и међу жртвама трговине људима, и међу ирегуларним мгрантима и међу азилантима је већи број оних испитаника који користе интернет него оних који га не користе. Статистички је значајан однос између броја жртава трговине људима које користе интернет и азиланата који користе интернет, као и однос између ирегуларних мигранта који користе интернет и азиланата који користе интернет. Први однос показује да су корисници интернета знатно заступљенији међу азилантима него међу жртвама теговине људима. Други однос показује да су корисници интернета знатно заступљенији међу азилантима него међу ирегуларним мигрантима.

Коришћење друштвених мрежа један је од предуслова да се жртва уопште нађе у ситуцаији да посредством тог облика комуникације буде врбована од стране трговаца људима, односно да трговац на тај начин ступи у контакт са њом те да тако остварен контакт касније одржава. Због тога је податак о броју жртава трговине људима, које користе друштвене мреже, битан као показатељ колико њих је у реалној могућности да буде изложено ризику од таквог облика виктимизације. Код жртава које су изашле из ланца трговине људима, коришћење друштвених мрежа, нарочито ако је неопрезно и небезбедно, може бити фактор који повећава ризик од њихове поновне виктимизације – на пример тако што би трговац људима или лица која су са њим повезана могла преко друштвених мрежа поново да ступе у контакт са њом, открију где се она тренутно налази и угрозе њену безбедност, или да је чак поново подвргну неком облику експлоатације. Од укупно 50 испитаника, њих 24 (48%) одговорили су да користе друштвене мреже, а њих 26 (52%) одговорило је да не користе друштвене мреже. Као што се може претпоставити, у питању је податак који нема статистичку значајност, односно из односа броја жртава трговине људима које користе и које не користе друштвене мреже не може се извести закључак о учесталости коришћења друштвених мрежа међу жртвама трговине људима. Од 24 испитаника који користе друштвене мреже, сви су навели да имају налог на Facebook-у, а 1 испитаник је навео да има налог на Twitter-у. Истовремено, међутим, 5 испитаника навело је да нема налог ни на једној друштвеној мрежи.

8.1 Подаци о контексту трговине људима

У највећем броју случајева из испитиваног узорка, трафикер је ступио у контакт са жртвом 2012. године - 23 случаја односно 46%. У по 8 случајева (16%) трафикер је ступио у контакт са жртвом 2011, односно 2013. године. У по 2 случаја, трафикер је ступио у контакт са жртвом 2010, 2008. и 1995. године, док је у по 1 случају то учињено 1988, 2001, 2006. и 2009. године. Само 1 испитаник није навео које године је трафикер први пут ступио у контакт са њим.

Повезана са годином када је трафикер по први пут ступио у контакт са жртвом, година регрутације, односно година укључивања у трговину људима показује колико је времена протекло од момента када је трафикер по први пут остварио контакт са жртвом, па до момента када је она била подвргнута експлоатацији. Овај податак говори о дужини трајања периода врбовања жртве и показује колико је времена било потребно трафикеру да жртву укључи у ланац трговине људима. Упоређивањем дужине периода врбовања са подацима о томе да ли је трафикер том приликом и у ту сврху користио, односно злоупотребљавао информационо-комуникационе технологије, може се утврдити да ли њихова

примена олакшава, односно убрзава процес врбовања жртве и у коликој мери. Повезивањем године регрутације са годином изласка из ланца трговине људима, логично, може се видети колико дуго је свеукупна експлоатација жртве трајала.

Највећи број жртава обухваћених овим истраживањем регрутован је 2012. године – њих 20 (40%), затим 2013. године – њих 12 (24%), па 2011. године – њих 7 (14%). Током 2010. године регрутована су 4 испитаника (8%), током 2009. године регрутовано је 5 испитаника (10%), док је по један испитаник регрутован 2006. и 1995. године. Када се упореде подаци о години када је жртва регрутована, односно укључена у трговину људима и година када је трафикер први пут ступио у контакт са њом, може се закључити да је у 41 случају (82%) период између та два тренутка („период врбовања“) био краћи од годину дана. У 5 случајева (10%) је период врбовања трајао годину дана, док је у 4 случаја (8%) тај период износио 2 године или више. Када су у питању случајеви где је период врбовања трајао преко 2 године, у 1 се радило о периоду од 8 година, у 1 од 15 и у 1 од 22 године.

Највећи број испитаника из овог узорка потражило је помоћ током 2013. године – њих 28 (56%). Током 2012. године помоћ је потражило 16 испитаника (32%), током 2011. године 3 испитаника (6%), током 2009. године 2 испитаника (4%), а током 2006. године 1 испитаник (2%). У 26 случајева (52%) је период између тренутка регрутације и тренутка тражења помоћи од стране жртве трајао мање од годину дана, у 16 случајева (32%) је трајао годину дана, у 4 случаја је трајао 3 године, у 2 случаја је трајао 4 године, у 1 случају је трајао 2 године, а у 1 чак 16 година.

Подаци о субјектима којима су се жртве обратиле за помоћ у свом настојању да изађу из трговине људима показују колико су оне поверења поклањале појединим органима, институцијама, организацијам или појединцима. То такође указује и на њихову упознатост са тим који субјекти су надлежни и овлашћени да им помогну. Највећи број испитаника се за помоћ обратио полицији – 41 испитаник, односно 82% од укупног броја испитаника. Другом државном органу обратила су се 4 испитаника (8%), невладиној организацији обратила су се 2 испитаника (4%), док су се члану породице за помоћ обратила такође 2 испитаника. Један испитаник обратио се за помоћ истовремено и члану породице и невладиној организацији. Од државних органа којима су се жртве обратиле за помоћ, а који не спадају у органе унутрашњих послова, наведени су: Центар за социјални рад у 2 случаја и здравствена установа у 2 случаја. Када су у питању невладине организације, помоћ је затржена од: организације ЛЕФО[848], АСТРА[849] и „сигурна кућа“[850].

---

848 Организација „ЛЕФО“ је невладина организација са седиштем у Бечу која се бави заштитом права жена миграната, а посебно сексуалних радница и жртава трговине људима. Основана је 1985. године и настоји да одговори на разноврсне и комплексне потребе жена миграната, које су настале као резултат миграција током протеклих 25 година. У фокусу ове организације јесте заштита оних жена миграната које спадају у категорију сексуалних радница и или жртава трговине људима. И данас „ЛЕФО“ представља једину невладину организацију у Аустрији која се бави пружањем подршке и правних савета овој категорији корисника. Извор: http://www.lefoe.at/index.php/About_LEF%C3%96.html, 28.10.2013;

849 Организација „АСТРА“ је локална невладина организација посвећена борби против трговине људима основана 2000. године. Третира различите облике трговине људима и категорије жртава – жене, децу и мушкарце. Истовремено делује у области превенције, едукације, подизања јавне свести, пружања директне помоћи жртвама, реинтеграције, истраживања и извештавања, јавног заступања на стратешком и оперативном нивоу и подржава изградњу функционалног и ефикасног система за сузбијање трговине људима који поштује људска права жртава. Извор: http://www.astra.org.rs/o-astri/, 28.10.2013;

Када се упореди са годином регрутације, односно годином укључења у трговину људима, година изласка из трговине људима показује колико је трајао период експлоатације. Када се упореди са годином када се жртва некоме обратила за помоћ, година изласка из трговине људима показује колико је субјект, коме се жртва обратила за помоћ, заправо био спреман да реагује и колика је била његова еикасност. То је посебно важно када су у питању државни органи, али и невладине организације, јер се уз одређене разерве дужина тог периода може сматрати критеријумом за евалуацију квалитета, брзине и ефикасности њиховог рада. Од 50 испитаника, њих 24 (48%) из трговине људима је изашло 2013. године, њих 14 (28%) 2012. године, 2 (4%) 2011. године, 2 (4%) су изашла 2009 године, 1(2%) је изашао 2008. године и 1(2%) 2006. године. У 43 случаја из испитиваног узорка, период између године обраћања за помоћ и године изласка из трговине људима је трајао мање од годину дана, док је у једном случају он био дужи од 1, а краћи од три године.

Дужина овог временског периода показује колико је укупно трајао период експлоатације. У 22 случаја из испитаног узорка, тај период је био краћи од годину дана, у 15 случајева је трајао годину дана, у 1 случају је трајао 2 године, у 4 случаја је трајао 3 године, у 1 случају је трајао 4 године и у 1 случају је трајао чак 13 година.

Место где је жртва смештена након прекида експлоатације показује начин на који је она решила своје стамбено питање по изласку из трговине људима и ствара општу слику о томе како се она „снашла“ и да ли је успела да се након виктимизације врати у нормалне и редовне животне токове. Смештај жртве у своју матичну породицу могао би показати да на страни породице постоји подршка жртви те да изостаје стигматизација од стране чланова породице, па и уже заједнице у односу на жртву због природе експлоатације којој је била изложена.

Са друге стране, смештај жртве у оквиру институција Републике Србије (као што је на пример Центар за заштиту жртава трговине људима) показује спремност и капацитете наше земље да пружи жртвама и овај, веома значајан вид подршке, помоћи и заштите. Наиме, у случају жртава трговине људима које су успеле да изађу из ланца трговине, смештај често не значи само кров над главом, већ представља и заштиту од њихове поновљене виктимизације и то у првом реду од стране трафикера од кога су успеле да се отргну. До поновљене виктимизације би у таквим случајевима могло доћи не само због жеље трафикера да настави да остварује добит експлоатисањем жртве, већ и због његове жеље да онемогући жртву да сведочи и изнесе доказе против њега у евентуалном судском поступку. Од укупно 50 испитаника, њих 24 (48%) је након прекида експлоатације нашло смештај у породици свог порекла, њих 12 (24%) смештај је пронашло у „сигурној кући“, 4 испитаника (8%) обезбедили су себи самостално смештај. Укупно 8 испитаника (16%) навело је да се сместило на „друго место“, а 1 испитаник није одговорио на питање. Од 8 испитаника који су се определили за опцију „нешто друго“, 1 је навео

850 Сигурне женске куће су настале као пројекат СОС-телефона и Саветовалишта за жртве породичног насиља, а данас су самостални пројекти које реализују невладине организације и центри за социјални рад уз подршку локалних самоуправа. Намењене су женама и деци које трпе насиље од стране другог члана породице и пружају: смештај и исхрану, сигурност, емотивну подршку, правну помоћ, разне обуке у циљу оспособљавања за лакше запошљавање, помоћ при проналажењу посла, подршку у доношењу одлука и подршку у реализацији донетих одлука. Носилац пројекта је организација „АДРА Србија“. Извор: http://sigurnakuca.org/index.php?option=com_content&view=section&layout=blog&id=6&Itemid=56, 28.10.2013;

да је смештен код сестре, 1 у хранитељској породици, 2 су смештена у изнајмљеној соби, 2 у прихватилишту, 2 у дому за децу, 1 код пријатеља, 1 у изнајмљеном стану и 1 у породици ванбрачног партнера. Анализирани подаци показују да је најчешћи случај да се жртве трговине по прекиду експлоатације сместе у породицу свог порекла, док је по заступљености на другом месту смештај жртава у „сигурне куће".

Највећи број испитаника из овог узорка били су жртве сексуалне експлоатације 29 је било изложено само сексуалној експлоатацији док је у 1 случају она била комбинована са радном експлоатацијом а у 1 случају са принудом на вршење кривичних дела. У 29 случајева (58%) жртве су биле изложене искључиво сексуалној експлоатацији. У 5 случајева (10%) жртве су биле изложене радној експлоатацији, у 5 случајева (10%) радило се о принуди на закључење брака, у 6 случајева (12%) о принуди на просјачење, у 2 случаја о принуди на вршење кривичних дела, а у 1 случају је дошло до прекида у фази врбовања, тако да жртва није била изложена ниједном облику експлоатације.

Поред тога, у 2 случаја је постојало комбиновање различитих облика експлоатације жртве. У једном случају се радило о комбиновању сексуалне експлоатације и радне експлоатације, а у другом о комбиновању сексуалне експлоатације и принуде на вршење кривичних дела. И наведена два случаја комбиноване, односно вишеструке експлоатације треба узети у обзир приликом израчунавања укупног броја случајева који су били подвргнути неком од видова експлоатације. Тако, ако се они узму у обзир, следи да је сексуалној експлоатацији укупно био подвргнут 31 испитаник, радној експлоатацији укупно 6 испитаника, а принуди на вршење кривичних дела 3 испитаника.

Анализирани подаци показују да је од типова трговине људима, односно од облика експлоатације жртава трговине људима најзаступљенија била сексуална експлоатација, о којој је било речи у 58% случајева. Од укупно 31 случаја сексуалне експлоатације (у 29 случајева је у питању била искључиво сексуална експлоатација док је у 1 случају она комбинована са радном експлоатацијом, а у другом са принудом на вршење кривичних дела), 15 жртава је било српске националности, 13 жртава је било ромске националности, 1 мађарске, 1 словачке и 1 молдавске. Од укупно 6 случајева радне експлоатације (у 5 случајева се радило искључиво о радној експлоатацији, док је у 1 случају она комбинована са сексуалном експлоатацијом), 4 жртве су биле српске националности, а 2 ромске. Од укупно 5 случајева трговине људима ради принуде на закључење брака, 3 жртве су биле ромске, а 2 српске националности.Од укупно 6 случајева трговине људима ради принуде на просјачење, 4 жртве су биле ромске, а 2 српске националности. Када је у питању трговина људима ради принуде на вршење кривичних дела, у сва 3 случаја (у 2 се радило искључиво о принуди на вршење кривичних дела док је у 1 она комбинована са сексуалном експлоатацијом) жртве су биле српске националности.

Страни држављани, испитаници мађарске, словачке и молдавске националности били су изложени само сексуалној експлоатацији, док је међу припадницима српске националности било свих облика експлоатације. Код припадника ромске националности забележени су сви облици експлоатације осим принуде на вршење кривичних дела. Као што је већ истакнуто, ниједна од жртава није навелада је била врбована због трговине органима.

8.2 Контекст регрутације и начина одржавања контакта

Радни статус жртве у тренутку када је трафикер ступио у контакт са њом може бити показатељ у којој мери је незапосленост фактор виктимизације у случају кривичног дела трговине људима. Наиме, познато је да жртве трговине људима често дођу у ситуацију у којој су експлоатисане управо у жељи да пронађу посао или додатни извор прихода. Од 50 испитаника, 41 (82%) испитаник је у тренутку када је трговац људима ступио у контакт са њима био незапослен, 4 испитаника (8%) су били запослени, 2 (4%) су била привремено запослена, а 2 (4%) повремено запослена. Један испитаник није унео одговор на ово питање. Дакле, међу жртванма трговине људима које су обухваћене овим истраживањем, најзаступљенија су била незапослена лица и тај податак јесте статистички значајан, утолико што указује да је већа вероватноћа да ће незапослено лице постати жртвом трговине људима него лице које има стално запослење. Наведени подаци могли би се употребити као аргументи у прилог претпоставци да је незапосленост један од фактора ризика од постајања жртвом кривичног дела трговине људима. Ипак, опет треба имати на уму незавидну величину узорка који је обухваћен овим истраживањем.

Од укупно 4 испитаника који су у моменту регрутације били запослени, 3 су имали између 19 и 33 година, а 1 између 50 и 65 година. Од укупно 41 испитаника који је у тренутку регрутације био незапослен, њих 20 су били малолетни, тачније, њих 6 имало је између 6 и 14 година, 4 су имала између 15 и 16, а 10 између 17 и 18 година. Од пунолетних незапослених испитаника, њих 18 имало је између 19 и 33 година, 3 су имали између 34 и 49 година. Највећи број испитаника је, у тренутку регрутације, био незапослен – њих 18, тј. 75%. У питању су лица од 19 до 33 година.

Од укупно 4 запослена испитаника, 2 су у тренутку регрутације боравила у урбаном подручју, а 2 у руралном. Од 41 незапосленог испитаника, у тренутку регрутације 33 су боравили у урбаном подручју, а 8 испитаника је боравило у руралном подручју. Оба испитаника који су били запослени на привременим пословима боравили су у тренутку регрутације у урбаном подручју, а од повремено запослених испитаника 1 је боравио у урбаном, а 1 у рурачном подручју, у тренутку регрутације. Наведени подаци показују да су међу испитаницима најзаступљенији они који су у тренутку регрутације били незапослени и који суборавили у урбаном подручју.

Као што је већ истакнуто, низак степен образовања представља један од фактора који смањују конкурентност појединца на тржишту рада, те самим тим и вероватноћу да ће он бити незапослен. Истовремено, незапосленост појединца, логично, један је од главних узрока његовог лошег економског статуса, будући да не поседује извор редовних и легалних прихода. Лош економски статус, проузрокован по правилу незапосленошћу и необразовањем и непоседовањем одговарајућих стручних квалификација за постизање конкурентности на тржишту рада, сматра се једним од фактора који повећавају ризик од виктимизације у случају кривичног дела трговине људима. Наведене претпоставке потврђују и подаци прикупљени у овом истраживању, који показују да је већина испитаника-жртава трговине људима у тренутку регрутације била ниског нивоа образовања, као и да је већина њих у тренутку регрутације била незапослена.

Од 49 испитаника који су се изјаснили о свом радном статусу, 41 испитаник је био незапослен у тренутку регрутације. Од тога је њих 6 било без школе, њих 15

имало је уписану, а незавршену основну школу, њих 10 имало је завршену основну школу, њих 5 уписану, а незавршену средњу школу, њих 4 имало је завршену средњу школу ,а 1 је имао уписан и незавршен факултет. То значи да у тренутку регрутације 21 испитаник није био запослен и није имао завршену основно образовање, да је њих 15 имало основно образовање, а њих 5 средње образовање. Међутим, приликом анализе образовања и радног статуса треба узети у обзир и године старости испитаника, будући да су неки од њих управо деца школског узраста, те да се од њих и не може објективно очекивати да поседују виши степен образовања нити да буду у радном односу. Тако треба истаћи да је од укупно 41 испитаника, колико их је било незапослено у тренутку регрутације, њих 6 било узраста од 6 до 14 година, њих 4 узраста од 15 до 16 година и њих 10 узраста од 17 до 18 година. Будући да се малолетник може запослити тек са навршених 15 година живота, 6 испитаника из ове категорије нису уопште ни били у законској могућности да заснују радни однос. Исто важи и за образовање. При томе треба навести да су сви испитаници који су били запослени у тренутку регрутације били пунолетни (4 који су били запослени, 2 који су обављели привремене и 2 који су обављели повремене послове). Од 4 запослена 3 су имала између 19 и 33 година, а 1 између 50 и 65 година, док су лица запослена на привременим, односно повременим пословима спадала у категорију од 13 до 33 година.

Као што је већ истакнуто у делу анализе која се односи на генералне податке о жртви, место запослења је веома важан фактор који може допринети повећању ризика од виктимизације. Такође је наглашено да постоје одређена радна места која се сматрају посебно погодним за врбовање жртава трговине људима. Ту спадају нарочито: кафићи, кладионице, ноћни клубови, кафане и слична места, која су позната по томе да се на њима жртве врбују за трговину људима, посебно у сврху сексуалне експлоатације. У том смислу, чињеницу да је неко лице запослено не треба увек посматрати као фактор који ће умањити ризик од виктимизације. Иако особа тада има извор прихода, те није због недостатка прихода принуђена да се подвргава неком облику експлоатације, њено место запослења је баш подобно да је доведе у положај експлоатисаности, односно да је учини жртвом трговине људима.

Од испитаника који су навели да су у тренутку регрутације били запослени, било да је реч о „редовном“ запослењу (4 испитаника), било да се ради о привременим пословима (2 испитаника) односно повременим пословима (2 испитаника), њих 4 навели су да су били запослени у кафићу, 1 је навео да је био запослен у продавници, а 1 у кладионици. Такви одговори говоре у прилог наведеној претпоставци о местима где се жртве по правилу врбују.

Оцена сопственог економског статуса у тренутку када је трафикер ступио у контакт са жртвом показује да ли и у којој мери перципирање сопственог економског статуса као лошег или недовољно доброг, представља фактор који повећава ризик од виктимизације. Наиме, чињеница да је жртва у тренутку регрутације и, уопште, у периоду врбовања, свој економски статус доживљавала као лош или веома лош, говори у прилог томе да се подвргла експлоатацији од стране трафикера управо са намером да оствари приходе, односно обезбеди средства за живот за себе и чланове своје породице. Као и у делу у коме су анализирани општи подаци о садашњем економском статусу жртве, и овде треба нагласити да је у питању субјективна процена економског статуса, дакле да испитаник сам наводи на који начин он доживљава свој економски статус. Наравно, то не значи да се субјективна процена испитаника неће поклапати са његовом објективном

економском ситуацијом, али је као фактор ризика у овом случају ипак битније како је он сам доживљава, односно да ли је доживљава као тако лошу да га је она подстакла да се подвргне експлоатацији.

Од укупно 50 испитаника, њих 6 (12%) је свој економски статус у тренутку када су ступили у контакт са трафикером оценило као добар, њих 6 (12%) је свој економски статус оценило као осредњи. Чак 28 испитаника (56%) оценило је свој економски статус у тренутку регрутовања као лош, док га је њих 10 (20%) описало као веома лош. Наведени подаци показују да су међу жртвама трговине људима које су укључене у овај узорак најзаступљенија лица која свој економски статус описују као лош. Наведени о подаци показују да се већина испитаника негативно изразила о свом економском статусу у тренутку када је трафикер ступио у контакт са њима. Ако се саберу они испитаници који су свој економски статус описали као лош (њих 28) и они који су га описали као веома лош (њих 10) види се да се о свом економском статуси у негативном смислу изјаснило 38 од 50 испитаника, што чини 76% од укупног броја испитаника. Иако је узорак веома мали те све процене треба чинити са резервом, наведено показује да су жртве углавном биле незадовољне својим економским статусом у тренутку када их је трафикер контактирао.

Од укупно 6 испитаника који су свој економски статус у тренутку када је трафикер ступио у контакт са њима оценили као добар, 2 су била запослена, а 4 незапослена. Од 5 испитаника који су свој економски статус оценили као осредњи, 4 испитаника су била незапослена, а 1 је био запосолен на привременим пословима. Од 28 испитаника који су свој економски статус у моменту регрутације описали као лош, 23 испитаника су били незапослени, 2 су била запослена, 1 је обављао привремене послове, а 2 су обављели повремене послове. Од 10 испитаника који су свој економски статус описали као лош, свих 10 испитаника су били незапослени. То показује да је највећи број незапослених испитаника (33 од 41) свој економски статус оценио негативно – као лош (23) односно веома лош (10). Међутим, од 4 запослена испитаника, 2 су свој економски статус оценила као лош, док су га 2 оценила као добар. Од запослених на привременим пословима 1 испитаник је свој економски статус описао као осредњи, а 1 као лош, док су оба испитаника, који су у тренутку регрутације обављали повремене послове, своје економски статус описали као лош.

Интересантно је да је међу испитаницима који су свој економски статус описали као добар било више незапослених (4 од 6) него запослених (2 од 6), као и да је међу испитаницима који су свој економски статус описали као осредњи такође било 4 незапослена док је 1 обављао привремене послове. Дакле само 2 запослена испитаника су свој економски статус оценила позитивно – као добар, док су га преостала 2 описала као лош. Исо тако, 1 испитаник који је обављао привремене послове, оценио је свој економски статус као осредњи, док је 1 који је такође обављао те послове и 2 који су обављали повремене послове, свој економски статус у време регрутације оценили као лош. Наведени подаци показују да је међу жртвана трговине људима, које су обухваћене овим узорком, највише било лица која су незапослена и која су истовремено свој економски статус описала као лош. Али, ако се узме у обзир податак да су они испитаници који су у моменту врбовања били запослени као своја радна места навели продавницу, кафић и кладионицу и ако се познају услови рада и висине зараде запослених на тим местима, може се разумети због чега половина њих није била задовољна својим економским статусом, упркос поседовању каквог-таквог запослења.

Од 50 испитаника, њих 4 (8%) навело је да су врбовани на радном месту, њих 11 (22%) навело је да су врбовани у сопственој кући, један испитаник (2%) врбован је на одмору, а 34 испитаника (68%) на другом јавном месту. Наведени подаци говоре да је најучесталије врбовање жртава на јавним местима која се могу описати као „друга јавна места“, односно на местима која нису: радно место, сопствена кућа жртве или место где се она налази на одмору.

Од укупно 4 испитаника који су врбовани на радном месту, у 3 случаја се радило о врбовању у сврху сексуалне експлоатације, док је у једном случају испитаник на радном месту врбован истовремено у сврху сексуалне и радне експлоатације. Од укупно 11 случајева врбовања у сопственој кући, 4 су била учињена у сврху сексуалне експлоатације, 3 у сврху принуде на закључење брака и 4 ради принуде на просјачење. Испитаник који је био на одмору врбован је у циљу радне експлоатације. Када су у питању врбовања учињена на другим јавним местима, у 23 случаја се радило о врбовању у сврху сексуалне експлоатације, у 4 случаја је у питању било врбовање у сврху радне експлоатације, у 2 случаја ради принуде на закључење брака, у 2 случаја ради принуде на просјачење и у 2 случаја ради принуде на вршење кривичних дела.

Када је у питању тип експлоатације треба нагласити да је на испитиваном узорку сексуално врбовање ради сексуалне експлоатације у највећем броју случајева учињено на другом јавном месту (34 случаја), затим у сопственој кући жртве (у 11 случајеве), а на радном месту у 4 случаја. Врбовање у сврху радне експлоатације је у једном случају вршено док је жртва била на одмору, док је у другом случају, када је радна експлоатација комбинована са сексуалном, врбовање учињено на радном месту. Врбовање ради принуде на закључење брака, као и ради принуде на просјачење је спровођено у сопственој кући жртве и на другом јавном месту, а врбовање у циљу принуде на вршење других кривичних дела учињено је на другом јавном месту. Ако се узме у обзир место запослења које су жртве навеле као своје радно место у тренутку када је трафикер ступио у контакт са њима, потврђује се претпоставка да кафићи, кладионице, па и бутици представљају места која се већ традиционално сматрај подобним за врбовање, посебно у сврху сексуалне експлоатације, која је у 1 случају испитиваног узорка комбинована са радном експлоатацијом.

Највећи број испитаника није био у браку у тренутку када је трафикер ступио у контакт са њима. Међу испитаницима који су се изјаснили као неожењени/неудате били су присутни сви облици експлоатације, а највише је било случајева сексуалне експлоатације. Од укупно 42 испитаника који у тренутк када је трговац људима ступио у контакт са њима нису били у браку, њих 26 било је изложено сексуалној експлоатацији, 4 радној, 5 принуди на закључење брака, 6 принуди на просјачење, 3 принуди на вршење кривичних дела, а у 1 случају је дошло до прекида у фази врбовања. Од 3 испитаника који су били ожењени/удати у моменту када је трговац људима ступио у контакт са њима, 2 су била изложена радној експлоатацији, а 1 сексуалној. Сва три испитаника који су били разведени, били су изложени сексуалној експлоатацији. Испитаник који је био удовац/удовица био је изложен сексуалној експлоатацији. Испитаник који је изјавио да је у тренутку врбовања живео у ванбрачној заједници, био је изложен принуди на просјачење. Дакле, наведени подаци показју да је најчешћи случај да жртве које нису у браку буду подвргнуте сексуалној експлоатацији.

У тренутку врбовања, највећи број испитаника живео је код родитеља – њих 27, односно 54%. У изнајмљеном стану живело је 12 испитаника (24%), 6 испитаника (12%) живело је у привременом боравишту које им је обезбедила Влада Републике Србије, а у свом стану је живело 5 испитаника (10%). Наведени подаци показују да су у испитаном узорку били најзаступљенији испитаници који су у тренутку врбовања становали код родитеља. Од 27 испитаника који су у тренутку врбовања живели код родитеља, 2 су врбована на свом радном месту, 7 испитаника врбовано је у сопственој кући,а 18 на другом радном месту. Свих 6 испитаника смештених у привременом боравишту које им је обезбедила Влада Републике Србије, изјавили су да су врбовани на другом јавном месту. Од 12 испитаника који су у тренутку када је трафикер ступио у контакт са њима живели у изнајмљеном стану, 2 су врбована на радном месту, 2 су врбована у сопственој кући, а 8 на другом јавном месту. Од 5 испитаника који су у моменту врбовања живели у свом стану, 2 су врбована у сопственој кући, 1 на одмору, а 1 на другом јавном месту. Анализирани подаци показују да је међу жртвама трговине људима, из испитаног узорка, највише оних које су у тренутку врбовања живеле код родитеља и које су врбоване на неком јавном месту, дакле, изван сопственог дома.

Од укупно 50 испитаника, њих 38 (76%) изјавило је да је трговац људима први контакт са њима остварио лично. У 8 случајева (16%) први контакт је остварен преко познаника, у 1 случају (2%) путем мобилног телефона, у 1 случају (2%) путем интернета, а у 1 случају (2%) на други начин, тачније, путем огласа. Дакле, најзаступљенији начин успостављања првог контакта са жртвама из испитаног узорка био је личним путем, без употребе информационо-комуникационих технологија.

Сабирањем укупног броја контаката који су остварени лично (38) и преко посредника (8), може се закључити да је у 46 случајева први контакт са жртвом остварен без употребе било какве информационо-комуникационе технологије. Путем интернета, први контак остварен је у 1 случају, а исто се односи и на мобилни телефон. Није познато на који начин је објављен оглас, путем којег је дошло до првог контакта у једном случају, те није познато да ли је и ту можда употребљен интернет или су у питању „класични“ огласи објављени у новинама.

Од 38 испитаника који су први контакт са трговцем људима остварили лично, њих 18 је у том тренутку становало код родитеља, њих 6 је становало у привременом боравишту које им је обезбедила Влада Републике Србије, њих 11 је живело у изнајмљеном стану, а 3 у свом стану. Дакле, највећи број испитаника који су први конткакт са трафикером остварили лично, живео је код родитеља у тренутку врбовања. Свих 8 испитаника који су први контакт са трговцем људима остварили преко познаника, у тренутку врбовања живели су код родитеља. Испитаник са којим је трговац људима остварио први контакт путем мобилног телефона живео је у тренутку врбовања у свом стану. Испитаник са којим је трговац људима први контакт остварио путем интернета живео је у тренутку врбовања код родитеља. Испитаник са којим је трговац људима први пут ступио у контакт путем огласа, живео је у том тренутку у свом стану. Од испитаника који су у тренутку врбовања били смештени код родитеља, њих 18 (66,67%) је први контакт са трафикером остварило лично, њих 8 (29,63%) преко познаника, а у 1 случају је контакт остварен путем интернета. Свих 6 испитаника, који су у тренутку врбовања боравили у привременом смештају који им је обезбедила Влада Републике Србије, остварило је први контакт са трговцем људима лично. Од 12 испитаника који су у тренутку

врбовања живели у изнајмљеном стану, са њих 11 је трговац људима први пут ступио у контакт лично, док је само са једним први контакт остварен путем мобилног телефона. Од 4 испитаника који су у тренутку врбовања живели у свом стану, њих 3 је први контакт са трговцем људима остварило лично, док је само један први контакт остварен путем огласа. Анализирани подаци показују да су трафикери у највећем броју случајева личним путем контактирали оне жртве које су у тренутку врбовања живеле у изнајмљеном стану, па затим оне које су у том тренутку живеле код родитеља.

Мали проценат испитаника је изјавио да говори неки страни језик тачније, само њих 7, а 41 испитаник је изјавио је да не говори ни један страни језик, док у 2 случаја нема уноса. Од 38 испитаника са којима је трговац људима први контакт остварио лично, њих 4 говори неки страни језик, а њих 33 не говори страни језик. Од испитаника који су први контакт са трговцем остварили преко познаника, 2 говоре страни језик, а 6 не говоре. Испитаник са којим је трафикер први контакт остварио путем мобилног телефона не говори страни језик. Испитаник са којим је трговац људима први контакт остварио путем интернета такође је изјавио да не говори ни један страни језик. Помало је изненађујуће што испитаник користи интернет, а не говори ни један страни језик, будући да је за употребу овог облика информационо-комуникационих технологија потребно барем елементарно познавање енглеског језиак. Са друге стране, могуће је претпоставити да се сналази на интернету, а да ипак не говори страни језик у смислу да не зна да га користи у свакодневној комуникацији. У сваком случају, може се приметити да су у оба случаја када су информационо-комуникационе технологије употребљене за остваривање првог контакта, у питању биле жртве које не говоре стране језике, што показује да, макар на овом узорку, познавање страних језика није представљало предуслов за виктимизацију путем злоупотребе информационо-комуникационих технологија. Са испитаницима који говоре страни језик трговци су, у највећем броју случајева, остварили први пут контакт лично, а затим преко посредника, док је у 1 случају до контакта дошло путем огласа.

Упоређивањем начина на који је трговац људима остварио први контакт са жртвом са податком о томе да ли жртва користи друштвене мреже или не и да ли и на којој од њих има отворен налог може показати да ли и у колико случајева су друштвене мреже послужиле као средство за врбовање жртава трговине људима. Од укупно 38 испитаника који су први контакт са трговцем људима остварили лично, њих 20 користи друштвене мреже. Од тога 14 испитаника има налог на *Facebook-у*, 1 испитаник има налог на *Twitter-у,* а 5 испитаника користе друштвене мреже, али немају свој налог ни на једној. Свих 8 испитаника, са којима је трговац људима први контакт остварио преко познаника, користе друштвене мреже и свих 8 имају налог на *Facebook-у.* Испитаник са којим је трговац људима први контакт остварио путем интернета користи друштвене мреже и има налог на *Facebook-у.* Испитаник са којим је трговац људима први контакт остварио путем огласа не користи друштвене мреже.

Ови подаци показују да је, иако укупно 23 испитаника има налог на *Facebook-у* а 1 на Twitter-у, први контакт са трафикером у највећем броју случајева остварен лично или преко познаника. Управо су лица која су имала налог на Facebook-у и *Twitter-у* остварила тај контакт лично, односно преко посредника. То показује да, упркос поседовању налога на друштвеним мрежама трговац људима ипак није одабрао тај начин за ступање у први конатакт са њима. Само један испитаник, са

којим је трговац људима први контакт остварио путем интернета, користи друштвене мреже и има налог на *Facebook-y*, што указује на могућност да је *Facebook* том приликом злоупотребљен у сврху вербовања жртава трговине људима.

Од укупно 38 испитаника са којима је трговац људима ступио у први контакт лично, њих 6 је узраста од 6-14 година, њих 5 је узраста од 15 до 16 година, њих 7 је узраста од 17 до 18 година, 17 испитаника има између 19 и 33 године, а 3 испитаника имају између 34 и 49 година. Од испитаника са којима је трговац људима ступио у први контакт преко посредника, 2 имају између 17 и 18 година, а 6 између 19 и 33 године. Испитаник са којим је трговац људима први контакт остварио лично има између 50 и 65 година. Испитаник са којим је трговац људима први контакт остварио путем мобилног телефона има између 19 и 33 године. Испитаник са којим је трговац људима први контакт остварио путем интернета има између 17 и 18 година. Осим једног малолетног испитаника, са којим је први контакт остварен путем интернета, са свим осталим малолетним испитаницима је трговац људима први контакт остварио лично односно преко посредника. Међу пунолетним испитаницима заступљени су сви наведени начини остваривања контакта осим путем интернета. Од укупно 38 испитаника, са којима је трговац људима први контакт остварио лично, њих 29 живи у урбаној средини, а њих 9 у руралној средини. Од укупно 8 испитаника са којима је трговац људима први контакт остварио преко познаника, њих 7 живи у урбаној средина, а само 1 у руралној. Испитаник са којим је трговац људима први контакт остварио путем огласа живи у урбаном подручју. Испитаник са којим је трговац људима први контакт остварио путем мобилног телефона живи у руралном подручју. Испитаник са којим је трговац људима први контакт остварио путем интернета живи у урбаном подручју.

Приступ информационо-комуникационим технологијама у тренутку вербовања показује да ли је и у коликој мери могућност да се лако, једноставно и брзо приступи овом виду комуникације допринела виктимизацији неког лица. Приликом одговарања на питање „да ли сте у тренутку када је трговац људима ступио у контакт са Вама имали приступ информационо-комуникационим технологијама?“ испитаници су могли да се определе за већи број опција. Прикупљени подаци показују да је највећи број испитаника имао приступ информационо-комуникационим технологијама у тренутку вербовања. Укупно 30 испитаника (57%) имало је приступ од куће, 12 испитаника (23%) имало је приступ са другог места, а 3 испитаника (6%) имало је приступ и од куће и са другог места. Укупно 11 испитаника (20%) није имало приступ информационо-комуникационим технологијама у тренутку вербовања. Ипак, треба напоменути да је, упркос томе што је скоро 80% испитаника имало приступ информационо-комуникационим технологијама у тренутку вербовања (било од куће, било са неког другог места), први контакт трговца људима са њима у највећем броју случајева остварен лично или преко познаника, те да је информационо-комуникациона технологија у ту сврху злоупотребљена само у 2 случаја – у једном случају је то био мобилни телефон, а у другом случају интернет. Од 38 испитаника са којима је трговац људима први контакт остварио лично, њих 20 је имало приступ информационо-комуникационим технологијама од куће, њих 10 је имало приступ са другог места, а 2 су имала приступ и од куће и са другог места. Укупно 9 испитаника са којима је трговац људима први контакт остварио лично није имало приступ информационо-комуникационим технологијама. Од 8 испитаника са којима је трговац људима први контакт остварио преко познаника, њих 6 је имало

приступ информационо-комуникационим технологијама од куће, а 2 су имала тај приступ са другог места.

Испитаник са којим је први контак остварен путем мобилног телефона, имао је приступ од куће. Испитаник са којим је први контакт остварен путем огласа имао је приступ од куће. Испитаник са којим је први контакт остварен путем интернета имао је такође приступ од куће. Од укупно 29 испитаника који су имали приступ информационо-комуникационим технологијама од куће, њих 20 остварило је први контакт са трговцем људима лично, 6 преко посредника, а по 1 путем мобилног телефона, огласа и интернета. Од укупно 12 испитаника који су имали приступ информационо-комуникационим технологијама са другог места, са њих 10 је први контакт остварен лично а са 2 преко посредника. То показује да ниједан испитаник који је имао приступ информационо-комуникационим технологијама са другог места није остварио први контак са трафикером тим путем већ да је увек у питању био лични контакт – било директан било преко неког лица – познаника. Свих 9 испитаника који у тренутку вербовања нису имали приступ информационо-комуникационим технологијама остварили су први контакт са трговцем људима лично. Исто међутим важи и за оне испитаника који су у тренутку вербовања имали приступ информационо-комуникационим технологијама и од куће и са другог места.

Од укупно 27 испитаника који су имали приступ информационо-комуникационим технологијама од куће, 3 имају од 15 до 16 година, 5 имају од 17 до 18 година, 19 испитаника има од 19 до 33 године, 2 имају између 34 и 49 и 1 од 50 до 65. Од укупно 12 испитаника који су имали приступ информационо-комуникационим технологијама са другог места, 2 имају између 6 и 14 година, 1 има између 15 и 16, 3 између 17 и 18, а 6 испитаника има између 19 и 33 година. Од укупно 9 испитаника који у тренутку вербовања нису имали приступ информационо-комуникационим технологијама, 4 су имала између 6 и 14 година, 1 између 15 и 16, 1 између 17 и 18, 1 између 19 и 33 и 2 између 34 и 49. Један испитаник који је имао приступ информационо-комуникационим технологијама и од куће и са другог места имао је између 15 и 16, а други између 17 и 18 година. Ниједан испитаник, узраста од 6 до 14 година, није у тренутку вербовања имао приступ информационо-комуникационим технологијама од куће. Са другог места су од њих приступ имала 2 испитаника, а уопште нису имала приступ 4 испитаника. Од 5 испитаника узраста од 15 до 16 година 1 није имао приступ информационо-комуникационим технологијама, 1 је имао и од куће и са другог места, 1 је имао са другог места, а 3 од куће. Од 10 испитаника узраста од 17 до 18 година, 1 није имао приступ информационо-комуникационим технологијама, 1 је имао и од куће и са другог места, 3 су имала са другог места, а 5 од куће. Од 24 испитаника старости од 19 до 33 године, њих 19 је имало приступ информационо-комуникационим технологијама од куће, 6 са другог места, 1 уопште није имао приступ. Испитаник старости од 50 до 65 година имао је приступ информационо-комуникационим технологијама од куће.

Податак о томе којој информационо-комуникационој технологији је жртва имала приступ у време вербовања заправо сужава круг оних жртава које су могле бити злоупотребљене од стране трафикера. Наравно, треба имати на уму да је велика већина првих контаката са трафикером у овом узорку остварена лично или преко посредника, тако да податак о томе да ли је жртва имала приступ информационо- комуникационим технологијама у време вербовања не говори много о њиховој злоупотреби у сврху трговине људима у овом случају. Само фиксном

телефону су у време врбовања приступ имала 2 испитаника, и фиксном и мобилном телефону је приступ имало 8 испитаника, и фиксном телефону и мобилном телефону и интернету је приступ имало 9 испитаника, само мобилном телефону је приступ имало 19 испитаника, и мобилном телефону и интернету су приступ имала 3 испитаника. Када се посматра збирно, може се констатовати да је фиксном телефону приступ имало укупно 19 испитаника, да је мобилном телефону приступ имало укупно 39 испитаника, да је интернету имало приступ укупно 13 испитаника. Укупно 8 испитаника није унело податак о томе којој информационо-комуникационој технологији су имали приступ у време врбовања. Анализа наведених података показује да је најзаступљенија информационо-комуникациона технологија којој су имале приступ жртве трговине људима из овог узорка мобилни телефон (55% испитаника имало је приступ мобилном телефону), да је на другом месту по заступљености фиксни телефон (27% испитаника имало је приступ фиксном телефону), а на трећем интернет (18% испитаника имало је приступ интернету).

0д укупно 50 испитаника, 22 (44%) је изјвило да су у време врбовања користили друштвене мреже. Са друге стране, 26 испитаника (52%) изјавило је да у време врбовања нису користили друштвене мреже. Два испитаника нису унела одговор на ово питање. Наведени подаци немају статистичку значајност у смислу процене да ли су жртве трговине људима, које су укључене у овај узорак, склоне да користе друштвене мреже у време врбовања, будући да је однос оних који су их користили за свега неколико процената нижи од оних које нису. То треба имати у виду приликом анализирања свих осталих података у вези са злоупотребом овог облика информационо-комуникационих технологија за врбовање жртава трговине људима као и за одржавање контакта са њима. У време врбовања, 22 испитаника (73%) су имала налог на *Facebook-y*, 3 испитаника (10%) су имала налог на *Twitter-y*, док њих 5 није имало налог ни на једној друштвеној мрежи. Наведени подаци показују да су међу оним жртвама које су имале налог на некој друштвеној мрежи најзаступљенији корисници *Facebook-a*.

Упоређивање да ли и које друштвене мреже користе жртве трговине људима, ирегулани мигранти и азиланти, може показати колика вероватноћа постоји међу припадницима ове три категорије да ће такав облик информационо-комуникационих технологија бити злоупотребљен у сврху њихових илегалних миграција. Подразумева се да употреба друштвених мрежа не искључује могућност да до илегалних миграција ових категорија становништва дође и посредством неких других информационо-комуникационих технологија или употребом неких других средстава. Ипак, њихово коришћење може у знатној мери олакшати комуникацију, размену информација између, на пример, трафикера и жртве трговине људима или ирегуларних миграната односно азиланата са лицима која им помажу приликом илегалних миграција.

Када су у питању жртве трговине људима, улога друштвених мрежа је важна и током самог процеса врбовања жртава, будући да на тај начин трафикер може остварити први контакт са њима и даље наставити одржавање тог контакта. Такође, преко друштвених мрежа је могуће „рекламирање“, односно оглашавање послова које обављају жртве трговине људима и нуђење услуга, нарочито када је у питању сексуална експлоатација, али и радна експлоатација, као и експлоатација ради продаје органа. Упоређивањем процента оних испитаника који користе друштвене мреже у свакој од наведених категорија, може се закључити да су на друштвеним мрежама најактивнији азиланти, затим следе ирегуларни мигранти, па тек онда

жртве трговине људима. Од 52 азиланта, њих 46 (88,46%) користи друштвене мреже, а њих 6 (11,54%) не користи, од 91 ирегуларног мигранта, њих 54 (59,34%) користи друштвене мреже, а њих 37 (40,66%) не користи, од 48 жртава трговине људима, 22 (45,83%) користе друштвене мреже, а 26 (54,17%) не користе. Када се саберу испитаници из све три категорије (жртве трговине људима, ирегуларни мигранти и азиланти) може се видети да је и свеукупно посматрано већи број оних испитаника који користе друштвене мреже него оних који их не користе. Тачније, од укупно 187 испитаника који су у све три категорије одговорили на ово питање, 124 испитаника (66,31%) користи друштвене мреже, док их 63 (33,69%) не користи. Анализирани подаци показују да је заступљеност корисника друштвених мрежа међу азилантима већа него што је то случај са жртвама трговине људима, као и да је заступљеност корисника друштвених мрежа међу азилантима већа него што је то случај са ирегуларним мигрантима. Дакле, азиланти су склонији да користе друштвене мреже него жртве трговине људима и ирегуларни мигранти.

И начин на који је трговац људима одржавао контакт са жртвом може показати у којој мери је злоупотреба информационо-комуникационих технологија допринела виктимизацији, исто као што је то случај са начином остваривања првог контакта између жртве и тргова људима. У случају испитаника из овог узорка комуникација се одвијала на неколико начина: лично, преко посредника, путем мобилног телефона и путем интернета. Искључиво личним путем комуникација се одвијала у 21 случају (42%), и лично и путем мобилног телефона се одвијала у 17 случајева (38%). Трговац је одржавао контакт са жртвом и лично и путем мобилног телефона и путем интернета само у 1 случају (2%) и у питању је био случај сексуалне експлоатације. Одржавање контакта са жртвом искључиво путем мобилног телефона било је присутно у 5 случајева (10%), искључиво путем интернета, контакт је одржаван само у 2 случаја (4%), а контакт је преко посредника одржаван само у 1 случају (2%). Један испитаник није унео податак о томе на који начин је трафикер одржавао контакт са њим.

Пошто је у неколико случајева контакт са жртвом одржаван комбиновањем неколико средстава комуникације, потребно је сагледати и колико је укупно коришћена свака информационо-комуникациона технологија или други начин комуницирања. Највећи број контаката са жртвом, чак 41 (58%), одржаван је лично, мобилни телефон је коришћен укупно у 25 случајева (35%), путем интернета је контакт одржаван укупно у 3 случаја (4%), док је контакт преко посредника одржаван само у 1 случају. Наведени подаци показују да је, као и у случајевима врбовања жртава трговине људима, односно остваривања првог контакта трафикера са жртвом, лични контакт најзаступљенији начин на који је трговац одржавао контакт са жртвом. Контакт трафикера са жртвом одржаван је лично у укупно 41 случају (58%), с тим што је у 17 случајева лични контакт комбинован са употребом мобилног телефона, док је у 1 случају лични контакт комбинован са комуникацијом путем мобилног телефона и путем интернета.

Мобилни телефон као средство за одржавање контакта трафикера са жртвом коришћен је у укупно 25 случајева, с тим што је у 17 случајева он комбинован са личним контактом, а у 1 случају са личним контактом и контактом путем интернета. Интернет је као средство одржавања контакта између трговца људима и жртве коришћен у укупно 3 случаја. Од тога је у 1 случају комбинован са личним контактом и контактом путем мобилног телефона. Преко посредника је контакт одржаван само

у 1 случају и тај начин одржавања контакта није комбинован ни са једним другим начином.

Од 41 случаја, где је контакт одржаван лично (било искључиво лично, било у комбинацији са мобилним телефоном и интернетом) , 25 случајева спада у сексуалну експлоатацију, 5 у радну експлоатацију, 4 случаја су принуда на закључење брака, у 6 случајева се радило о принуди на просјачење, у 2 случаја о принуди на вршење кривичних дела, а у 1 случају је у питању прекид у фази врбовања. Од 25 случајева када је коришћен мобилни телефон (било у комбинацији са личним контактом било са интернетом), 18 случајева спада у сексуалну експлоатацију, 2 спадају у радну експлоатацију, 2 случаја су била принуда на закључење брака, 2 принуда на просјачење, 1 принуда на вршење кривичних дела, а у једном је дошло до прекида у фази врбовања.

Од 3 случаја где је за одржавање контакта коришћен интернет, 2 случаја су спадала у сексуалну експлоатацију, а 1 је принуда на закључење брака. У 1 случају сексуалне експлоатације интернет је коришћен као једини начин за одржавање контакта трафикера са жртвом, док је у другом коришћен у комбинацији са личним контакотом и мобилним телефоном. У случају где је интернет коришћен за одржавање контакта трафикера са жртвом ради принуде на закључење брака, то је уједно био и једини начин одржавања контакта. Један случај где је контакт одржаван преко посредника био је случај радне експлоатације. У случајевима сексуалне експлоатације је у највећем броју случајева за одржавање контакта коришћен лични контакт (25), а затим мобилни телефон (18). Путем интернета је за сврху сексуалне експлоатације контакт одржаван само у 2 случаја. Када је у питању радна експлоатација, најзаступљенији начин одржавања контакта трафикера са жртвом је био лични контакт (5 случајева), затим контакт путем мобилног телефона (2 случаја), а у 1 случају је контакт одржаван преко посредника. Приликом принуде на закључење брака, контакт је лично одржаван у 4 случаја, мобилни телефон је коришћен у 2 случаја, а контакт је одржаван путем интернета само у 1 случају. У случајевима принуда на вршење кривичних дела, контакт је одржаван лично у 2 ситуације, а у 1 је коришћен мобилни телефон. У случају где је дошло до прекида у фази врбовања, контакт је одржаван лично и путем мобилног телефона.

Може се уочити да је одржавање контакта са жртвом личним путем, као и путем мобилног телефона, било присутно код сваког типа трговине људима, односно код сваког типа експлоатације, с тим што су, као што је већ наведено, у неким случајевима ови начини примењивани као једини начини одржавања контакта са жртвом, док су у неким другим комбиновани међусобно, односно са интернетом.

Остваривање увида у то какво је мишљење жртава трговине људима о ризицима коришћења информационо-комуникационих технологија и о могућностима превенције трговине људима, треба да омогући да се процени да ли је потребна едукација грађана о томе и да ли би, да су биле едуковане о наведеним ризицима жртве могле да избегну виктимизацију. На питање да ли мисле да су упознати са ризицима које са собом носи употреба информационо-комуникационих технологија, 24 испитаника (48%) кажу да јесу, док је 26 испитаника (52%) одговорило да нису.

9. АНАЛИЗА ПОДАТАКА ПРИКУПЉЕНИХ ОД ДРЖАВНИХ ОРГАНА И НЕВЛАДИНИХ ОРГАНИЗАЦИЈА

Интервјуом је обухваћено укупно 40 испитаника који су запослени у државним институцијама и невладиним организацијама у Републици Србији, који се у свом раду сусрећу са случајевима трговине људима. Подаци су обрађени у програмима Microsoft Office Excel и Statistical Package for the Social Sciences (SPSS).

Укупно 5 испитаника интервјуисано је у Панчеву, 5 у Београду, 3 у Прокупљу, 3 у Зрењанину, 3 у Нишу, 2 у Крагујевцу, док је по 1 испитаник интервјуисан у Новом Пазару, Лесковцу, Врању, Димитровграду, Јагодини, Кикинди, Краљеву, Ужицу, Ваљеву, Сомбору, Крушевцу, Долову, Новом Саду, Пироту и Сремској Митровици. Један испитаник је на пољу предвиђеном за унос података о месту интервјуисања навео Црвени крст Србије, док код једног испитаника није унет податак о месту интервјуисања. Од укупно 40 испитаника, који су обухваћени овим истраживањем, њих 33 су запослени у владином сектору, 2 испитаника су запослена у невладином сектору, а 3 испитаника нису унели податке о сектору где су запослени. Од 40 испитаника, 3 раде за Министарство унутрашњих послова Републике Србије, у полицијским управама ради 24 испитаника и то 5 у Панчеву, 3 у Прокупљу, 3 у Зрењанину и по 1 у Крагујевцу, Сремској Митровици, Лесковцу, Врању, Нишу, Јагодини, Прокупљу, Кикинди, Краљеву, Ужицу, Сомбору, Крушевцу, Пироту и Новом Саду. За 2 испитаника није унет податак о организацији у којој ради.

Као одговор на питање о природи поступања испитаника, односно својству или карактеру радњи које он предузима у односу на жртве и учиниоце кривичног дела трговине људима, испитаници су могли да заокруже неколико опција: откривање учинилаца кривичних дела, превентивно деловање или хуманитарно деловање. Искључиво откривањем учинилаца кривичних дела бави се 10 испитаника, искључиво хуманитарним деловањем бави се 5 испитаника, док се само превентивним деловањем не бави ни један од испитаника. Превентивно деловање јавља се само у комбинацији са хуманитарним (у 3 случаја) и у комбинацији са откривањем учинилаца кривичних дела (у 4 случаја). И превентивно и хуманитарно и у циљу откривања учинилаца кривичних дела делује највећи број испитаника – њих 13 (односно, 34, 21% од укупног броја испитаника).

Када се саберу испитаници који делују у сваком од наведених својстава, види се да је највише оних који поступају са циљем откривања учинилаца кривичних дела (укупно 30 испитаника или 75%), затим оних који делују хуманитарно (укупно 24 испитаника или приближно 60%) и, на крају, оних који делују превентивно (укупно 20 испитаника или 50%). Према сазнањима државних органа и невладиних организација, учиниоци кривичног дела трговине људима су у највећем броју случајева из праксе користили неку од информационо-комуникационих технологија у некој од фаза извршења тог кривичног дела. Од укупно 40 испитаника, њих 36 (94,74%) изјавило је да су трговци људима користили неку од информационо-комуникационих технологија у некој од фази извршења кривичног дела трговине људима, док су само 2 испитаника (5,26%) изјавила да трговци људима том приликом нису користили информационо-комуникационе технологије.

Када је у питању облик информационо-комуникационих технологије које је трговац људима користио у некој од фази извршења тог кривичног дела, према сазнањима представника државног и невладиног сектора, у 16 случјева је коришћен само мобилни телефон, док је у 2 случаја коришћен само рачунар. У 16 случајева коришћени су и мобилни телефон и рачунар, у 1 случају коришћен је мобилни телефон и неки други начин комуниакције, док су у 1 случају коришћени и мобилни телефон и рачунар и неки други начин комуникације. Два испитаника нису одговорила на ово питање. Када се саберу сви случајеви у којима је коришћена нека од информационо-комуникационих технологија, било као једино средство, било у комбинацији са неким другим средством комуникације, може се видети да је мобилни телефон коришћен у највећем броју случајева – укупно 36 (од тога, у 16 случајева самостално, у 16 случајева у комбинацији са рачунаром, у 1 случају у комбинацији са рачунаром и другим начином, у 1 случају у комбинацији са другим начином), док је рачунар коришћен у 20 случајева, с тим што је од тога само у 2 случаја коришћен самостално, док је у 16 случајева коришћен у комбинацији са мобилним телефоном, а у 1 случају у комбинацији са мобилним телефоном и неким другим начином комуникације.

Када су у питању конкретни канали који су били употребљавани за комуникацију трговца људима са жртвом, а који спадају у савремене информационо-комуникационе технологије, испитаници су навели: друштвене мреже (*Facebook, Twitter, LinkedIn*...), *Skype*, *Viber*, е-пошту, али и интернет уопште и мобилни телефон. При томе су испитаници могли да се определе за више од једног одговора, што значи да наведени канали комуникације нису увек употребљавани као једини начин за остваривање контакта, већ некада самостално, а некада међусобно комбиновани. Као конкретни начин комуникације, 32 испитаника навело је интернет, али без прецизирања о ком облику комуникације на интернету се ради, а 31 испитаник навео је мобилни телефон. Друштвене мреже је навело укупно 16 испитаника, *Skype* њих 9, *Viber* 3, е-пошту 11. Укупно 5 испитаника није унело одговор на ово питање.Према сазнањима испитаника, у 26 случајева је одговор на питање да ли жртве трговине људима користе друштвене мреже био позитиван. У 4 случаја испитаници нису одговорили на ово питање.

Када су у питању друштвене мреже на којима су према сазнањима испитаника активни трговци људима из случајева са којима су се сусретали у свом досадашњем раду, као могући одговори били су понуђени: *Facebook, Twitter, Линкедлн, Google+, Фоурсqуаре* и друге. Као опција била је понуђена констатација да трговци људима са којима су се сусретали у случајевима на којима раде немају налог ни на једној друштвеној мрежи. Само је *Facebook* наведен у 14 случајева, *Facebook* и *Twitter* у 6 случајева, *Facebook* и *Google+* у 3 случаја, *Facebook* и друга друштвена мрежа у 1 случају. У 1 случају наведено је да су трговци људима користили *Facebook*, али да нису имали свој налог ни на једној друштвеној мрежи. У 1 случају наведено је да испитаник нема сазнања о томе да ли су трговци људима поседовали налог на друштвеним мрежама. Укупно 11 испитаника пропустило је да одговори на ово питање.

Било да их користе самостално или у комбинацији са неком другом друштвеном мрежом, према сазнањима испитаника, трговци људима су најактивнији на следећим друштвеним мрежама: на *Facebook-y* (у 27 случајева), на *Twitter-y* (у 6 случајева) и на *Google+* (3 случаја). Као што је већ истакнуто, у 1 случају је наведено да су трговци људима користили друге друштвене мреже, док је у

2 случаја наведено да трговац људима није имао налог ни на једној друштвеној мрежи. Иако су као друштвене мреже били понуђени и *LinkedIn* и *Фоурсqуаре*, ниједан испитаник није навео да су трговци људима користили било коју од те 2 друштвене мреже.

Ипак, чињеница да су трговци људима активни на некој од друштвених мрежа не значи сама по себи да су они те друштвене мреже увек и у сваком случају злоупотребљавали у сврху вербовања жртава или одржавања контакта са њима. Због тога су испитаници посебно упитани „да ли имају сазнања о томе да ли су учиниоци кривичног дела трговина људима на чијим су случајевима радили, користили рачунар или мобилни телефон у некој од фаза извршења кривичног дела трговина људима".

Од укупно 40 испитаника, 31 је одговорио да су, према његовим сазнањима, у некој од фази извршења кривичног дела трговине људима трговци користили рачунар или мобилни телефон. Насупрот томе, само 2 испитаника одговорила су да према њиховим сазнањима ни рачунар ни мобилни телефон нису коришћени од стране трафикера приликом извршења овог кривичног дела. Укупно 5 испитаника није одговорило на ово питање. Испитаницима је постављено питање „да ли је и у колико мери према њиховим сазнањима употреба рачунара, односно мобилног телефона помогла трговцу људима приликом успостављања и одржавања контакта са жртвом, као и у одржавању контакта и размени информација са другим трговцима људима". Као могући одговори на ово питање били су наведени: "није му помогло", "веома мало", "доста му је помогло" и "није ми познато".

Испитаницима је такође постављено питање о фази трговине људима у којој је према њиховим сазнањима коришћен рачунар или мобилни телефом. Као могући договори били су понуђени: у фази вербовања, у фази експлоатације и у фази превожења. Било је могуће заокружити више од једног одговора. У највећем броју случајева, одговор испитаника је био да је рачунар или мобилни телефон коришћен у свим фазама трговине људима (укупно 16 испитаника или 42,11%). Укупно 8 испитаника (21,4 %) навело је да су рачунар или мобилни телефон коришћени само у фази вербовања, а 2 испитаника (5,26%) су навела да су рачунар или мобилни телефон коришћени само у фази експлоатације. Укупно 2 испитаника (5,26%) су навела да су рачунар или мобилни телефон коришћени у фази вербовања и у фази експлоатације, а 2 (5,26%) да су рачунар или мобилни телефон коришћени у фази вербовања и у фази превожења.

Испитан је и став представника државних органа и невладиних организација о томе да ли би трговци људима успели да ступе у контакт са својим жртвама без помоћи рачунара или мобилног телефона. Као одговори били су понуђени „да", „не" и „можда". Од укупно 38 испитаника који су одговорили на ово питање, њих 19 (50%) навело је да сматрају да би трговци људима успели да ступе у контакт са својим жртвама и без употребе информационо-комуникационих технологија као што су мобилни телефон и рачунар. Са друге стране, 4 испитаника (10,53%) истакла су да сматрају да трговци у томе не би успели без рачунара или мобилног телефона. За опцију „можда" определило се укупно 15 испитаника (39,47%).

Када је у питању заступљеност случајева коришћења мобилних телефона или рачунара на јавним местима (кафе, парк, шопинг-центар, трг или друго јавно место) у циљу вербовања жртве у досадашњој пракси испитаника, њих 18 (47,37%) одговорило је да су ове информационо-комуникационе технологије коришћене на

наведеним местима у сврху врбовања, њих 6 (15,79%) је одговорило да нису, док је њих 14 (36,84%) одговорило да им није познато да ли јесу или нису.

Када је у питању начин на који је трафикер одржавао контакт са жртвом, као могући одговори били су понуђени следећи начини: лично, путем фиксног телефона, путем мобилног телефона, путем интернета, преко посредника и на други начин. У 7 случајева наведено је да је трафикер одржавао контакт са жртвом искључиво личним путем. Такође у 7 случајева је наведено да је трафикер одржавао контакт са жртвом искључиво путем мобилног телефона. У 1 случају је наведено да је трафикер одржавао контакт са жртвом искључиво преко посредника. Одржавање контакта и лично и путем мобилног телефона било је наведено од стране 7 испитаника, у по 1 случају наведено је комбиновање личног контакта и контакта преко посредника, комбиновање контакта путем мобилног телефона и путем посредника и комбиновање контакта путем мобилног телефона и путем интернета. Укупно 5 испитаника навели су да су трафикери одржавали контакт са жртвама лично, путем мобилног телефона и преко посредника, у 2 случаја да су то чинили лично, путем мобилног телефона и путем интернета, а у 1 лично путем фиксног и мобилног телефона. Укупно 3 испитаника навела су да је трафикер одржавао контакт са жртвом лично, путем мобилног телефона, путем интернета, преко посредника. Један испитаник навео је да је трафикер одржавао контакт са жртвом лично, путем фиксног телефона, путем мобилног телефона, путем интернет и преко посредника.

Када се саберу сви случајеви употребе појединих облика одржавања контакта између трговца људима и жртве, може се приметити да су лични контакт и контакт путем мобилног телефона најзаступљенији. Контакт путем мобилних телефона наведен је, било као самосталан било у комбинацији са другим видовима комуникације у 30 случајева, а лични у 29 случајева. Контакт преко посредника, било самостално било у комбинацији са другим облицима комуникације, био је наведен 13 пута, контакт путем интернета 8 пута и контакт путем фиксног телефона 3 пута.

Мишљење представника државних органа и невладиних организација о томе да ли су жртве трговине људима упознате са ризицима употребе информационо-комуникационих технологија може указивати на то да ли је потребно спроводити едукацију грађана о тој проблематици – било да је у питању општа јавност, било да су у питању посебне циљне групе, као што су лица која су услед неког разлога изложена посебно великом ризику од виктимизације. Мишљење 25 испитаника, представника државних органа и невладиних организација јеста да грађани нису упознати са ризицима које са собом носи употреба информационо-комуникационих технологија, док њих 13 мисли да јесу. Дакле, запослени који су били укључени у овај узарак у већини случајева мисле да грађани нису у довољној мери упознати са наведеним ризицима, те би било оправдано размотрити какви модалитети едукације грађана стоје на располагању представницима државног и цивилног сектора и који облици сарадње би у том смислу дошли у обзир.

10. УПОРЕЂИВАЊЕ ПОДАТАКА ИЗ УПИТНИКА ЗА ЖРТВЕ ТРГОВИНЕ ЉУДИМА СА ПОДАЦИМА ИЗ УПИТНИКА КОЈИ СЕ ОДНОСЕ НА ИРЕГУЛАРНЕ МИГРАНТЕ, АЗИЛАНТЕ И ТРГОВЦЕ ЉУДИМА

10.1 Знање коришћења рачунара (жртве трговине људима, ирегуларни мигранти, азиланти)

Од 49 жртава трговине људима које су одговориле на питање о знању употребе рачунара, њих 27 одговорило је потврдно, а 22 су одговориле одрично. Од 44 ирегуларна мигранта, 24 је одговорило да зна да користи рачунар, а 20 да не зна. Од 53 азиланта, њих 44 је одговорило да зна да користи рачунар, а њих 9 да не зна.

Из наведеног се може уочити да је најмањи број оних који не знају да користе рачунар присутан код азиланата, док је број жртава трговине људима и ирегуларних миграната који знају да користе рачунар знатно мањи, како у апсолутном износу (27 жртава и 24 мигранта), тако и у односу на укупан број припадника тих категорија (нешто више од 50%). Такав однос између ове три категорије показује да је код азиланата већа вероватноћа да ће злоупотребити информационо-комуникационе технологије у сврху илегалних миграција него што је то код ирегуларних миграната, односно у случају жртава трговине људима – вероватноћа да ће бити врбоване или експлоатисане злоупотребом информационо-комуникационих технологија од стране трговца људима.

У том смислу, веома је значајно препознати ову категорију као могуће будуће категорије извршилаца различитих врста кривичних дела ВТК, нпр. КД из чл. 304 и 304а, односно као субјекте криминалистичке контроле у будућности. Значајно је такође то предвидети у будућим поступањима припадника униформисане и криминалистичке полиције у вези са азилантским центрима, али и у облицима сарадње са центрима за социјални рад и радницима одређених институција у овим центрима.

Од 50 испитаника жртава трговине људима, њих 27 користи интернет, а њих 23 не користи интернет, од 91 испитаника ирегуларних миграната, њих 54 користи интернет, а њих 37 не, од 53 испитаника – азиланта, њих 47 користи интернет, а њих 6 не користи интернет. Највећи проценат испитаника који користе интернет налази се међу азилантима – чак 47 азиланата од 53, односно 88,68% испитаних азиланата користи интернет док га њих 6 (11,32%) не користи. На другом месту су ирегуларни мигранти – од 91 испитаника њих 54 (59,34%) користи интернет, а њих 37 (40,66%) га не користи. На крају, најмањи број испитаника који користе интернет налази се међу жртвама трговине људима – њих 27 користи интернет (54%), а њих 23 га не користи (46%).

У смислу деловања полицијских службеника у овој области неопходно је препознати ову категорију лица као објективно најагилнију у погледу предузимања појединих незаконитих радњи, а посебно могуће везе са кривичним делима из области ВТК. Такође их можемо посебно апострофирати као групу од значаја за

безбедносно покривање, односно од интереса за службу. У том смислу они би били предмет криминалистичке контроле, али вероватно и обраде.

У сваком случају, и међу жртвама трговине људима, и међу ирегуларним мигрантима, и међу азилантима већи је број оних испитаника који користе интернет него оних који га не користе. Статистички је значајан однос између броја жртава трговине људима које користе интернет и азиланата који користе интернет, као и однос између ирегуларних миграната који користе интернет и азиланата који користе интернет. Први однос показује да су корисници интернета знатно заступљенији међу азилантима него међу жртвама трговине људима. Други однос показује да су корисници интернета знатно заступљенији међу азилантима него међу ирегуларним мигрантима.

У том смислу ово је добра смерница и за даље поступање припадника полиције према овим категоријама лица и за осмишљавање даљих стратегија у поступању са њима, односно увезивање напора различитих државних органа у проактивном поступању у овој области, али и у вези са ВТК.

Упоређивање података о томе да ли и које друштвене мреже користе жртве трговине људима, ирегулани мигранти и азиланти, може показати колика вероватноћа постоји међу припадницима ове три категорије да ће такав облик информационо-комуникационих технологија бити злоупотребљен у сврху њихових илегалних миграција. Подразумева се да употреба друштвених мрежа не искључује могућност да до илегалних миграција ових категорија становништва дође и посредством неких других информационо-комуникационих технологија или употребом неких других средстава. Ипак, њихово коришћење може у знатној мери олакшати комуникацију, размену информација између, на пример трафикера и жртве трговине људима, или ирегуларних миграната, односно азиланата са лицима која им помажу приликом илегалних миграција.

У вези са овим резултатима неопходно је разумети да је од значаја за разматрање примене посебних доказних радњи у овој области за више различитих кривичних дела, при чему нека од кривичних дела из области ВТК не подразумевају могућност примене ових мера, односно мере не покривају одредбе Законика у вези само са тим делима, али је могуће примењивање мера на дела из области ирегуларних миграција и трговине људима у вези са кривичним делима из ВТК. О овоме треба водити рачуна на практичној равни.

10.2 Коришћење друштвених мрежа (жртве трговине људима, ирегуларни мигранти, азиланти)

Упоређивањем процента оних испитаника који користе друштвене мреже у свакој од наведених категорија (жртве трговине људима, ирегуларни мигранти, азиланти), може се закључити да су на друштвеним мрежама најактивнији азиланти, затим следе ирегуларни мигранти, па тек онда жртве трговине људима. Од 52 азиланта, њих 46 (88,46%) користи друштвене мреже, а њих 6 (11,54%) не користи, од 91 ирегуларног мигранта, њих 54 (59,34%) користи друштвене мреже, а њих 37 (40,66%) не користи, од 48 жртава трговине људима, 22 (45,83%) користе друштвене мреже, а 26 (54,17%) не користе. Када се саберу испитаници из све три категорије (жртве трговине људима, ирегуларни мигранти и азиланти) може се видети да је и свеукупно посматрано већи број оних испитаника који користе

друштвене мреже него оних који их не користе. Тачније, од укупно 187 испитаника који су у све три категорије одговорили на ово питање, 124 испитаника (66,31%) користи друштвене мреже, док их 63 (33,69%) не користи. Анализирани подаци показују да је заступљеност корисника друштвених мрежа међу азилантима већа него што је то случај са жртвама трговине људима, као и да је заступљеност корисника друштвених мрежа међу азилантима већа него што је то случај са ирегуларним мигрантима. Дакле, азиланти су склонији да користе друштвене мреже него жртве трговине људима и ирегуларни мигранти.

Посебно је значајна информација о заступљености азиланата у вези са социјалним мрежама, па је у том смислу могућа примена ОСИНТ метода у прикупљању обавештења о извршиоцима кривичних дела из ове области или о кретањима у оквирима криминогене средине и лица која контактирају азилане у циљу вршења незаконитих активности.

10.3 Укрштање са подацима везаним за трговце људима

На питање да ли су трговци људима према којима су поступали **имали мобилни телефон** одговор није унело 7 (20,00%) анкетираних полицијских службеника. Од 28 полицијских службеника, који су на ово питање дали одговор њих, 26 (92,86% од 28) одговорило је да јесу, а 2 (7,14%) да нису. Када је у питању поседовање мобилног телефона од стране жртава трговине људима, од 50 испитаника, 41 испитаник (82%) поседује мобилни телефон, а њих 9 (18%) га не поседује, што значи да су међу жртвама трговине људима које су ушле у овај узорак била заступљенија лица која поседују мобилни телефон у односу на она која га не поседују.

На питање да ли су трговци људима знали да **користе интернет** одговор није унело 11 (31,43%) анкетираних полицијских службеника. Од 24 полицијска службеника који су одговорили на ово питање, њих 14 (58,33% од 24) је одговорило да јесу, а 10 (41,67%) да нису. У погледу коришћења интернета, од 50 испитаних жртава трговине људима, њих 27 (54%) је изјавило да користи интернет, док је њих 23 (46%) изјавило да не користи интернет. Пошто је укупно 27 испитаника од 50 изјавило да зна да користи рачунар, може се претпоставити да истих 27 испитаника користи и интернет.

На питање да ли су трговци људима **користили друштвене мреже** одговор није унело 10 анкетираних полицијских службеника (28,57%). Од 25 полицијских службеника који су одговорили на ово питање, њих 11 (44,00% од 25) је одговорило да јесу, а 14 (56,00%) да то нису радили. Када је реч о употреби друштвених мрежа од стране жртава трговине људима, од укупно 50 испитаника, њих 24 (48%) је одговорило да користе друштвене мреже, а њих 26 (52%) да не користе дтуштвене мреже. Као што се може претпоставити, у питању је податак који нема статистичку значајност, односно из односа броја жртава трговине људима које користе и које не користе друштвене мреже не може се извести закључак о учесталости коришћења друштвених мрежа међу жртвама трговине људима. Од 24 испитаника који користе друштвене мреже, сви су навели да имају налог на *Facebook-y*, а 1 испитаник је навео да има налог на *Twitter-y*. Истовремено, међутим, 5 испитаника је навело да нема налог ни на једној друштвеној мрежи. Од 11 полицијских службеника који су констатовали да су трговци људима користили друштвене мреже, 1 није определио

мрежу на којој је трговац људима отворио налог, њих 6 (60,00% од 10) је навело да су се трговци при избору мреже определили за *Facebook*, 3 (30%) да је избор трговаца био и *Facebook* и *Twitter*, а 1 (10,00%) да су избор трговца били *Facebook* и *Foursquare*.

Сагледавањем односа одговора на питање о **коришћењу интернета од стране трговаца људима** и оних на питање о томе да ли су трговци познавали жртву пре извршења кривичног дела трговине људима, уочено је да је највећи број трговаца људима познавао жртву и пре извршења кривичног дела. Оно што посебно упада у очи је чињеница да су они трговци људима који су користили рачунар у значајном броју случајева (у 38,46% случајева) успели да дело изврше над особама које нису знали пре извршења кривичног дела. Када су у питању извршиоци који нису користили интернет, случајеви регрутовања жртава изван миљеа особа које је трговац људима знао пре извршења кривичног дела, није забалежен.

Одговор на питање на који је начин извршилац кривичног дела трговине људима **ступио у контакт са жртвом** нису унела 2 полицијска службеника, 19 (57,57% од 33) полицијских службеника је навело да је то урађено лично, односно кроз непосредни контакт (укључујући и 4 случаја злоупотребе сродничих односа, 1 случај живота у заједничком домаћинству и 1 случај удварања), 11 (33,33%) је навело да је тај контакт остварен преко друге особе (преко родитеља, мајке, сродника, пријатеља, комшије, познаника), 2 (6,06%) су навела да је контакт остварен преко огласа, а 1 (3,03%) да је са овим циљем злоупотребљен интернет. Када су у питању одговори жртава трговине људима, од укупно 50 испитаника, њих 38 (76%) изјавило је да је трговац људима први контакт са њима остварио лично. У 8 случајева (16%) је први контакт остварен преко познаника, у 1 случају (2%) путем мобилног телефона, у 1 случају (2%) путем интернета, а у 1 случају (2%) на други начин, тачније, путем огласа. Дакле, најзаступљенији начин успостављања првог контакта са жртвама из испитаног узорка био је личним путем, без употребе информационо-комуникационих технологија. Сабирањем укупног броја контаката који су остварени лично (38) и преко посредника (8) може се закључити да је у 46 случајева први контакт са жртвом остварен без употребе било какве информационо-комуникационе технологије. Путем интернета, први контакт остварен је у 1 случају, а исто се односи и на мобилни телефон. Није познато на који начин је објављен оглас путем којег је дошло до првог контакта у једном случају те није познато да ли је и ту можда употребљен интернет или су у питању огласи објављени у штампи.

Томе треба додати и поређење податка о начину на који је трговац људима остварио први контакт са жртвом са податком о томе да ли жртва користи друштвене мреже или не и да ли и на којој од њих има отворен налог, што може показати да ли и у колико случајева су друштвене мреже послужиле као средство за врбовање жртава трговине људима. Од укупно 38 испитаника који су први контакт са трговцем људима остварили лично, њих 20 користи друштвене мреже. Од тога 14 испитаника има налог на Facebook-у, 1 испитаник има налог на Twitter-у а 5 испитаника користе друштвене мреже, али немају свој налог ни на једној. Од 8 испитаника са којима је трговац људима први контакт остварио преко познаника, свих 8 користе друштвене мреже и свих 8 имају налог на *Facebook-у*. Испитаник са којим је трговац људима први контакт остварио путем интернета, користи друштвене мреже и има налог на *Facebook-у*. Испитаник са којим је трговац људима први контакт остварио путем огласа не користи друштвене мреже. Ови подаци показују да је, иако укупно 23 испитаника има налог на *Facebook-у* а 1 на *Twitter-у*, први

контакт са трафикером у највећем броју случајева остварен лично или преко познаника. Управо су лица која су имала налог на *Facebook-у* и *Twitter-у* остварила тај контакт лично, односно преко посредника. То показује да, упркос поседовању налога на друштвеним мрежама, трговац људима ипак није одабрао тај начин за ступање у први конатакт са њима. Само један испитаник са којим је трговац људима први контакт остварио путем интернета користи друштвене мреже и има налог на *Facebook-у*, што указује на могућност да је *Facebook* том приликом злоупотребљен у сврху вербовања жртава трговине људима.

У прилог томе да учесталост вербовања/довођења у заблуду жртава трговине људима преко друштвених мрежа можда и није толико учестала колико се сматра да јесте, говоре и подаци добијени од стране полицијских службеника који су радили са трговцима људима. Према овим подацима, на питање на који је начин извршилац кривичног дела трговине људима **вербовао/довео у заблуду жртву** трговине људима одговор није унело 7 полицијских службеника, 11 (39,29% од 28) полицијских службеника је навело да је то урађено лажним обећањем (у погледу посла, добре зараде, стана и хране, односно удаје у иностранству), 7 (25,00%) је издвојило злоупотребу поверења, по 2 (7,14%) принуду, малолетство жртве, њену зависност од наркотика, емотивну везаност за извршиоца, а по 1 (3,57%) злоупотребу положаја, односно комуникацију преко *Facebook-а*.

У погледу **облика експлоатације жртава** евидентирани су следећи подаци. Највећи број полицијских службеника 17 (51,51% од 33) поступао је поводом случајева у којима су жртве експлоатисане кроз сексуалну експлоатацију. О случајевима који су укључивали сексуалну и радну експлоатацију у својим упитницима сведочило је 6 (18,18%) полицијских службеника. Њих 5 (15,15%) је поступало у случајевима у којима је била присутна само радна експлоатација, а по 2 (6,06%) у случајевима који су се манифестовали кроз принудно просјачење жртава, односно кроз вршење кривичних дела (укључујући и посредовање у проституцији). За 1 (3,03%) жртву је наведено да није експлоатисана. Одговор на ово питање нису унела 2 полицијска службеника. Када се упореде сви облици експлоатације жртава трговине људима са којима су се сусретали анкетирани полицијски службеници, јасно је да су и они у својој пракси најчешће поступали према трговцима који су жртве експлоатисали кроз принудну проституцију. Ово важи за 23 од 38 евидентираних случајева присутних облика експлотације (60,53%). Радна експлотација је била присутна у 11 од 38 случајева експлоатације (28,95%), а оне кроз принудно просјачење, односно вршење кривичних дела у по 2 од 38 случајева експлоатације (по 5,26%).

Учесталост сексуалне експлоатације жртава трговине људима потврђују и подаци добијени од представника оних субјеката који раде са жртвама трговине људима. Према њиховим наводима, највећи број жртава трговине људима из узорка овог истраживања били су жртве сексуалне експлоатације, 29 њих је било изложено само сексуалној експлоатацији док је у 1 случају она била комбинована са радном експлоатацијом, а у 1 случају са принудом на вршење кривичних дела. У 29 случајева (58%) жртве су биле изложене искључиво сексуалној експлоатацији. У 5 случајева (10%) жртве су биле изложене радној експлоатацији, у 5 случајева (10%) се радило о принуди на закључење брака, у 6 случајева (12%) о принуди на просјачење, у 2 случаја о принуди на вршење кривичних дела, а у 1 случају је дошло до прекида у фази вербовања, тако да жртва није била изложена ниједном облику експлоатације. Поред тога, у 2 случаја је постојало комбиновање различитих облика

експлоатације жртве. У једном случају се радило о комбиновању сексуалне експлоатације и радне експлоатације, а у другом о комбиновању сексуалне експлоатације и принуде на вршење кривичних дела. И наведена два случаја комбиноване, односно вишеструке експлоатације треба узети у обзир приликом израчунавања укупног броја случајева који су били подвргнути неком од видова експлоатације. Тако, ако се они узму у обзир, следи да је сексуалној експлоатацији укупно било подвргнут 31 испитаник, радној експлоатацији укупно 6 испитаника, а принуди на вршење кривичних дела 3 испитаника. Анализирани подаци показују да је од типова трговине људима, односно од облика експлоатације жртава трговине људима најзаступљенија била сексуална експлоатација, о којој је било речи у 58% случајева.

Одговор на питање о **времеском периоду у ком је вршена експлоатација жртава** није унело 6 полицијских службеника. О експлоатација жртава која је трајала 1 месец податке је навео 1 (3,45% од 29) полицијски службеник, о 4 месеца су посведочила 2 (6,90%) полицијска службеника, о 6-месечној експлоатацији податке је унело 6 (20,69%) полицијских службеника, а о 7 месеци 1 (3,45%) полицијски службеник. Да је експлотација трајала 1 годину констатовало је 9 (31,03%) полицијских службеника, а да је трајала 2 године посведочило је 7 (24,14%) полицијских службеника. О експлоатацији која је трајала 3 године податке је унео 1 (3,45%) полицијски службеник. Експлоатацију која је трајала 6 година навела су 2 (6,90%) полицијска службеника. Када су у питању подаци представника субјеката који су радили са жртвама трговине људима о трајању периода експлоатације, наводи се да је у 22 случаја из испитаног узорка тај период био краћи од годину дана, у 15 случајева је он трајао годину дана, у 1 случају је трајао 2 године, у 4 случаја је трајао 3 године, у 1 случају је трајао 4 године и у 1 случају је трајао чак 13 година.

Одређење у погледу тога **којој је информационо-комуникационој технологији извршилац имао приступ** у време извршења кривичног дела није дало 8 (22,86%) полицијских службеника. Од осталих 27, највећи број њих, чак 17 (62,97% од 27) навело је да су трговци људима имали приступ мобилном телефону, 5 (14,29%) да су имали приступ и фиксном и мобилном телефону, 4 (14,81%) да су имали приступ мобилном телефону и интернету, а 1 (3,73%) да је извршилац у време извршења имао приступ фиксном телефону. Гледајући сумарно 26 од 27 (96,30%) полицијских службеника, који су поступали у предметима трговине људима, поступали су према извршиоцима који су имали приступ мобилном телефону, њих 6 (22,22%) према извршиоцима који су имали приступ фиксном телефону, а 4 према онима који су имали приступ интернету (14,81%).

Податак о томе којој информационо-комуникационој технологији је жртва имала приступ у време врбовања заправо сужава круг оних које су могле бити злоупотребљене од стране трафикера. Наравно, треба имати на уму да је велика већина првих контаката са трафикером у овом узорку остварена лично или преко посредника, тако да податак о томе да ли је жртва имала приступ информационо-комуникационим технологијама у време врбовања не говори много о њиховој злоупотреби у сврху трговине људима у овом случају. Само фиксном телефону су у време врбовања приступ имала 2 испитаника, фиксном и мобилном телефону је приступ имало 8 испитаника, и фиксном телефону и мобилном телефону и интернету је приступ имало 9 испитаника, само мобилном телефону је приступ имало 19 испитаника, мобилном телефону и интернету су приступ имала 3 испитаника. Када

се посматра зборно, може се констатовати да је фиксном телефону приступ имало укупно 19 испитаника, да је мобилном телефону приступ имало укупно 39 испитаника, да је интернету имало приступ укупно 13 испитаника. Укупно 8 испитаника није унело податак о томе којој информационо-комуникационој технологији су имали приступ у време врбовања. Анализа наведених података показује да је најзаступљенија информационо-комуникациона технологија којој су имале приступ жртве трговине људима из овог узорка мобилни телефон (55% испитаника имало је приступ мобилном телефону), да је на другом месту по заступљености фиксни телефон (27% испитаника имало је приступ фиксном телефону), а на трећем интернет (18% испитаника имало је приступ интернету).

Оно што је овде значајно јесте постојање могућности за искоришћавање ових технологија у сврхе експлоатисања жртава од стране трафикера и других лица у њиховом кругу (како лица која су у фази врбовања или некој другој фази) а што указује такође и на могућности које исти нису искористили. Но, са повећањем рачунарске и информатичке писмености свих слојева становништва ово је један моменат на који треба посебно обратити пажњу у смислу проактивног деловања, односно, превентивног поступања. У том смислу је од значаја разматрати деловање у правцу ширења и јачања свести о могућим злоупотребама, пре него што до њих стварно дође, али и деловања на могуће будуће жртве кроз подизања свести о могућностима и приликама за експлоатисање

На питање да ли су извршиоци **користили друштвене мреже у време извршења кривичног дела** није одговорило 13 (43,33%) анкетираних полицијских службеника. Од 22, њих 14 (63,64% од 22) је констатовало да извршиоци нису користили друштвене мреже у време извршења кривичног дела, а 8 (36,36%) да јесу. Од ових 8 полицијских службеника њих 6 (75,00%) је поступало према извршиоцима који су имали налог на *Facebook-u*, а 2 (25,00%) према онима који су имали налог на *Facebook-u* и *Twitter-u*. Другим речима, сви извршиоци кривичног дела трговине људима, који су користили друштвене мреже у време извршења кривичног дела, имали су налог на *Facebook-u*. Када је у питању коришћење друштвених мрежа од стране жртава трговине људима у време врбовања, 22 испитаника (73%) су имала налог на *Facebook-y*, 3 испитаника (10%) су имала налог на *Twitter-y*, док њих 5 није имало налог ни на једној друштвеној мрежи. Наведени подаци показују да су међу оним жртвама које су имале налог на некој друштвеној мрежи најзаступљенији корисници *Facebook*-а.

И **начин на који је трговац људима одржавао контакт са жртвом** може показати у којој мери је злоупотреба информационо-комуникационих технологија допринела виктимизацији, исто као што је то случај са начином остваривања првог контакта између жртве и трговине људима. У случају испитаника из овог узорка комуникација се одвијала на неколико начина: лично, преко посредника, путем мобилног телефона и путем интернета. Искључиво личним путем комуникација се одвијала у 21 случају (42%), и лично и путем мобилног телефона се одвијала у 17 случајева (38%). Трговац је одржавао контакт са жртвом и лично и путем мобилног телефона и путем интернета само у 1 случају (2%) и у питању је био случај сексуалне експлоатације. Одржавање контакта са жртвом искључиво путем мобилног телефона било је присутно у 5 случајева (10%), искључиво путем интернета, контакт је одржаван само у 2 случаја (4%), а контакт је преко посредника одржаван само у 1 случају (2%). Један испитаник није унео податак о томе на који начин је трафикер одржавао кнтакт са њим.

Када се сагледа колико је укупно коришћена свака информационо-комуникациона технологија или други начин комуницирања, може се видети да је највећи број контаката са жртвом, 41 (58%), одржаван лично, мобилни телефон је коришћен укупно у 25 случајева (35%), путем интернета је контакт одржаван укупно у 3 случаја (4%), док је контакт преко посредника одржаван само у 1 случају. Наведени подаци показују да је, као и у случајевима врбовања жртава трговине људима, односно остваривања првог контакта трафикера са жртвом, лични контакт најзаступљенији начин на који је трговац одржавао контакт са жртвом. Контакт трафикера са жртвом одржаван је лично у укупно 41 случају (58%), с тим што је у 17 случајева лични контакт комбинован са употребом мобилног телефона, док је у 1 случају лични контакт комбинован са комуникацијом путем мобилног телефона и путем интернета.

Доминантност личног контакта и контакта путем мобилног телефона као начина одржавања комуникације трговца људима са жртвом потврђују и одговори полицијских службеника који су радили са трговцима људима. Наиме, у погледу **начина одржавања везе трговаца са жртвом** нису се изјаснила 4 полицијска службеника, а њих 10 (32,26% од 31) каже да су ови контакти били лични и путем мобилног телефона. Њих 6 (19,35%) је констатовало да су ови контакти одржавани лично, по 5 (16,13%) да су одржавани путем мобилног телефона, односно лично, путем мобилног телефона и преко посредника, 3 (9,68%) да су одржавани лично, путем мобилног телефона и фиксног телефона, а по 1 (3,22%) да су одржавани лично, путем мобилног телефона и интернета, односно само преко интернета. Гледајући сумарно, 25 од 31 (80,64%) полицијског службеника поступало је у предметима трговине људима у којима су извршиоци са жртвама контактирали лично, њих 24 (77,42%) у предметима у којима се ова комуникација одвијала путем мобилног телефона, 5 (16,13%) у предметима у којима се ова комуникација одвијала преко посредника, 3 (9,68%) у предметима у којима се ова комуникација одвијала путем фиксног телефона, а 2 (6,45%) у предметима у којима се ова комуникација одвијала путем интернета.

11. ЗАКЉУЧЦИ И ПРЕПОРУКЕ

На основу наведених статистичких података може се констатовати да су међу жртвама трговине људима знатно заступљенија лица женског него лица мушког пола, и то особе између 19 и 33 година. Велика већина испитаника је пореклом са ових простора, и то српске или ромске националности. Образовање испитаника који чине овај узорак је на прилично ниском нивоу, што се може посматрати као фактор виктимизације јер отежава проналажење регуларног запослења, те је особа „принуђена“ да пронађе извор прихода и обезбеди себи егзистенцију на неки други начин. Ипак, треба имати у виду да је у питању мали узорак, ограничен на жртве испитане у одређеном временском периоду, што не допушта да се из њега изведе генерални закључак о томе да су жртве трговине људима у нашој земљи по правилу ниског степена образовања. Међу жртвама су најзаступљенија незапослена лица. Такође, највећи број испитаника оценило је свој економски статус као лош или чак веома лош и то како садашњи тако и у тренутку врбовања, што јасно показује у којој мери незапосленост, низак ниво образовања и негативан став о сопственој економској ситуацији доприносе виктимизацији. Однос броја испитаника који знају

и који не знају да користе рачунар није статистички значајан, будући да је разлика само 10% у корист првих. Велика већина испитаника поседује мобилни телефон, док је број оних који поседују рачунар знатно мањи. Податак о односу броја жртава које користе и које не користе друштвене мреже нема статистичку значајност, јер је њихов однос скоро 50-50.

Највећи број жртава регрутован је 2012. године, а највише њих потражило је помоћ током 2013. године и то од полиције. У највећем броју случајева радило се о сексуалној експлоатацији.

Најзаступљенији начин успостављања првог контакта са жртвама из испитаног узорка био је личним, директним, непосредним путем и то без употребе било каквих информационо-комуникационих технологија. Наиме, иако укупно 23 испитаника има налог на *Facebook*-у, први контакт са трафикером је у највећем броју случајева остварен лично или преко познаника, што показује да, упркос поседовању налога на друштвеним мрежама, трговац људима ипак није одабрао тај начин за ступање у први конатакт са њима. Само један испитаник са којим је трговац људима први контакт остварио путем интернета, користи друштвене мреже и има налог на *Facebook-у*, што указује на могућност да је Facebook том приликом злоупотребљен у сврху вербовања жртава трговине људима. То показује да на конкретном узорку приступ информационо-комуникационим технологимјама од стране жртве није имао знатнијег утицаја на њену виктимизацију. Будући да је први контакт у највећем броју случајева остварен лично или преко познаника, дакле без ослањања на информационо-комуникационе технологије. Лични контакт је и најзаступљенији начин на који је трговац одржавао контакт са жртвом, с тим што је он понекад комбинован са употребом мобилног телефона, а само ретко и са интернетом.

То, међутим не може бити основ за извођење закључка да у Србији нема случајева вербовања жртава трговине људима путем злоупотребе информационо-комуникационих технологија. Наиме, наведени подаци представљају само пресек тренутне ситуације и слика су једног веома малог узорка који се не може третирати као репрезентативан. Због тога би требало размотрити спровођење оваквих истраживања и у будућности и то редовно и на различитим узорцима, јер би се тек онда, након дуготрајног праћења могла креирати реална слика о заступљености и доприносу информационо-комуникационих технологија у процесу трговине људима и њиховом доприносу виктимизацији.

ЛИТЕРАТУРА

1. Анђелковић, М. Беширевић, В. Вукасовић, Т. Глигорић, М. Николић, Д. Оташевић, О. Радовић, И. Wijers, М. (2011), Трговина људима у Републици Србији, Извештај за период 2000–2010, АСТРА – Акција против трговине људима, Београд
2. Батрићевић, А. (2013), Еколошка кривична дела – злочини без жртве? *Темида,* 16 (1)
3. Батрићевић, А. (2010), Међународни стандарди у превенцији насилничког криминалитета код малолетника, (ур. Лепосава Крон) *Насилнички криминал: етиологија, феноменологија превенција*, Инситутут за криминолошка и социолошка истраживања, Београд
4. Батрићевић, А. (2008). Грађанско-правна одговорност због повреде права на сопствену слику, Бранич, 121 (1-2)
5. *Декларација о основним принципима правде за жртве злочина и злоупотребе власти*, усвојена Резолуцијом Генералне скупштине Уједињених нација број 40/34 од 29. новембра 1985. године
6. Голубовић, С. Голубовић, Н. (2011), Примена теорије рационалног избора у анализи трговине људима, *Наука, безбедност, полиција,* 16 (2)
7. Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009.
8. Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009. члан 4 и Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001.
9. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела, Службени гласник РС, бр. 42/2002, 27/2003, 39 /2003, 67/2003, 29/2004, 45/2005 и 72/2009.
10. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, број 61/2005 и 104/2009.
11. Закон о полицији, Службени гласник РС, бр. 101/2005, 63/2009 и 92/2011.
12. Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица, Службени гласник РС, бр. 85/2005.
13. Закон о програму заштите учесника у кривичном поступку, Службени гласник *РС*, бр. 85/2005.
14. Јефтовић, М. Милашиновић, С. (2002), *Самоугрожавање друштва – социјално-патолошке девијације*, Синекс, Београд
15. Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд
16. Јовашевић, Д. Батрићевић, А. (2013), Organized Crime As a Threat to Security Systems – Serbian Experience, *Studia Securitatis (Security Studies),* 7 (2)
17. Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005,72/2009, 111/2009 и 121/2012.
18. Лазаревић, Љ. (2011), *Коментар Кривичног законика Републике Србије*, Савремена администрација, Београд
19. Мијалковић, С. и Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд
20. Мијалковић, С. (2005). Облици и видови трговине људима. *Темида*, 8(1)
21. Николић-Ристановић, В. (2009), Трговина мушкарцима у Србији, Виктимолошко друштво Србије, Београд
22. Николић-Ристановић, В. Ћопић, С. Миливојевић, С. Симеуновић-Патић, Б. Михић, Б. (2004), Трговина људима у Србији, Виктимолошко друштво Србије, Организација за европску безбедност и сарадњу, Београд

23. Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001.
24. Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог *криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001.*
25. Situational Overview on Trafficking in Human Beings, European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Warsaw, June 2011, http://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Situational_Overview_on_Trafficking_in_Human_Beings.pdf, 01.11.2013.
26. Strategic Project on Eurojust's action against trafficking in human beings, Final report and action plan, The European Union's Judicial Cooperation Unit (EUROJUST), October, 2012, http://eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Eurojust%20action%20against%20trafficking%20in%20human%20beings%20%28October%202012%29/THB-report-2012-10-18-EN.pdf, 01.11.2013.
27. Save the Children (2011), Регионални извјештај о просјачењу дјеце, распрострањеност, превенција и сузбијање дјечјег просјачења, Save the Children, Сарајево, стр. 12.
28. Стратегија борбе против трговине људима у Републици Србији, Службени гласник РС, бр. 111/2006.
29. Стојановић, З. (2006), Коментар Кривичног законика, Службени гласник, Београд
30. Смерница 2, *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, United Nations High Commisissioner for Human Rights to the Economic and Social Council, E/2002/68/Add.1, New York, 2002.
31. Trafficking in Human Beings in the European Union, OC Networks in the South-East European Sphere, Analysis and Knowledge, The Hague, 1 September 2011, https://www.europol.europa.eu/sites/default/files/publications/trafficking_in_human_beings_in_the_european_union_2011.pdf, 01.11.2013.
32. Устав Републике Србије, Службени гласник РС, бр. 98/2006.
33. Convention (No. 29) concerning Forced Labor, Adopted on 28 June 1930 by the General Conference of the International Labor Organization at its 14th session, at: Human Rights - A Compilation of International Instruments Volume I, Universal Instruments, United Nations, New York and Geneva, 1994.

Проф. др Милан Жарковић
Криминалистичко полицијски универзитет
Криминалистичко-полицијска академија

Митар Ђурашковић
Министарство унутрашњих послова Републике Србије

КРИМИНАЛНА АКТИВНОСТ ТРГОВАЦА ЉУДИМА

Садржај

Табеле

1. УВОД

Трговци људима су сва лица која су укључена у процес трговине људима (учествују у врбовању жртава, њиховом спровођењу, превожењу, чувању, обезбеђењу смештаја, контролисању или експлоатицији). Могу деловати као део међународних организованих криминалних група (најчешће припадају етнички или национално хомогених групама, али могу бити и различитог порекла) или као мале групе без чврсте унутрашње структуре (често укључују и чланове породице жртве), али и као појединци (како мушкарци, тако и жене) који, најчешће, већ имају криминалну прошлост.

Упркос различитостима облика трговине људима и специфичностима улога извршилаца, може се рећи да међу трговцима људима преовлађују особе које одликује рационални приступ злочину и радњама које предузимају (процењују ризик, трошкове и корист) и које не презају да, зарад личне користи, свесно униште живот другог човека.[851] Одликују их лукавство, препреденост, подмуклост, вештина лажног самоприказивања и манипулисања другима (њиховим осећањима и очекивањима), саможивост, истрајност и неосетљивост на бол и патње других, усмереност на тренутно задовољење властитих потреба, флексибилност у успостављању контроле, доминације и експлоатисања, одсуство емпатичког разумевања жртве (са одличним предвиђањем њеног понашања), агресивност, безобзирност, свирепост, суровост, окрутност и спремност на примену претњи, уцена, одмазди, насиља, подмићивање и корупцију.[852] Уз различитости ситуација и улога трговаца људима у злочину, код сваког појединца присутне су различите комбинације наведених, али и других одлика личности.

2. МЕТОДОЛОШКЕ НАПОМЕНЕ

Околности везане за извршиоце кривичног дела трговине људима из члана 388 Кривичног законика Републике Србије и особености њиховог криминалног деловања, укључујући и оне које се могу означити као злоупотреба савремених информативно- комуникационих технологија, утврђиване су кроз анализу података из 35 упитника попуњених од стране полицијских службеника Министарства унутрашњих послова Републике Србије (МУП РС). Полицијским службеницима који су поступали у предметима трговине људима упитници су дистрибуирани преко Управе граничне полиције.

Из 14 подручних полицијских управа упитник је попунио 31 полицијски службеник. Из полицијске управе ПУ Зрењанин упитнике је попунило 9 полицијских службеника, из ПУ Панчево 6, из ПУ Прокупље и Краљево по 3, из ПУ за град Београд 2, а по 1 из ПУ Нови Пазар, ПУ Кикинда, ПУ Сомбор, ПУ Ужице, ПУ Ваљево, ПУ Ниш, ПУ Сремска Митровица, ПУ Врање и ПУ Нови Сад. Упитник је попунио и 1

851 Жарковић М. Елез С. (2010), Основни елементи поступања полицијских службеника у супротстављању трговини људима, Тематски зборник: Сузбијање трговине људима – добре праксе, Приручник за институције, АСТРА – Акција против трговине људима, Београд, стр. 59;

852 Њихово насиље је незаустављиво, сврховито и без емоција. Као социјални предатори они су у непрестаном и немилосрдном лову на плен у коме је све дозвољено. Радуловић Д. (2006), Психологија криминала, психопатија и преступништво, Београд, стр. 310;

полицијски службеник са граничног прелаза Хоргош. Податке о организационој јединици нису унела 2 полицијска службеника која су попунила упитник.

Попуњавање упитника подразумевало је искуство полицијских службеника на пословима спречавања и сузбијања кривичног дела трговине људима. Гледано кроз призму линијске службе којој припадају, 24 (77,42%) анкетирана полицијска службеника су навела да обављају послове из делокруга рада Одељења пограничне полиције (ОПП), 5 (16,13%) да су полицијски службеници ангажовани у оквиру Одељења за странце (ОЗС), 2 (6,45%) да су полицијски службеници Управе за странце (УЗС). Прецизније одређење линијске службе нису извршила 3 (8,57%) анкетирана полицијска службеника (из ПУ Краљево), а 1 (2,86%) упитник није садржао одговор на ово питање

Примарна обрада попуњених упитника извршена је од стране службеника Управе за аналитику МУП-а РС. Подаци су обрађени у програмима *Microsoft Office Excel* и *Statistical Package for the Social Sciences (SPSS).*

3. ТРГОВЦИ ЉУДИМА

У погледу података **о полу трговаца људима** у 20 (57,14% од 35) анкетних упитника наведено је да су полицијски службеници поступали према трговцима људима мушког пола, у 10 да су поступали према трговцима женског пола (28,57%), а у 5 да се поступало према трговцима оба пола (14,29%). Гледано сумарно, од 35 анкетираних полицијских службеника њих 25 (71,43%) је поступало према трговцима мушког пола, а њих 15 (42,86%) према трговцима - женама. Ови подаци указују на то да се особе мушког пола чешће појављују као извршиоци кривичног дела трговине људима, али и на то да су у овој позицији значајно присутне и особе женског пола. Учешће особа женског пола међу трговцима људима, поводом чије криминалне делатности су поступали анкетирани полицијски службеници одвијало се кроз саизвршилаштво, али и кроз самостално извршење овог кривичног дела. Шире гледано, искуство говори да се особе женског пола у саизвршилаштву посебно ангажују у фази регрутације (вербовања), а неретко и током контроле жртава. Према подацима из 198 кривичних пријава, које су полицијски службеници МУП-а РС поднели у периоду од 2008. до 2012. године, за извршење кривичног дела трговине људима, надлежним јавним тужиоцима пријављено је 394 учинилаца. Међу пријављеним лицима биле су 303 особе мушког и 91 особа женског пола.

Табела 1. Пол трговаца људима

Анкетирани полицијски службеници су поступали према трговцима људима	Број	%
мушког пола	25	71,43
женског пола	15	42,86

На питање о **годинама живота трговаца људима** према којима су поступали, један полицијски службеник није одговорио, а највећи број њих, чак 21 (61,76% од 34) навео је да су трговци људима, према којима су поступали, били старости између 35 и 55 година, 8 (23,53%) да су били старости између 21 и 35 година, 3

(8,82%) да су у питању били извршиоци старости између 55 и 65 година, а 1 (2,94%) да је поступано према извршиоцу старости између 18 и 21 година. У једном анкетном упитнику (2,94%) наведено је да су полицијски службеници поступали према трговцима старости између 21 и 35 година, као и према онима старости између 35 и 55 година. Видљиво је да су сви анкетирани полицијски службеници поступали само према пунолетним извршиоцима кривичног дела трговине људима. Притом, само једно поступање је било усмерено према млађем пунолетном лицу (старијем од 18, а млађем од 21 године).

Табела 2. Старосна структура трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима старости	Број	%
14 - 18 година	-	-
18 - 21 година	1	2,94
21 – 35 година	9	26,47
35 – 55 година	22	64,70
55 – 65 година	3	8,82
преко 65 година	-	-

У погледу **државе рођења трговаца људима** подаци су унети у 33 од 35 упитника. Према овим подацима, сви трговци људима из случајева у којима су анкетирани полицијски службеници поступали, рођени су на територији бивше Социјалистичке Федеративне Републике Југославије (СФРЈ). Прецизирајући одговор, 2 полицијска службеника су навела да су поступања била усмерена ка трговцима људима који су рођени на територији бивше Савезне Републике Југославије (СРЈ), а њих 20 да су у питању били трговци људима рођени на територији Републике Србије (РС). У вези са одговором на питање о држави рођења трговаца људима према којима су анкетирани полицијски службеници поступали, на уму треба имати и чињеницу да је, након распада СФРЈ, СРЈ (која је проглашена априла 1992. године), државна заједница Србије и Црне Горе (егзистирала у периоду од фебруара 2003. до маја 2006. године) обухватала територију данашње Републике Црне Горе и Републике Србије, као и то да је Република Србија самостална држава од јуна 2006. године. Увидом у податке о месту рођења троваца установљено је да је један, за ког је наведено да је рођен у СФРЈ, рођен у Босни и Херцеговини (у месту Доња Пакленица). Према подацима из 198 кривичних пријава, које су полицијски службеници МУП-а РС поднели надлежним јавним тужиоцима у периоду 2008 - 2012. године, а за извршење кривичног дела трговине људима, међу 394 пријављених учинилаца било је 377 домаћих и 17 страних држављана.[853]

Податке о **националности** извршилаца кривичног дела трговине људима према којима су поступали нису навела 4 анкетирана полицијска службеника. У 31 упитнику полицијски службеници су навели да су поступали према извршиоцима српске националности у 16 (51,61% од 31) случајева, а у 11 (35,48%) према извршиоцима ромске националности. Према извршиоцима муслиманске националности поступала су 2 (6,54%) анкетирана полицијска службеника (према 1 трговцу мушког пола, а у 1 случају у саизвршилаштву су биле особе оба пола,

853 Детаљније у: Мијалковић С. и Жарковић М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, стр. 194 и 195.

муслиманске националности). Према особи мушког пола мађарске националности поступао је 1(3,22%) полицијски службеник. У 1 случају (3,22%) полицијски службеници су поступали према извршиоцима међу којима су биле особе, како српске, тако и ромске и муслиманске националности (поступало је ОЗС ПУ Нови Пазар). Од 16 полицијских службеника који су поступали у случајевима трговине људима, чији су извршиоци били српске националности, њих 11 је поступало према особама мушког пола, а 5 према особама женског пола. Од 11 полицијских службеника који су поступали у случајевима трговине људима чији су извршиоци били ромске националности, њих 5 је поступало према трговцима људима мушког пола, 4 према трговцима људима женског пола, а 2 према извршиоцима оба пола.

Податке о томе да ли је извршилац кривичног дела трговине људима у време извршења кривичног дела **живео у месту пријављеног боравка** или не није навео 1 анкетирани полицијски службеник. Међу осталим анкетираним полицијским службеницима њих 23 (67,65%) навело је да су трговци људима живели у месту боравка у време извршења кривичног дела, а 11 (32,35%) да су трговци људима живели на другој адреси, а не у месту пријављеног боравка.

Табела 3. У ком месту су трговци људима живели у време извешења кривичног дела

Анкетирани полицијски службеници поступали су према трговцима људима који су живели	Број	%
у месту боравка	23	67,65
на непријављеној адреси	11	32,35

У погледу **брачног статуса** трговаца људима податке није навео 1 полицијски службеник. Од 34 анкетирана полицијска службеника, њих 17 (50,00% од 34) је навело да су трговци људима у предметима у којима су поступали били ожењени/удати, 7 (20,58%) да се радило о разведеним особама, по 4 (11,76%) да су извршиоци били неожењени/неудати, односно у ванбрачној заједници. У 1 (2,94%) случају предмет полицијске обраде био је трговац људима који је био удовац, а у 1 (2,94%) случају неудата особа женског пола, а са њом и 1 трговац који је био неожењен, а живео је у ванбрачној заједници.

Табела 4. Брачни статус трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су били	Број	%
ожењени/удати	17	50
разведени	7	20,58
неожењени/неудати	4	11,76
удовац	1	2,94
у ванбрачној заједници	5	14,70

У погледу **услова становања** у 18 (52,94% од 34) упитника констатовано је да су трговци људима живели у свом, а у 11 (32,35%) да су живели у изнајмљеном стану. У 3 (8,82%) упитника наведено је да су извршиоци живели код родитеља, а у 2

(5,88%) да су живели у привременом боравишту који ми је обезбедила Влада Србије. У једном упитнику нису наведени подаци о условима становања извршилаца кривичног дела трговине људима.

Када је реч о **школској спреми** трговаца људима констатовано је да је 11 (32,35% од 34) анкетираних полицијских службеника поступало према извршиоцима са завршеном основном школом, по 7 (20,59%) према онима са завршеном средњом школом/гимназијом, односно према лицима без школе, 4 (11,76%) према онима који су имали уписану, а незавршену средњу школу/гимназију, 3 (8,82%) према онима који су имали уписану, али незавршену основну школу, по 1 (2,94%) према извршиоцу који је имао завршену вишу школу, односно према извршиоцима који су имали уписану али незавршену основну школу и онима који су имали уписану али незавршену средњу школу/гимназију. У једном упитнику нису наведени подаци о школској спреми извршилаца кривичног дела трговине људима према којима су полицијски службеници поступали.

Табела 5. Сумирани приказ школске спреме трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима	Број	%
са основном школом	16	44,12
без школе	11	20,59
са средњом школом	7	20,59
са вишом школом	1	2,94

У погледу **радног статуса** трговаца људима, највећи број анкетираних полицијских службеника, њих 22 (66,66% од 33) навео је да је поступао према извршиоцима који су били незапослени/не, 4 (12,12%) према привремено запосленим, 3 (9,09%) према повремено запосленим, а по 2 (6,06%) према запосленим, односно пензионерима. У два упитника нису наведени релевантни подаци о радном статусу трговаца људима.

Табела 6. Радни статус трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су били	Број	%
незапослени/не	22	66,66
привремено запослени/не	4	12,12
повремено запослени/не	3	9,09
запослени/не	2	6,06
пензионери	2	6,06

Највећи број анкетираних полицијских службеника, њих 23 (65,71% од 35) није унео податке о томе где су трговци људима били **запослени** у време извршења кривичног дела (ово у контексту констатације да су 22 полицијска службеника навела да су поступала према незапосленим лицима). Уз 2 случаја (5,71% од 35) су трговци били запослени као физички радници, у по 1 случају (2,86%) извршиоци су били запослени у приватном сектору, затим као директор у приватном сектору, у

бифеу, као конобарица, на приватним пословима, на грађевини, као власник кафане, као земљорадник, као радник у једном, односно другом предузећу у Зрењанину.

Гледано из перспективе анкетираних полицијских службеника **економски статус** трговаца у време криминалног деловања оцењен је као осредњи у 12 (35,29% од 34) упитника, као лош у 10 (29,41%), као веома лош у 8 (23,53%), као веома добар у 2 (5,88%), а као добар у 2 (5,88%) упитника. У једном упитнику нису наведени подаци о економском статусу трговаца људима.

Табела 7. Економски статус трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима чији је економски статус	Број	%
средњи	12	66,66
лош	10	6,06
веома лош	8	9,09
добар	2	12,12
веома добар	2	6,06

На питање да ли трговци људима према којима су поступали анкетирани полицијски службеници **говоре неки страни језик,** 10 (28,57% од 35) анкетираних полицијских службеника није унело одговор. Разлог је вероватно чињеница да се током криминалистичке обраде и обезбеђења доказа овој околности не придаје значај у свим случајевима. Од 25 полицијских службеника који су одговорили на ово питање њих 18 (72,00% од 25) је навело да трговци људима према којима су они поступали не говоре ни један страни језик, а 7 (28%) да говоре. Притом, у 3 упитника наведено је да су извршиоци говорили по један језик (италијански, руски, француски), а у 2 да су говорили по два језика (ромски и немачки).

У 11 (31,43%) упитника полицијски службеници нису унели одговор на питање да ли су трговци људима према којима су поступали **знали да користе рачунар.** И овоме је вероватно разлог чињеница да се током криминалистичке обраде и обезбеђења доказа овој околности не придаје значај у свим случајевима. Од 24 полицијска службеника који су одговорили на ово питање, њих 13 (54,17% од 24) је одговорило одрично, а 11 (45,83%) потврдно.

Табела 8. Познавање рада на рачунару од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су знали да користе рачунар	Број	%
да	11	45,83
не	13	54,17

Велики број анкетираних полицијских службеника није одговорио ни на питање да ли су трговци људима према којима су поступали **имали рачунар**, тачније њих 10 (28,57%). Они који су одговорили да трговци људима нису имали рачунар било је 14 (56,00% од 25), 8 (33,33%) да су трговци људима код куће имали десктоп

рачунар, 2 (8,33%) да су имали лаптоп/ноутбук, 1 (4,17%) да су имали и десктоп рачунар и лаптоп/ноутбук.

Табела 9. Поседовање рачунара од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су имали рачунар	Број	%
да	11	44,00
не	14	56,00

На питање да ли су трговци људима према којима су поступали **имали мобилни телефон** одговор није унело 7 (20,00%) анкетираних полицијских службеника. Од 28 полицијских службеника који су на ово питање дали одговор, њих 26 (92,86% од 28) је одговорило да јесу, а 2 (7,14%) да нису.

Табела 10. Поседовање мобилног телефона од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су имали мобилни телефон	Број	%
да	26	92,86
не	2	7,14

На питање да ли су трговци људима знали да **користе интернет** одговор није унело 11 (31,43%) анкетираних полицијских службеника. Од 24 полицијска службеника који су одговорили на ово питање, њих 14 (58,33% од 24) је одговорило да јесу, а 10 (41,67%) да нису.

Табела 11. Коришћење интернета од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су знали да користе интернет	Број	%
да	14	58,33
не	10	41,67

На питање да ли су трговци људима **користили друштвене мреже** одговор није унело 10 (28,57%) анкетираних полицијских службеника. Од 25 полицијских службеника који су одговорили на ово питање, њих 11 (44,00% од 25) је одговорило да јесу, а 14 (56,00%) да то нису радили.

Табела 12. Коришћење друштвених мрежа од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су користили друштвене мреже	Број	%
да	11	44,00
не	14	56,00

Од 11 полицијских службеника који су констатовали да су трговци људима користили друштвене мреже, 1 није определио мрежу на којој је трговац људима отворио налог, њих 6 (60,00% од 10) је навело да су се трговци при избору мреже на којој ће отворити налог определили за *Facebook*, 3 (30%) да је избор трговаца био и *Facebook-y* и *Twitter-y*, а 1 (10,00%) да су избор трговца *били Facebook и Foursquare*.

Табела 13. Друтвене мреже које су користили трговаци људима према којима су поступали анкетирани полицијски службеници

Анкетирани полицијски службеници поступали су према трговцима људима који су користили	Број	%
Facebook	10	90,90
Twitter	3	27,27
Foursquare	1	9,09

У погледу података о криминалној прошлости у 5 упитника овај податак није унет. Од 30 полицијских службеника који су унели одговор на ово питање њих 28 (93,33% од 30) је навело да су трговци људима према којима су поступали били евидентирани у оперативним евиденцијама МУП-а РС, а у 2 (6,67%) да нису.

Табела 14.Евидентираност трговаца људима у оперативним евиденцијама МУП-а РС

Анкетирани полицијски службеници поступали су према трговцима људима који су били евидентирани у оперативним евиденцијама МУП-а РС	Број	%
да	28	93,33
не	2	6,67

Податке о **претходној осуђиваности трговаца људима** према којима су поступали није унело 5 анкетираних полицијских службеника. Од 30 полицијских службеника који су унели одговор, 12 (40,00% од 30) је навело да су у питању осуде за имовинска кривична дела, 8 (26,67%) да су у питању осуде због извршења кривичног дела трговине људима, по 2 (6,67%) да је реч о осудама за силовање, за ванбрачну заједницу са малолетним лицем, односно за угрожавање јавног саобраћаја, а по 1 (3,33%) за тешку телесну повреду, изазивање опште опасности, недозвољену трговину, неосновано добијање и коришћење кредита и друге погодности.

Табела 15. Претходна осуђиваност трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су осуђивани за:	Број	%
имовинска кривична дела	12	40,00
трговину људима	8	26,67
силовање	2	6,67
ванбрачну заједницу са малолетним лице	2	6,67
угрожавање јавног саобраћаја	2	6,67
тешку телесну повреду,	1	3,33
изазивање опште опасности,	1	3,33
недозвољену трговину	1	3,33
неосновано добијање и коришћење кредита и друге погодности	1	3,33

У односу на околност да ли су кривична дела трговине људима извршиоци учинили самостално или у саизвршилаштву, 3 полицијска службеника нису дала одговор. Да су дела вршена у групи навело је њих 16 (50,00% од 32), да су извршиоци деловали самостално одговорило је 13 (40,62%) анкетираних, 2 (6,25%) да је саизвршилаштво обухватало ванбрачног друга, а 1 (3,13%) да је у питању било саизвршилаштво супружника. У 198 кривичних пријава, које су полицијски службеници МУП-а РС поднели у периоду од 2008. до 2012. године за извршење кривичног дела трговине људима надлежним јавним тужиоцима пријављено је 394 учиниоца. Овај податак наводи на закључак да су, статистички гледано, поднетим кривичним пријавама обухваћена по два извршиоца.

4. КРИМИНАЛНА ДЕЛАТНОСТ ТРГОВАЦА ЉУДИМА

Шире гледано, у поступку врбовања и регрутације, тј. успостављања контакта са потенцијалним жртвама трговци људима користе све расположиве, а у конкретном случају делотворне начине врбовања. Поред осталог, уз злоупотребу познанстава, наводно искрених љубавних и пријатељских, али и породичних веза (у овом контексту пажњу заслужују лица која имају криминалну прошлост, односно она са манифестацијама социјално патолошког понашања) ово подразумева и прикривеност коју омогућавају савремене информативно-комуникацијске технологије.[854]

Податке о томе да ли су извршиоци кривичног дела трговине људима **познавали жртву** пре извршења кривичног дела нису унела 3 анкетирана полицијска службеника. У криминалистичким обрадама у којима је поступало 27 (84,38% од 32) анкетираних полицијских службеника извршилац кривичног дела трговине људима познавао је жртву пре извршења кривичног дела, док је 5 (15,62%) анкетираних службеника поступало у предметима у којима извршиоци, пре извршења кривичног дела, нису познавали жртву.

854 Жарковић М. Елез С. (2010). *ibid.* стр. 60.

Табела 16. Претходно познанство жртава од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су претходно познавали жртву	Број	%
да	27	84,38
не	5	15,62

Сагледавањем односа одговора на питање о коришћењу интернета од стране трговаца људима и оних на питање о томе да ли су трговци познавали жртву пре извршења кривичног дела трговине људима, уочено је да је највећи број трговаца људима познавао жртву и пре извршења кривичног дела. Оно што је посебно уочљиво је чињеница да су они трговци људима који су користили рачунар у значајном броју случајева (у 38,46% случајева) успели да дело учине над особама које нису знали пре извршења кривичног дела. Када су у питању извршиоци који нису користили интернет, случајеви регрутовања жртава изван миљеа особа које је трговац људима знао пре извршења кривичног дела, није забележен.

Табела 17.

Да ли користи интернет	Да ли је знао жртву P27 - da	P27 - ne	Укупно
да (14)	8	5	13
%	61.54%	38.46%	100
не (10)	9	0	9
%	100.00%	0.00%	100
Укупно	17	5	22

(χ^2 = 4.480, df=1, p<0.05)

Готово идентично је и у погледу оних трговаца људима који су користили друштвене мреже. Чињеница је да су они извршиоци који су користили друштвену мрежу у 50% случајева успели да дело изврше над особама које нису знали пре извршења кривичног дела. Када су у питању извршиоци који нису користили друштвене мреже, случајеви регрутовања жртава изван миљеа особа које је трговац људима знао пре извршења кривичног дела, није забалежен.

Табела 18.

Да ли користи друштвене мреже	Да ли је знао жртву П27 - да	П27 – не	Укупно
а (11 да)	5	5	10
%	27.78%	100.00%	
б (14 не)	13	0	13
%	72.22%	0.00%	
Укупно	18	5	23

(χ^2 =8.306, df=1, p<0.005)

Одговор на питање на који је начин извршилац кривичног дела трговине људима **ступио у контакт са жртвом** нису унела 2 полицијска службеника, 19 (57,57% од 33) полицијских службеника је навело да је то урађено лично, односно кроз непосредни контакт (укључујући и 4 случаја злоупотребе сродничих односа, један случај живота у заједничком домаћинству и један случај удварања), 11 (33,33%) је навело да је тај контакт остварен преко друге особе (преко родитеља, мајке, сродника, пријатеља, комшије, познаника), 2 (6,06%) су навела да је контакт остварен преко огласа, а 1 (3,03%) да је у овом циљу злоупотребљен интернет.

Табела 19. Начин ступања у контакт трговца са жртвом

Анкетирани полицијски службеници поступали су према трговцима људима који су у контакт са жртвама ступили	Број	%
лично/кроз непосредни контакт	19	57,57
преко друге особе	11	33,33
преко огласа	2	6,06
преко интернета	1	3,03

Гледано кроз призму досадашњих искустава у пракси супротстављања трговини људима на територији Републике Србије, превара жртава у фази вербовања и регрутације много је учесталија појава од отмице.[855] На питање на који је начин извршилац кривичног дела трговине људима **вербовао/довео у заблуду жртву** трговине људима одговор није унело 7 полицијских службеника, 11 (39,29% од 28) полицијских службеника је навело да је то урађено лажним обећањем (у погледу посла, добре зараде, стана и хране, односно удаје у иностранству), 7 (25,00%) је издвојило злоупотребу поверења, по 2 (7,14%) принуду, малолетство жртве, њену зависност од наркотика, емотивну везаност за извршиоца, а по 1 (3,57%) злоупотребу положаја, односно комуникацију преко *Facebook-a*.

855 Жарковић М., Елез С. ibid. стр. 60.

Табела 20. Начин врбовања/регрутовања жртава од стране трговаца људима

Анкетирани полицијски службеници поступали су према трговцима људима који су жртве врбовали/регрутовали злоупотребом	Број	%
лажног обећања	11	39,29
поверења	7	25,00
принуде	2	7,14
малолетства жртве	2	7,14
њене зависности од наркотика	2	7,14
емотивне везаности за извршиоца	2	7,14
положаја	1	3,57
комуникације преко *Facebook*-а	1	3,57

Нова појавност кривичног дела трговине људима на територији Републике Србије огледа се, поред осталог, и у променама механизама контроле које трговци примењују према жртвама. Уместо, раније доминантних метода физичког злостављања и застрашивања (бруталног пребијања), све чешће се прибегава перфиднијим поступцима условљавања, манипулације и контроле.[856]

Одговарајући на питање да ли су извршиоци кривичног дела трговине људима **ограничавали кретање жртве,** 22 полицијска службеника (68,75% од 32) су констатовала примену овог начина контролисања жртве, 2 полицијска службеника (6,25%) су констатовала да су извршиоци то радили делимично, док је њих 8 (25,00%) негирало коришћење овог начина контролисања жртава. Одговор на ово питање нису унела 3 (8,57%) полицијска службеника.

Табела 21. Ограничавање кретања жртава од стране трговаца људима

Трговци људима према којима су поступали анкетирани полицијски службеници су ограничавали кретање жртвама у циљу њихове контроле	Број	%
да	22	68,75
не	8	25,00
да, делимично	2	6,25

О **одузимању личних докумената** у анкетним упитницима није се изјаснило 7 (20,00%) анкетираних полицијских службеника, а потврдно је одговорило њих 19 (67,86% од 28). Њих 9 (32,14%) је констатовало да извршиоци нису примењивали овај начин контролисања жртве.

856 Žarković M. Dragičević-Dičić R. Nikolić-Garotić S. Jekić-Bradajić G. Majić M. Vitorović M. (2011). Krivičnopravni sistem i sudska praksa u oblasti borbe protiv trgovine ljudima u Srbiji, Studija, Zajednički program UNHCR, UNDOC и IOM za borbu protiv trgovine ljudima u Srbiji, Beograd, str. 33;

Табела 22. Одузимање личних докумената жртава од стране трговаца људима

Трговци људима према којима су поступали анкетирани полицијски службеници су жртвама одузимали лична документа у циљу њихове контроле	Број	%
да	19	67,86
не	9	32,14

Према исказима 28 (84,85% од 33) полицијских службеника извршиоци кривичног дела трговине људима употребљавали су **силу** или **претњу према жртви** у циљу успостављања и одржавања контроле, њих 5 (15.15%) је негирало примену овог начина контроле жртве. Одговор на ово питање нису унела 2 полицијска службеника.

Табела 23. Примена силе/претње према жртава од стране трговаца људима

Трговци људима према којима су поступали анкетирани полицијски службеници су примењивали силу/претњу према жртвама у циљу њихове контроле	Број	%
да	28	84,85
не	5	15,15

У процени примене претње према члановима породице жртве или њој блиским лицима, 11 (33,33%) полицијских службеника није унело одговор. Од оних који су дали одговор њих 12 (50,00% од 24) је констатовало примену овог начина успостављања и одржавања контроле над жртвом. Исти број полицијских службеника (12, односно 50,00%) констатовао је да трговци људима са чијом криминалном активношћу су се сусретали нису користили претње према члановима породице жртве или њој блиским лицима.

Табела 24. Примена претње према члановима породице жртве или њој блиским лицима од стране трговаца људима

Трговци људима према којима су поступали анкетирани полицијски службеници су примењивали претњу према члановима породице жртве или њој блиским лицима у циљу контроле жртава	Број	%
да	12	50,00
не	12	50,00

Табела 25. Време трајања контакта трговца људима са жртвама

Анкетирани полицијски службеници поступали су према трговцима људима који су жртве експлотаисали	Број	%
неколико дана	1	3,57
један месец	5	17,86
два месеца	1	3,57
четири месеца	1	3,57
шест месеци	5	17,86
седам месеци	2	7,14
годину дана	7	25,00
две године	4	14,29
три године	1	3,57
шест година	1	3,57

У погледу **облика експлоатације жртава** евидентирани су следећи подаци. Највећи број полицијских службеника 17 (51,51% од 33) поступао је поводом случајева у којима су жртве експлоатисане кроз сексуалну експлоатацију. О случајевима који су укључивали сексуалну и радну експлоатацију у својим упитницима сведочило је 6 (18,18%) полицијских службеника. Њих 5 (15,15%) је поступало у случајевима у којима је била присутна само радна експлоатација, а по 2 (6,06%) у случајевима који су се манифестовали кроз принудно просјачење жртава, односно кроз вршење кривичних дела (укључујући и посредовање у вршењу проституције). За 1 (3,03%) жртву је наведено да није експлоатисана. Одговор на ово питање нису унела 2 полицијска службеника. Када се упореде сви облици експлоатације жртава трговине људима са којима су се сусретали анкетирани полицијски службеници, јасно је да су и они у својој пракси најчешће поступали према трговцима који су жртве експлоатисали кроз принудну проституцију. Ово у 23 од 38 евидентираних случајева присутних облика експлотације (60,53%). Радна експлотација је била присутна у 11 од 38 случајева експлоатације (28,95%), а оне кроз принудно просјачење, односно вршење кривичних дела у по 2 од 38 случајева експлоатације (по 5,26%).

Табела 26. Облици експлоатације жртава

Анкетирани полицијски службеници поступали су према трговцима људима који су жртве експлотаисали кроз	Број	%
сексуалну експлоатацију	23	60,53
радну експлоатацију	11	28,95
принудно просјачење	2	5,26
принудно вршење кривичних дела	2	5,26

Према подацима МУП-а РС, 213 жртава кривичног дела трговине људима у трогодишњем периоду (2010 - 2012) експлоатисано је кроз различите облике, а поједине од њих и кроз вишеструку експлоатацију. С обзиром на ову чињеницу, број евидентираних начина, односно евидентно присутних облика експлоатације ових

жртава досеже 242. Присутна у 153 случаја, најзаступљенија је сексуална експлотација жртава (63,22%). Радна експлоатација је откривена у 34 (14,05%) случаја, принудно просјачење у 33 (13,64%), принуда на вршење кривичних дела у 11 (4,54%), а принудни брак у 8 (3,31%) случајева. У 3 (1.24%) од 242 случаја није дошло до планиране експлоатације жртава.

Одговор на питање о **месту на ком су жртве експлоатисане** није унело 5 полицијских службеника. Међу 30 одговора су и одговори 4 (13,33% од 30) полицијска службеника који су навели да је то рађено у иностранству (2 пута Француска, 1 Русија, а у једном случају није наведена конкретна држава). Са експлоатацијом жртве у Републици Србији и иностранству (Босни и Херцеговини) сусрео се 1 (3,33%) полицијски службеник. У случајевима експлоатације жртава само на територији Републике Србије поступао је 21 (63,64%) полицијски службеник. Лоцирање места експлоатације везивањем за улицу (без навођења територије државе) извршила су 3 (10,00%) полицијска службеника, а 1 (3,33%) је у одговору навео да је експлоатација чињена на различитим местима. У погледу уже локације на којој је вршена експлоатација жртава неведени су подаци о саобраћајници, и то на улици од стране 3 полицијска службеника, о Ибарској магистрали, као и о локалу трговца људима од стране 1 полицијског службеника. Руралне средине, као просторни оквир у ком је вршена експлоатација жртава, навело је 7 полицијских службеника (23,33% од 30).

Одговор на питање о **времеском периоду у ком је вршена експлоатација жртава** није унело 6 полицијских службеника. Временски период трајања експлоатације жртава био је 1 месец, о чему сведочи 1 (3,45% од 29) полицијски службеник, 4 месеца што посведочила 2 (6,90%) полицијска службеника, затим 6 месеци, тврде 6 полицијских службеника(20,69%), па 7 месеци - 1 (3,45%) полицијски службеник. Да је експлотација трајала 1 годину констатовало је 9 (31,03%) полицијских службеника, а да је трајала 2 године посведочило је 7 (24,14%) полицијских службеника. О експлоатацији која је трајала 3 године податке је унео 1 (3,45%) полицијски службеник. Експлоатацију која је трајала 6 година навела су 2 (6,90%) полицијска службеника.

Табела 27. Време трајања експлоатације жртава

Анкетирани полицијски службеници поступали су према трговацима људима који су жртве експлоатисали	Број	%
један месец	1	3,45
четири месеца	2	6,90
шест месеци	6	20,69
седам месеци	1	3,45
годину дана	9	31,03
две године	7	24,14
три године	1	3,45
шест година	2	6,90

5. КОРИШЋЕЊЕ САВРЕМЕНИХ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА У ИЗВРШЕЊУ КРИВИЧНОГ ДЕЛА ТРГОВИНЕ ЉУДИМА

У погледу околности **коришћења комуникационе технологије** у време извршења кривичног дела трговине људима констатована је велика учесталост. Од стране 5 анкетираних полицијских службеника ови подаци нису ни унети, а њих 10 (33,33% од 30) је навело да су трговци људима ово чинили од куће, 7 (23,33%) да су то радили са другог места, а 8 (26.67%) да су трговци комуникационе технологије користили и од куће и са другог места. За 5 (16,67%) извршилаца констатовано је да нису користили комуникационе технологије у време извршења кривичног дела трговине људима. Гледајући сумарно, 18 од 25 (72,00%) полицијских службеника који су поступали у предметима трговине људима поступали су према извршиоцима који су користили комуникационе технологије које имају у свом стану, а њих 15 (60,00%) према извршиоцима који су користили комуникационе технологије док су се налазили *на неком другом месту*.

Табела 28. Коришћење комуникационих технологија од стране извршилаца у време извршења кривичног дела трговине људима

Да ли су анкетирани полицијски службеници поступали према извршиоцима који су у време извршења кривичног дела трговине људима користили комуникационе технологије?	Број	%
да, у стану	10	33,33
да, на другом месту	7	23,33
да, у стану и на другом месту	8	26,67
не	5	16,67

Одређење у погледу тога **којој је информационо-комуникационој технологији извршилац имао приступ** у време извршења кривичног дела није дало 8 (22,86%) полицијских службеника. Од осталих 27, највећи број њих, чак 17 (62,97% од 27) навео је да су трговци људима имали приступ мобилном телефону, 5 (14,29%) да су имали приступ и фиксном и мобилном телефону, 4 (14,81%) да су имали приступ мобилном телефону и интернету, а 1 (3,73%) да је извршилац у време извршења имао приступ фиксном телефону. Гледајући сумарно 26 од 27 (96,30%) полицијских службеника који су поступали у предметима трговине људима поступали су према извршиоцима кривичног дела који су имали приступ мобилном телефону, њих 6 (22,22%) према извршиоцима који су имали приступ фиксном телефону, а 4 према онима који су имали приступ интернету (14,81%).

Табела 29. Коришћење појединих видова комуникационе технологије од стране извршилаца у време извршења кривичног дела трговине људима

Којим видовима/облицима комуникационе технологије су имали приступ извршиоци у време извршења кривичног дела трговине људима према којима су поступали анкетирани полицијски службеници?	Број	%
мобилном телефону	26	96,30
фиксном телефону	6	22,22
интернету	4	14,81

Очекивани позитиван одговор на питање које је следило о томе да су извршиоци користили савремене информационо-комуникационе технологије у извршењу кривичног дела трговине људима и то у погледу **фазе у процесу трговине у којој** се то дешавало, изостао је у 2 упитника (укупно у њих 7). Највећи број анкетираних полицијских службеника, тачније њих 9 од 28 (32,14% од 28) истакао је злопупотребу ових средстава у фази вербовања и експлоатације, 7 (25,00%) у више фаза (без њиховог прецизирања), 5 (17,86%) везано за фазу експлоатације, по 2 (7,14%) везано за све фазе, односно за фазе вербовања, транспорта и експлоатације, а по 1 (3,57%) за фазу вербовања, фазу транспорта, односно фазу транспорта и експлоатације. Гледајући сумарно, а у складу са могућностима груписања датих одговора, од 28 полицијских службеника 19 (67,86%) је поступало у предметима трговине према извршиоцима који су савремене информационе технологије злоупотребљавали у фази експлоатације, 15 (53,57%) према извршиоцима који су ове технологије користили у фази вербовања, а 4 (14,28%) према онима који су је злоупотребљавали у фази транспорта жртава.

Табела 30. Коришћење комуникационе технологије од стране извршилаца у време појединим фазама извршења кривичног дела трговине људима

Фазе трговине људима у којима су трговци људима, према којима су поступали анкетирани полицијски службеници, користили комуникационе технологије	Број	%
у фази вербовања	15	53,57
у фази транспорта	4	14,28
у фази експлотације	19	67,86

На питање да ли су извршиоци **користили друштвене мреже у време извршења кривичног дела** није одговорило 13 (43,33%) анкетираних полицијских службеника. Од 22, њих 14 (63,64% од 22) је констатовало да извршиоци нису користили друштвене мреже у време извршења кривичног дела, а 8 (36,36%) да јесу. Од ових 8 полицијских службеника њих 6 (75,00%) је поступало према извршиоцима који су имали налог на *Facebook-у*, а 2 (25,00%) према онима који су имали налог на *Facebook-у* и *Twitter-у*. Другим речима, сви извршиоци кривичног дела трговине људима који су користили друштвене мреже у време извршења кривичног дела имали су налог на *Facebook-у*.

Табела 31. Коришћење друштвених мрежа од старне извршилаца у време извршења кривичног дела трговине људима

Да ли су трговци људима према којима су поступали анкетирани полицијски службеници користили друштвене мреже у време извршења кривичног дела?	Број	%
да	8	36,36
не	14	63,64

У погледу **начина одржавања везе трговаца са жртвом** нису се изјаснила 4 полицијска службеника, а 10 (32,26% од 31) је рекло да су ови контакти били лично и путем мобилног телефона. Њих 6 (19,35%) је констатовало да су ови контакти одржавани лично, по 5 (16,13%) да су одржавани путем мобилног телефона, односно лично, путем мобилног телефона и преко посредника, 3 (9,68%) да су одржавани лично, путем мобилног телефона и фиксног телефона, а по 1 (3,22%) да су одржавани лично, путем мобилног телефона и интернета, односно само преко интернета. Гледајући сумарно, 25 од 31 (80,64%) полицијског службеника поступало је у предметима трговине људима у којима су извршиоци са жртвама контактирали лично, њих 24 (77,42%) у предметима у којима се ова комуникација одвијала путем мобилног телефона, 5 (16,13%) у предметима у којима се ова комуникација одвијала преко посредника, 3 (9,68%) у предметима у којима се ова комуникација одвијала путем фиксног телефона, а 2 (6,45%) у предметима у којима се ова комуникација одвијала путем интернета.

Табела 32. Начин одржавања везе трговца за жртвама трговине људима

На који начин су одржавли везу са жртвама трговци људима према којима су поступали анкетирани полицијски службеници	Број	%
лично	25	80,64
путем мобилног телефона	24	77,42
преко посредника	5	16,13
путем фиксног телефона	3	9,68
путем интернета	2	6,45

На питање да ли су **средства савремених комуникационих технологија пронађена и одузета** од трговаца људима одговор није дало 10 анкетираних полицијских службеника (28,57%). Њих 19 (76,00% од 25) је одговорило да су у предметима у којима су поступали ова средства била пронађена и одузета, а 6 (24,00%) да нису.

Табела 33. Средства савремених технологија пронађена су и одузета од трговаца људима

Анкетирани полицијски службеници су пронашли и одузели средства савремених комуникационих технологија	Број	%
да	19	76,00
не	6	24,00

Одузета средства савремених комуникационих технологија су била **предмет експертизе** у оквиру поступања 18 (51,43% од 35,односно 94,74 од 19) анкетираних полицијских службеника.

Табела 34. Експертиза средства савремених технологија која су пронађена и одузета од трговаца људима

Средства савремених комуникационих технологија која су одузели анкетирани полицијски службеници су била предмет експертизе	Број	%
да	18	94,74
не	1	5,26

Констатовано је и то да су у 19 (70,37%) случајева привремено одузета средства савремених комуникација **коришћена као доказ у кривичном поступку**, а у 8 (29,63%) да нису.За 8 случајева ови подаци нису евидентирани.

Табела 35. Коришћење привремено одузетих срдстава савремених технологија као доказа

Средства савремених комуникационих технологија која су одузета од стране анкетираних полицијских службеника коришћена су као доказ у кривичном поступку	Број	%
да	19	70,37
не	8	29,63

ЛИТЕРАТУРА

1. Žarković, M. Dragičevićević-Dičić, R. Nikolić-Garotić, S. Jekić-Bradajić, G. Majić, M. Vitorović, M. (2011), Krivičnopravni sistem i sudska praksa u oblasti borbe protiv trgovine ljudima u Srbiji, Studija, Zajednički program UNHCR, UNDOC i IOM za borbu protiv trgovine ljudima u Srbiji, Beograd.
2. Жарковић М. Елез С. (2010), Основни елементи поступања полицијских службеника у супротстављању трговини људима, Тематски зборник: Сузбијање трговине људима – добре праксе, Приручник за институције, АСТРА – Акција против трговине људима, Београд.
3. Мијаилковић С. и Жарковић М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд.
4. Радуловић Д. (2006), Психологија криминала психопатија и преступништво, Београд.

проф др Милан Жарковић
Криминалистичко-полицијска академија

Митар Ђурашковић
Министарство унутрашњих послова Републике Србије

КРИМИНАЛНА АКТИВНОСТ КРИЈУМЧАРА ЉУДИМА

Садржај

Табеле

1. УВОД

Кријумчарење мигранта је у нашој земљи доскора препознавано као један од облика извршења кривичног дела *недозвољени прелаз државне границе*,[857] а чинило га је лице које се бави недозвољеним пребацивањем других преко границе, односно онај ко из користољубља омогућује другом недозвољени прелаз границе.

Законом о изменама и допунама Кривичног закона Републике Србије[858] из 2003. године, по први пут је издвојено као посебно кривично дело (у члану 111б) и кривично дело *трговина људима*. Поред осталог, уз кривично гоњење „трговаца људима", формулација законске одредбе омогућавала је и кривични прогон „кријумчара људи". Учињено је то на тај начин што је предвиђена одговорност и за онога ко довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности или тешких прилика другога врбује, превози, пребацује, предаје, посредује у предаји, сакрива или држи друго лице, а у циљу стицања неке користи.

Уочена одступања од принципа прокламованих међународним конвенцијама у погледу разликовања кривичног дела *кријумчарења мигранта* (људи) и кривичног дела *трговина људима* била су повод другачијег нормативног одређења бића оба кривична дела. Изменама кривичног законодавства из 2005. године, у групи кривичних дела против јавног реда и мира, у члану 350, као посебно кривично дело издвојено је кривично дело означено као *недозвољен прелаз државне границе и кријумчарење људи*.[859]

Овом одредбом, поред осталог, одговорност је предвиђена и за оног ко у намери да себи или другом прибави какву корист, омогућава другом недозвољени прелаз границе Србије и Црне Горе (у даљем тексту СЦГ) или недозвољени боравак или транзит кроз СЦГ, лицу које није држављанин СЦГ.[860]

Упркос настојању законодавца да унапреди нормативни одговор на проблем кријумчарења људи (мигранта) и решења садржана у одредбама члана 350 КЗ РС из 2005. године имала су извесне недостатке. Поред осталог, законодавцу се могло приговорити и то што је у погледу пасивног субјекта био недовољно одређен и дао могућност различитих тумачења норме у овом делу, а тиме и у погледу извршиоца овог кривичног дела. Према једном од тумачења инкриминација из члана 350 обухватала је радње кријумчарења особа које немају држављанство СЦГ, односно на кријумчарење мигранта.[861] С друге стране је гледиште које је овако постављен нормативни оквир у погледу пасивног субјеката кривичног дела тумачило шире од оног датог Протоколом против кријумчарења мигранта копном, морем и

857 Члан 249 ст. 2 Основног кривичног закона (Службени лист СФРЈ, бр. 44/76, 36/77, 34/84, 37/84, 74/87, 57/89, 3/90, 38/90, 45/90, 54/90, Службени лист СРЈ, бр. 35/92, 16/93, 31/93, 37/93, 24/94, 61/01, Службени гласник РС, бр. 39/03.);

858 Службени гласник РС, бр. 39/03;

859 Службени гласник РС, бр. 85/05, 88/05, 107/05;

860 Опширније у: Жарковић М. (2008), Кријумчарење мигранта у светлу одредаба Кривичног законика Републике Србије, у: Игњатовић, Ђ. (ур.) Стање криминалитета у Србији и правна средства реаговања, II део, Правни факултет у Београду, Београд, стр. 203-215;

861 Стојановић З. (2006), Коментар Кривичног законика, Београд, стр. 738;

ваздухом[862], и дозвољавало могућност да се као кријумчарена особа појави и домаћи држављанин. Ово, уз друге аргументе, и уз позивање на чињеницу да је у називу кривичног дела назначено да се односи на кријумчарење људи, а не само на кријумчарење миграната.

Изменама Кривичног законика из 2009. године[863], у члану 350 извршено је прецизирање текста у погледу пасивног субјекта, на начин да се уопште не помиње држављанство кријумчареног лица. Овим је учињен значајан искорак ка ефикаснијем спречавању и сузбијању кријумчарења свих лица (укључујући и домаће држављане), а тиме и штетних појава које прате ово кривично дело, као и последица које може да узрокује (укључујући и експлоатацију претходно кријумчарених лица). Поред осталог, одредбе кривичног дела недозвољен прелаз државне границе и кријумчарење људи из члана 350 КЗ РС предвиђају и одговорност за онога „ко у намери да себи или другом прибави какву корист, омогућава другом недозвољен прелаз границе Србије или недозвољен боравак или транзит кроз Србију".

2. МЕТОДОЛОШКЕ НАПОМЕНЕ

У циљу утврђивања чињеница од значаја за сагледавање различитих околности везаних за особе за које је, на нивоу основане сумње, утврђено да су учествовале у кријумчарењу људи (против њих су подношене кривичне пријаве) организована је анкета. На питања садржана у упитнику дистрибуираном преко Управе граничне полиције одговорило је 88 полицијских службеника, и то из: Регионалног центра граничне полиције према (РЦГП) Црној Гори 27 (30,68%), Полицијске управе (ПУ) Ужице 11 (12,5%), ПУ Панчево и РЦГП према Мађарској по 5 (по 5,68%), из РЦГП према Румунији 4 (4.55%), ПУ Прокупље и РЦГП према Хрватској по 3 (по 3,41%), ПУ Пожаревац и Станице граничне полиције (СГП) Аеродром Ниш по 2 (2,27%) и по 1 (1,14%) из ПУ Чачак, ПУ Јагодина, ПУ Кикинда, ПУ Крагујевац, ПУ Краљево, ПУ Крушевац, ПУ Лесковац, ПУ Ниш, ПУ Нови Сад, ПУ Пирот, ПУ Смедерево, ПУ Сомбор, ПУ Сремска Митровица, ПУ Шабац, ПУ Ваљево, ПУ Врање, ПУ Зрењанин, РЦГП према Бугарској и РЦГП према Македонији.

Гледано кроз призму линијске службе којој припадају, од 88 анкетираних полицијских службеника, њих 41 (46,59%) је навело да обављају послове из делокруга рада РЦГП, 12 (13,64%) је навело да обавља послове из делокруга рада одељења пограничне полиције (5 из ПУ Панчево, 4 из ПУ Ужице и по 1 из ПУ Сомбор, ПУ Врање и ПУ Нови Сад), 9 (10,23%) да су полицијски службеници криминалистичке полиције (2 из ПУ Пожаревац и 7 из ПУ Ужице), 2 (2,27%) да су ангажовани на граничном прелазу Аеродром. Којој нижој организационој јединицу у оквиру ПУ припада није навело 17 (19,32%) анкетираних полицијских службеника из 15 ПУ (3 из ПУ Прокупље и по 1 из ПУ Чачак, ПУ Јагодина, ПУ Кикинда, ПУ Крагујевац, ПУ Краљево, ПУ Лесковац, ПУ Ниш, ПУ Пирот, ПУ Сремска Митровица, ПУ Шабац, ПУ Смедерево, ПУ Зрењанин и ПУ Ваљево, као и 7 (7,95%) полицијских

862 У национално законодавство уведен Законом о потврђивању Конвенције Уједињених нација против транснационалног организованог криминала и допунских протокола, од 22.6.2001. Службени лист СРЈ- Међународни уговори, број 6/2001;

863 Службени гласник РС, бр. 72/09;

службеника који су навели само то да су припадници МУП-а РС без било каквог ближег означавања ниже организационе јединице.

Анкетирани полицијски службеници су имали могућност да своје поступање у предметима везаним за кријумчарење људи определе као репресивно, превентивно и хуманитарно. Своје поступање 39 (44,32%) анкетираних полицијских службеника определило је као превентивно и репресивно, 18 (20,45%) као само репресивно, 10 (11,36%) као репресивно и хуманитарно, 7 (7,95%) као превентивно, репресивно и хуманитарно, 5 (5,68%) као само превентивно, 4 (4,54%) као само хуманитарно, а 2 (2,27%) као превентивно и хуманитарно. Гледано сумарно, од 88 анкетираних полицијских службеника, репресивно поступање као облик свог ангажовања навело је 74 испитаника (84,09%), превентивно њих 53 (60,23%), а хуманитарно 23 (26,14%).

Одређујући се у погледу сазнања која се односе на коришћење интернета у остваривању процеса кријумчарења људи, од 87 полицијских службеника који су дали одговор, њих 46 (52,87%) је потврдило да имају сазнања да кријумчари користе интернет у процесу кријумчарења људи. Да немају таква сазнања одговорио је 41 полицијски службеник (47,13%).

Табела 1. Коришћење интернета у процесу кријумчарења

Да ли имате сазнања да кријумчари користе интернет у процесу кријумчарења миграната?	Број	%
да	46	52,87
не	41	47,13

Мање од половине анкетираних полицијских службеника, тачније 42 (48,28%) одговорило је да има сазнања да кријумчари користе друштвене мреже у процесу илегалних миграција. Да нема сазнања о овоме одговорило је 45 анкетираних (51,72%) полицијских службеника. Иако су изјавили да имају сазнања о томе да кријумчари људи користе интернет у реализацији својих криминалних активности, поједини полицијски службеници негирали су да имају сазнања о томе да кријумчари притом користе друштвене мреже.

Табела 2. Коришћење друштвених мрежа у процесу кријумчарења миграната

Да ли имате сазнања да кријумчари користе друштвене мреже у процесу кријумчарења миграната?	Број	%
да	42	48,28
не	45	51,72

Потврђена је статистичка значајност ($p<0,001$) приликом поређења броја испитаника који користе интернет и оних који користе друштвене мреже у процесу илегалних миграција, тј. потврђено је да већина кријумчара (95,2%) који користе интернет користе и друштвене мреже у процесу кријумчарења миграната. С друге стране, велики удео кријумчара који не користе интернет (86,7%) не користе ни друштвене мреже у том процесу.

Табела 3. Коришћење интернета и друштвених мрежа у процесу кријумчарења миграната

Да ли ли имате сазнања да кријумчари користе интернет у процесу кријумчарења миграната?		Да ли кријумчари користе друштвене мреже у процесу кријумчарења миграната?		
		Да	Не	Укупно
да	број	40	6	46
	%	95,2	13,3	
не	број	2	39	41
	%	4,8	86,7	
укупно	број	42	45	87

Иако су се изјаснили да немају сазнања о томе да су кријумчари људима користили друштвене мреже у процесу кријумчарења људи (миграната), поједини од анкетираних полицијских службеника унели су одговор кроз прецизирање конкретне друштвене мреже на којима су кријумчари људи имали налог. Одговор није унело 35 полицијских службеника, а 7 анкетираних је навело да кријумчари људи нису имали налог ни на једној друштвеној мрежи. Као друштвене мреже (из листе понуђених одговора *Facebook, Twitter, LinkedIn и Google+*) на којима су активни кријумчари у погледу којих су поступали, од 46 (52,27% од 88 анкетираних) полицијских службеника који су дали потврдан одговор и определили друштвене мреже које су кријумчари људи злоупотребљавали, њих 23 (26,14% од укупног броја анкетираних, односно 50,00% од оних који су дали потврдан одговор и навели неку од друштвених мрежа) навели су да имају таква сазнања у погледу друштвене мреже *Facebook*. *Facebook* и *Twitter* навело је 7 испитаника (7,95% од укупног броја анкетираних, односно 15,22% од оних који су дали потврдан одговор). *Facebook*, *Twitter* и *Google+* издвојило је њих 4 (4,55% од укупног броја анкетираних, односно 8,69% од оних који су дали потврдан одговор). *Facebook* и *Google+* издвојила су 3 испитаника (3,41% од укупног броја анкетираних, односно 6,52% од оних који су дали потврдан одговор). По 2 испитаника издвојила су *Twitter*, односно *Google+* (по 2,28% од укупног броја анкетираних, односно 4,34% од оних који су дали потврдан одговор). По 1 испитаник издвојио је *Skype* и „неку другу која није била наведена у понуђеном избору“ (1.14% од укупног броја анкетираних, односно 2,18% од оних који су дали потврдан одговор), односно *Facebook* и *LinkedIn*. Исто и у погледу *Facebook*, *Twitter*, *LinkedIn*, *Google+*, као и за *Facebook*, *LinkedIn* и *Google+*, односно *Facebook*, *Google+* и „неке друге која није била наведена у понуђеном избору“.

Гледано сумарно, 41 анкетирани полицијски службеник (46,59% од укупног броја анкетираних, односно 77,36% од оних који су дали потврдан одговор у погледу коришћења појединих друштвених мрежа, тј. од њих 53) навео је да имају оперативна сазнања да су кријумчари људи користили друштвену мрежу *Facebook*, 14 (15,90% од укупног броја анкетираних, односно 26,41% од оних који су дали потврдан одговор) навело је да имају оперативна сазнања да су кријумчари људи користили друштвену мрежу *Twitter*, 12 (13,64% од укупног броја анкетираних, односно 22,61% од оних који су дали потврдан одговор) навело је да имају оперативна сазнања да су кријумчари људи користили друштвену мрежу *Google+*, 3 (3,61% о укупног броја анкетираних, односно 5,66% од оних који су дали потврдан одговор) навело је да имају оперативна сазнања да су кријумчари људи користили друштвену мрежу *LinkedIn*, 2 (2,27% о укупног броја анкетираних, односно 3,77% од

оних који су дали потврдан одговор) навело је да имају оперативна сазнања да су кријумчари људи користили друштвену мрежу *Skype* и „неку другу која није била наведена у понуђеном избору“. *Foursquare* као друшвену мрежу која се злоупотребљава од стране кријумчара није издвојио ни један испитаник.

Табела 4. Друштвене мреже на којима су били активни кријумчари и имали налог на њима

Друштвене мреже на којима су били активни кријумчари и имали налог на њима	Број	%
Facebook	41	77,36
Twitter	14	26,41
Google+	12	22,61
LinkedIn	3	5,66
нема налог ни на једној ДМ	7	13,21
друге	2	3,77
Foursquare	0	-

Из одговора 87 анкетираних полицијских службеника (један није унео одговор) произилази да је велики број кријумчара људи, са којима су се они сусретали у свом раду, користио рачунар - мобилни телефон током кријумчарења. Тако су се изјаснила 74 полицијска службеника (85,06% од оних који су одговорили). Ово је негирало 13 полицијских службеника (14,94% од оних који су одговорили).

Табела 5. Коришћење рачунара - мобилних телефона у процесу кријумчарења мигранта

Да ли имате сазнања да кријумчари користе рачунар/ мобилни телефон у процесу кријумчарења мигранта?	Број	%
да	74	85,06
не	13	14,94

На питање да ли су кријумчари на чијим случајевима су радили користили посебне апликације на рачунарима/мобилним телефонима приликом одређивања руте кретања (GPS) у процесу кријумчарења, одговор је дало 85 анкетираних. Њих 68 (80,00% од оних који су одговорили, односно 77,28% од свих анкетираних) одговорило је негативно. Позитивно је одговорило 17 анкетираних (20,00% од оних који су одговорили, односно 15,01% од свих анкетираних), при чему је један навео и то да је у питању била апликација *Google Maps*.

Табела 6. Коришћење посебних апликација на рачунарима/ мобилним телефонима у процесу кријумчарења мигранта

Да ли имате сазнања да кријумчари користили посебне апликације на рачунарима/мобилним телефонима приликом одређивања руте кретања (GPS) у процесу кријумчарења и рачунар/мобилни телефон у процесу кријумчарења мигранта	Број	%
не	68	80,00
да	17	20,00

Одговарајући на питање колико је рачунар/мобилни телефон помогао кријумчару у контакту са другим кријумчарима и у успостављању контаката са илегалним мигрантима, анкетирани полицијски службеници могли су да изаберу једну од више понуђених опција. Највећи број 62 (93,94% од оних који се нису изјаснили да им је ова чињеница непозната, односно 70,45% од свих анкетираних) сматра да им је доста помогао, а по 2 (3,03% од оних који се ниси изјаснили да им је ова чињеница непозната, односно 2,27% од свих анкетираних) да им је веома мало помогао, односно да им није помогао. Значајан број анкетираних полицијских службеника, 22 (25,00%) се изајснио да им није познато колико је рачунар/мобилни телефон био од помоћи кријумчару у контакту са другим кријумчарима, односно у успостављању контаката са илегалним мигрантима.

Табела 7. Коришћење рачунара/мобилних телефона приликом остваривања контаката са другим кријумчарима и успостављања контаката са илегалним мигрантима

Колико је рачунар/мобилни телефон помогао кријумчарима у контакту са другим кријумчарима?	Број	%
Доста му је помогао	62	70,45
Није ми познато	22	25,0
Није му помогао	2	2,27
Веома мало му је помогао	2	2,27

Табела 8. Коришћење рачунара/мобилних телефона приликом остваривања контаката са другим кријумчарима и успостављања контаката са илегалним мигрантима (без оних који су се изјаснили да им ова чињеница није позната)

Колико је рачунар/мобилни телефон помогао кријумчарима у контакту са другим кријумчарима?	Број	%
Доста му је помогао	62	93,94
Није му помогао	2	3,03
Веома мало му је помогао	2	3,03

Највећи број анкетираних, тачније њих 54 (61,36%), сматра да кријумчари не би успели да постигну досадашњи ток кријумчарења мигранта без помоћи рачунара/мобилног телефона. Знатно мањи број, тј. њих 6 (6,82%) мисли потпуно другачије. Значајан број анкетираних, тачније њих 28 (31,82%) се определо за

одговор да кријумчари можда не би успели да постигну досадашњи ток кријумчарења миграната без помоћи рачунара/мобилног телефона.

Табела 9. Остваривање досадашњег тока кријумчарења миграната без помоћи рачунара/мобилног телефона

Да ли би кријумчари људи успели да постигну досадашњи ток кријумчарења без помоћи рачунара/мобилног телефона?	Број	%
да	6	6,82
не	54	61,36
можда	28	31,82

На питање да ли су им у досадашњој пракси са кријумчарима познати случајеви коришћења мобилних телефона/рачунара на јавним местима, а у циљу организовања и креирања даље руте кријумчарења илегалних миграната (интернет-кафе, парк, шопинг-центар, трг или друго јавно место), највећи број анкетираних полицијских службеника, тј. њих 46 (52,27%) одговорио је да им то није познато. Знатан број, тачније њих 31 (35,23%) одговорио је потврдно, док је 11 (12,50%) анкетираних негирало да има оваква сазнања.

Табела 10. Коришћење мобилних телефона/рачунара на јавним местима, у циљу организовања и креирања даље руте кријумчарења илегалних миграната

Да ли су кријумчари користили мобилне телефоне/рачунаре на јавним местима, у циљу организовања и креирања даље руте кријумчарења ирегуларних миграната?	Број	%
да	31	35,2
не	11	12,5
није ми познато	46	52,3

Табела 11. Коришћење мобилних телефона/рачунара на јавним местима, у циљу организовања и креирања даље руте кријумчарења илегалних миграната (без оних који су се изјаснили да им ова чињеница није позната)

Да ли су кријумчари користили мобилне телефоне/рачунаре на јавним местима, у циљу организовања и креирања даље руте кријумчарења ирегуларних миграната?	Број	%
да	31	73,81
не	11	26,19
укупно	42	100

ЛИТЕРАТУРА

1. Жарковић М. 2008, Кријумчарење мигранта у светлу одредаба Кривичног законика Републике Србије, у: Игњатовић, Ђ. (ур) Стање криминалитета у Србији и правна средства реаговања, II део, Правни факултет у Београду, Београд.
2. Мијаилковић С. и Жарковић М. 2012, Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд.
3. Стојановић З. 2006, Коментар Кривичног Законика, Београд.

ЗАКЉУЧЦИ И ПРЕПОРУКЕ

Високотехнолошки криминал је постао реалност наше данашњице. Информационо-комуникационе технологије доживљавају све већу експанзију, па се са правом може очекивати да се тај тренд у будућности мора наставити. Сви сервиси на интернету теже да развију информациону средину која одговара свим корисницима, па тако привлачећи све већи број људи да користе информационо-комуникационе технологије, не само за забаву већ и за финансијске трансакције, за тражење посла и нових шанси за сопствени духовни или професионални развој. Формирана је велика критична маса жртава широм планете, а криминалци из различитих области мигрирају своје активности у област вискотехнолошког криминала. И у другим областима криминала приметна је све већа употреба информационо-комуникационих средстава, како у сврхе извршења кривични дела, тако и у сврхе проналаска саучесника, жртава и друго. У области илегалних миграција и трговине људима такође је јасно уочљива повећана употреба информационо-комуникационих средстава у криминалне сврхе.

Истраживачи су, на основу спроведених истраживања, закључили да растућа популарност *веб*-сајтова, који се називају друштвеним мрежама, почива на њиховим специфичним особинама као што су, примарно, заснованост на корисницима и на успостављању стално интеракције међу њима. Ту се нагласак ставља на заједницу која се формира на бази заједничких интересовања. Суштину такве заједнице чини олакшано отварање канала за слање и размену информација, па чак и олакшано везивање емоција за садржај порука. Корисници више не преузимају информације већ их креирају, деле, размењују, тако да они више нису потрошачи већ стваоци садржаја на интернету.

У литератури не постоји општа сагласност око тога да ли интернет разара или учвршћује друштвени живот својих корисника. Истраживања указују на то да је комуникација преко интернета привлачна интровертним, стидљивим и друштвено анксиозним појединцима који посредством друштвених мрежа на интернету остварују (социјалну) компензацију због незадовољавајуће социјалне комуникације у реалном животу, па чак и превазилазе проблеме које имају у комуникацији са другима. С друге стране, постоје мишљења да такве особе чине супституицију реалне комуникације виртуелном која може да доведе до бихејвиоралне зависности од интернета.

Посебан квалитет тих сајтова је да они омогућавају корисницима да обликују и учине доступним на увид другим корисницима своје личне мреже и да остварују међусобну интеракцију. Тиме је могуће остварити везу појединаца који на други начин, због објективних разлога (најчешће физичке недоступности) не могу бити повезани. Наравно, није обавезно да се на овим мрежама траже нови контакти већ би пре требало да буде уобичајено да се контакти одржавају са онима који су саставни део постојећих веза из реалног живота. Овај вид комуникације је у новије време постао посебно омиљен код припадника млађих генерација, мада полако осваја и старије и, наравно, образоване особе и оне који се могу сматрати информатички писменим у најширем значењу те речи.

Нема сумње да је корист од присуства на друштвеним мрежама један од битних мотива што им данас велики број људи приступа. Предности умрежености се пре свега огледају у повезаности са другима и у користи која може да следи из те повезаности (размена информација, лична и професионална промоција,

упознавање са истомишљеницима или онима који деле исте циљеве, интересе и вредности итд.). Недостатци од присуства на друштвеним мрежама се углавном крећу у домену угрожавања приватности података који се стављају другима на увид мада не треба занемарити ни опасност од замене реалног света виртуелним и отуђености која из тога природно следи, па чак и стицања патолошке зависности од интернета.

У контексту теме читавог пројекта ова материја има значај с обзиром на то да се уочава да постоји тенденција коришћења интернета и друштвених мрежа у вршењу многих кривичних дела, а између осталог и дела везаних за трговину људима и кријумчарења људи у различите сврхе, било да је у питању радна експлоатација, кријумчарење потенцијалних тражилаца политичког азила, секс-трафикинг или нешто друго. Тзв. тамна страна социјалног капитала овде долази до пуног изражаја због чињенице да вршиоци ових кривичних дела прелазе из реалног у виртуелни свет с намером да буду повезани не само са својим жртвама већ и са осталим актерима у ланцу криминала, што би требало да им омогући брзо деловање, размену информација о њиховом кретању и стању на терену и, свакако, оно за њих најзначајније, да стално буду бар један корак испред свих оних који желе да спрече и зауставе њихову противзакониту активност.

Циљ овог рада је да се утврде обрасци коришћења рачунара, интернета и друштвених мрежа у функцији јачања социјалног капитала.

Рачунари и, уопште, примена информационо-комуникационих технологија, ушли су код нас у свакодневну употребу релативно скоро, тако да још увек не можемо сматрати да су постали опште прихваћени, ни као алат за обављање различитих послова нити као средство редовне и свакодневне комуникације.

С обзиром да постоји закономерност у прихватању техничких и технолошких новина, **може се закључити да је употреба рачунара везана за:**

- **генерацијску припадност** – рачунаре су прихватиле пре свега млађе генерације тако да се може претпоставити да их сада највише користе млађи нараштаји (до 30 година) и делом средње генерације (од 30 до 45 година), док су старији мање заинтересовани за њихову свакодневну употребу;
- **степен образовања** – када су у питању средње и старије генерације, рачунаре чешће користе високо образоване особе, док у млађим генерацијама нема велике разлике у коришћењу рачунара у односу на ниво образовања;
- **друштвени статус** – припадници виших друштвених статуса у већој мери користе рачунаре него што то чине припадници нижих статусних група, без обзира на старост и ниво образовања.
- **тип и величина насеља насеља** – с обзиром на комуналну инфраструктуру, очекивана је највећа употреба рачунара у великим градовима и урбаним насељима.

Најраспрострањенија примена рачунара, за личне потребе, је за успостављање контаката и комуникацију са рођацима и познаницима посредством сајтова који се уобичајено називају друштвене мреже. У вези са тим:

- млађе генерације чешће користе рачунар у ове сврхе него старији;

- млађе генерације користе друштвене мреже примарно, ради забаве, док старији настоје да на тај начин одржавају контакте са пријатељима и родбином.
- коришћење рачунара и друштвених мрежа за обезбеђивање тзв. социјалног капитала, тј. ради **стицања интересно заснованих контаката** још увек код нас **није ушло у ширу употребу** али без обзира на то постоји тенденција да се рачунари, интернет и друштвене мреже користе и у ове сврхе.

Може се закључити и да:

1) велика већина становништва Србије, млађа од 45 година, готово у потпуности влада елементарним знањима потребним за рад на рачунарима. То још увек не значи да су оспособљени да обављају сложеније задатке, али у сваком случају су оспособљени за сналажење на интернету или неком од уобичајених програма за свакодневну употребу.
2) постоји веза генерацијске припадности са социјалним обрасцима коришћења рачунара у различите сврхе, с тим да су млађе генерације окренуте ка учењу, забави и комуникацији, а да рачунаре слабо користе због посла. Средња и старија генерација радног контигента рачунаре у највећој мери користе управо због посла и нешто мање због информисања и комуникације. Приметно је да употреба рачунара рапидно опада са генерацијском припадношћу што се и овом приликом може објаснити већом пријемчивошћу млађих нараштаја за коришћење информационо-комуникационих технологија за ове намене. Старији остају верни старим методама информисања посредством штампаних и електронских медија. У најстаријем делу радног контигента (између 45 и 60 година) долази до видног, ако не чак и рапидног опадања интереса за коришћење рачунара ради забаве и комуникације са другима. Старији остају верни традиционалним механизмима забаве и комуникације;
3) млади у највећој мери користе интернет, а са старошћу опада број његових корисника. Коришћење интернета код старијих генерација је делом и радно-професионално детерминисано, односно многи од њих користе интернет у вези са потребама посла или на послу;
4) касне 50-е или ране 60-е године су граница на којој рапидно опада употреба интернета и овде можемо говорити о генерацијском јазу који је, између осталог, условљен и историјским тренутком у којем су рачунари и њихова употреба стигли на наше просторе. Може се претпоставити да сама чињеница припадности радном контигенту представља значајну детерминанту коришћења интернета с обзиром да је данас готово незамисливо обављати свакодневне послове и радне задатке без помоћи информационо-комуникационих технологија;
5) генерално се може констатовати да највише врста сајтова посећују млађи од 30 година, с тим да су углавном заинтересовани за друштвене мреже, сајтове информативног, образовног и забавног карактера. С друге стране старије генерације углавном посећују сајтова који су информативне и образовне садржине, да би се код још старијих, преко 45 година то, генерално, свело само на информативне сајтове. У категорији старијих од 65 година тек је нешто мање од две четвртине оних који користе интернет.

Доказ да су млади спремнији да прихвате нове облике друштвености које нуди Интернет је и податак да више од три четвртине млађих од 30 година отвара профиле на друштвеним мрежама и ступа у редовну размену информација са познатим и непознатим особама, док се међу припадницима старијих генерација редукује број корисника друштвених мрежа, али и број особа са којима ови остварују редовну виртуелну интеракцију. Тако нпр. половина корисника интернета из генерације од 30 до 45 година и само четвртина њих из генерације од 45 до 60 година посећује сајтове друштвених мрежа док то чини занемарљив број старијих од 60 година (сваки десети).

На основу приказаних података се може закључити да не постоје битније разлике у социјалним обрасцима комуникације преко друштвених мрежа припадника различитих генерација. Видно је да постоји генерацијска разлика у смислу да старије генерације проводе мање времена на друштвеним мрежама, али се не може тврдити да постоји битна разлика између самих социјалних образаца остварене комуникације.

Генерални закључак који се може извести из приказаних података је да се друштвене мреже најчешће користе ради комуникације и остваривања блиских веза са породицом и најближим пријатељима, као и ради разбијања досаде и прекраћивања времена. Продуктивно коришћење друштвених мрежа је сведено на релативно малу меру и то најчешће код нешто старијих испитаника или, прецизније, средњег генерацијског скупа из радног контигент,а односно код оних који су већ укорењени у пословним активностима и који би, по логици ствари, требало да се налазе близу врхунца своје професионалне каријере. Ово је у складу са већ констатованим налазима ранијих истраживања да они који у реалном свету већ имају шире мреже друштвене подршке су, у принципу, склони да и интернет све више користе за одржавање својих веза. Они се више друже са већ познатим пријатељима и преко интернета и преко посебних сајтова друштвених мрежа, где настоје да одржавају и продубљују своје контакте и јачају успостављене везе, али, ипак, нису склони ка стварању нових познанстава.

Изгледа да млађи још увек нису препознали да друштвене мреже могу да имају велики потенцијал у својству и са циљем изградње социјалног капитала, а да старији, зато што се налазе у последној трећини својих каријера, више и немају нарочити интерес да се прилагођавају новим инструментима како би каријеру даље подстицали. Дакле, средњи део радног контигента је највише мотивисан да друштвене мреже инструментализује за заузимање и учвршћивање радних и уопште професионалних позиција, уз ограду да ни они значајније не одступају од остатка популације. Дакле, види се могућност, али генерално изостаје акција на капитализовању друштвених мрежа зарад јачања професионалних позиција и то примарно у средњој генерацији радног контигента.

Старије генерације, кад већ почињу да се укључују у активности на друштвеним мрежама, показују слична интересовања као и млађе, али само слабијег интензитета. Једина разлика међу генерацијама је у склоности млађих да више времена проводе на друштвеним мрежама, па да у складу с тим тенденцијски успостављају већи број контаката. Оног тренутка када сајтови друштвених мрежа буду имали дужи „радни стаж“ на интернету, моћи ћемо поузданије да тврдимо да ли се радн о тенденцији напуштања ових сајтова од стране старијих или се напросто ради о промени генерацијских образаца њиховог коришћења. За сада, друга претпоставка се чини реалнијом.

Намеће се као закључак да је велики број људи склон ка упознавању са потпуно непознатим особама са којима је пре тога остварио контакт путем интернета. У овом можемо, с једне стране, препознавати велики потенцијал за формирање виртуелног социјалног капитала, али с друге стране и велику опасност од злоупотреба оваквих познанстава. Релативно мали број познанстава, које је већина остварила, казује да су, и по овом критеријуму, интернет и друштвене мреж само потенцијани инструменти за изградњу социјалног капитала. Колико ће се они преточити у свакодневну праксу, остаје да се види у годинама које долазе. Но, и поред различитих мишљења која се тим поводом могу чути, реално је очекивати да ће овај начин комуникације обогатити праксу изградње социјалног капитала на различитим пољима свакодневног живата.

Факторском анализом су екстрахована три фактора који кумулативно покривају 54,33% варијансе.

Применом Облимин ротације екстрахована су три јасно издвојена фактора тако да смо први фактор назвали фактором секундарних веза, други смо назвали фактором примарних веза и трећи је фактор забаве или фактор опуштених комуникација.

У првом фактору доминирају потребе за разним врстама посредовања, тражење партнера за остваривање емотивних веза, упознавање нових људи, комуникација са непознатима, повезивање са особама истих или сличних интересовања, тражење или обављање посла. Овај фактор покрива 33,28% варијансе, те се може закључити да трећина комуникација посматране популације има за циљ успостављање секундарних веза посредством повезивања на друштвене мреже.

Реч је о томе да појединци ступају у међусобне односе са другим људима да би на основу заједничких вредности остварили социјалне интеракције и на бази њих градили социјалне мреже, које имају вредност која се не огледа само на емоционалном плану, већ и у врло конкретним користима које су резултат поверења, узајамности, размене информација и сарадње повезане у друштвене мреже. Овде је испуњен услов да се социјални капитал схвата као систем социјалних мрежа и норми насталих редовним социјалним интеракцијама, које олакшавају акцију појединаца и група унутар шире заједнице или друштва, односно као друштвени (заједнички) ресурс који олакшава/отежава приступ другим ресурсима, тј. потенцијално повећава компаративну предност у односу на оне који нису чланови мрежа. У крајњој линији, овако конципиран социјални капитал је израз личног (и друштвеног) поверења и представља везу која омогућава групну координацију и сарадњу ради постизања индивидуалне (или групне) користи.

У другом фактору, фактору примарних комуникација, налазе се потреба за зближавањем и комуникацијом са члановима породице и родбином, зближавање са пријатељима и проналажење рођака, пријатеља и познаника са којима су се готово изгубили контакти. Овај фактор покрива 13,22% варијансе. Други фактор се концентрише ка мање значајној форми социјалног капитала, који се гради унутар примарних група и који као своју кључну одредбу има емоционалну, материјалну и физичку подршку унутар примарних група, односно унутар круга релативно блиских сродника и најближих пријатељима са којима се, у принципу, успоставља интеракција лицем у лице.

У контексту овог фактора се може констатовати да су за њега значајне све приватне мреже и везе примарног типа, као што су везе са пријатељима и

породицом. У том смислу основ поверења могу бити не само пословни и слични интереси већ и различити облици солидарности као што су породична, политичко-идеолошка, религијска, интересна, унутаргрупна у било ком значењу те речи. Овде се ради о типу социјалног капитала који се показао актуелним код нижих друштвених слојева, ниже образованог и руралног дела становништва, који ослонац за разне личне и друштвене активности тражи и налази у породици, суседству или ужој локалној заједници. Социјални капитал у овом сегменту комуникација пре има форму социјалне и емоционалне подршке блиских него интересне повезаности социјално удаљених појединаца

Трећи фактор (забава и опуштене комуникације са мање битним особама који покрива 7,23% варијансе), генерално, није у функцији изградње и обликовања социјалног капитала. Оваквом стању сигурно да у извесној мери доприноси и чињеница да друштвене мреже много више користе млађе генерације него старије те да већина младих још увек није ушла у радни процес. Стога категорија колега и сарадника пре подразумева школске другове и мање блиске пријатеље него потенцијалне сараднике са којима се остварују везе и контакти ради задовољавања интереса који потичу из секундарних облика груписања.

С друге стране и насупрот претходној констатацији, у оквиру овог фактора можемо наћи и елементе који указују на потенцијал за активирање тзв. тамне стране социјалног капитала. Познаници, колеге и сарадници и тзв. он-лајн пријатељи могу бити база на основу које се могу градити разне затворене групе, групе клановског типа које имају потребу за одржавањем редовне комуникације ради обављања активности с друге стране закона. Разне криминалне групе којима су интернет и друштвене мреже потребни као инструмент повезивања са сарадницима на релативно удаљеним тачкама на терену, успевају да одрже комуникацију која и каква је до скора, из техничких разлога, била немогућа. Сада нова технолошка решења, посебно смарт телефони и мобилни интернет, активиран преко лаптоп или таблет рачунара, омогућавају брзу комуникацију, али и повећану мобилност, правовремено добијање информација о разним аспектима стања на терену. Захваљујући томе, они који се баве разним облицима кријумчарења, укључујући и кријумчарење људи, секс трафикинг, радну експлоатацију и слична кривична дела, успевају да се лако повезују и организују, укључујући ту и обмањивање многих који им се препуштају са поверењем, очекујући да ће им везе са таквим сојем људи помоћи у решавању неких егзистенцијалних проблема.

Евидентно је да скоро 18% млађих од 30 година остварује редовну или повремену комуникацију са непознатима. У контексту злоупотреба друштвених мрежа ова група корисника друштвених мрежа је потенцијално најугроженији од стране оних који друштвене мреже користе да би намамили жртве за своје криминалне намере. Посматрано према полу овакву врсту комуникације увек, често или понекад практикује 9,8% жена и 24,1% мушкараца. Крамеров V коефицијент унутар те старосне скупине је мали, али ипак статистички значајан ($V=0,19$; $p<0,000$). Можемо претпоставити да понекад жртве, нарочито унутар млађе женске популације, саме налазе понуде на подземном тржишту људи, сексуалних услуга или лажних пословних понуда, најчешће са сасвим другачијим намерама или наивним поверењем у он-лајн пријатеље који се често укључују на велики број профила и тиме аутоматски и без икакве провере постају пријатељи пријатеља и понекад задобијају бланко поверење без претходне провере. Мали је

корак да се од безазлене игре или наивног поверења упадне у замке организованог криминала.

Од највећег интересовања за савремено информационо-комуникационо друштво је да заштити своје ресурсе у овој области од криминала. Познавање карактеристика овог вида криминала требао би да буде један од приоритета.

Истраживањем у овој области добијени су резултати на основу којих се може рећи да Cyber криминал у Републици Србији прате следеће карактеристике:

- У Републици Србији, у теорији и пракси, појављују се као назаступљенија 3 термина: **високотехнолошки криминал**, **cyber (сајбер)** и **компјутерски криминал**. При томе под утицајем регулативе у којој је искључиво заступљен термин **високотехнолошки криминал**, поједини аутори аутоматски прихватају нормативно одређење, нарочито они који су повезани са борбом против овог криминала. Овај термин се налази и у преводу Конвенције о cyber (сајбер) криминалу, која је ратификована као Конвенција о високотехнолошком криминалу, иако у Будимпешти где је прихваћена није било те недоумице.
    - У теорији се код појединих аутора појављује и термин **cyber криминал**. Једна група аутора је остала код термина **компјутерски криминал** у својим старијим радовима, мада су неки и даље са овим термином у новијим. Модификација је присутна у термину **рачунарски криминал**. Једна од варијанти је термин **кибер криминал**.
    - Приликом дефинисања појма cyber криминала појавилили су се разни аспекти и приступи. Три су најчешћа: теоријски, нормативни и оперативни. У оквиру **теоријског** одређења појавило се више концепата: један полази од компјутерског криминала, други је окренут субер простору и трећи све посматра са аспекта различих наука и научних дисциплина. **Нормативни** приступ је везан за различита одређења у међународним, националним и саморегулаторним актима. **Оперативна** одређења полазе од потребе откривања, гоњења, хапшења, доказивања и кажњавања cyber учниоца.

Постоје бројне дефиниције cyber криминала, али било која дефиниција да се усвоји неспорна је чињеница да је cyber криминал комплексан, чак се сматра „кишобран"-термином који покрива разноврсне криминалне активности укључујући нападе на компјутерске податке и системе, нападе везане за компјутере, садржаје или својину, нарочито интелектуалну. Он је често транснационалан и понекад организован. У сваком случају то је феномен који има изузетан раст (по броју дела и категорија).

Да би се утврдио *modus operandi* учинилаца cyber криминала, анализира се начин понашања, односно како је и да ли је: **а)** била предузета припрема - учиниоци cyber криминала опсежно и систематски се припремају у више фаза; **б)** које су биле методе извршења дела - методологија извршења дела cyber криминала се стално усавршава; **в)** колико је било учниоца, односно осумњичених - појединци најмасовнија категорија, најопаснија и најатрактивнија је категорија организованог криминала, која је нарочито везана за групу кривичних дела против безбедности рачунарских података, али и одређена дела против полне слободе; и **г)** локација одакле су „оперисали" - учиниоци cyber криминала су често орјентисани на сопствену земљу и локалну заједницу.

Постоји велики број различитих класификација што показује разноврсност ових дела и комплексност њихових појавних облика, али и различитост критеријума који се користе.

Компјутерски криминал у бившој Југославији није новијег датума. Најважније је била, свакако, измена и допуна савезног Кривичног законика. У јуну 1998. године Радна група је припремила текст новог законика. Посебно поглавље (глава XXXIII) је било посвећено кривичним делима против система за електронску обраду података. Верзија посебног поглавља обухватала је пет кривичних дела. У каснијим верзијама преформулисани су наслови, чланови и њихов садржај. Пет, првобитно предвиђених, кривичних дела су преформулисана уз адекватну промену садржаја и уз додавање три нова.

Данас Кривични законик обухвата 8 кривичних дела груписаних у посебном поглављу *Кривична дела против безбедности рачунарских података:* оштећење рачунарских података и програма (чл. 298), рачунарска саботажа (чл. 299), прављење и уношење рачунарских вируса (чл.300), рачунарска превара (чл. 301), неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл.302), спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303), неовлашћено коришћење рачунара или рачунарске мреже (чл. 304), прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (чл. 304а).

Ако се узму у обзир и друга кривична дела која би могла да буду везана за одређене облике cyber криминала може се констатовати да је кривично законодавство Србије прилично опсежно испунило захтеве из Конвенције о cyber криминалу, али се ипак могу уочити да постоје одређена одступања.

У Кривичном законику дефинисан је покушај и саучесништво који су предвиђени по Конвенцији. Посебним Законом о одговорности правних лица за кривична дела прописана је и ова специфична кривична одговорност.

Учинио се и корак напред, тероризам који није предвиђен у Конвенцији, регулисан је, поред Кривичног законика и у посебном Закону о спречавању прања новца и финансирању тероризма, као и законима о потврђивању одговарајућих међународних аката (нпр. Закон о потврђивању Европске конвенције о сузбијању тероризма).

Међутим, у Кривичном законику нису експлицитно предвиђена као посебна кривична дела: незаконито пресретање (члан 3 Конвенције) и компјутерско фалсификовање (члан 7 Конвенције).

Конвенцију је пратио Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе, извршених преко рачунарских система, чија дела нису, такође, експлицитно инкриминисана у Кривичном законику.

Нека од процесних права предвиђена у Конвенцији унета су у Закон о кривичном поступку, али су изостале специфичности као што су: хитна заштита сачуваних рачунарских података, делимично откривање података о саобраћају и прикупљање рачунарских података у реалном времену.

Од 2005. године, када је донет Кривични законик Републике Србије, почела је нова ера регулације cyber криминала и нове тенденције у борби против њега.

Одељење за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Министарства унутрашњих послове Републике Србије и Одељење за борбу против високотехнолошког криминала Вишег јавног

тужилаштва у Београду подносили су пријаве за четири од осам дела која се налазе у Кривичном законику од:

а.) оштећење рачунарских података и програма
б.) рачунарска саботажа
в.) прављење и уношење рачунарских вируса
г.) рачунарска превара

Одељење за борбу против високотехнолошког криминала Министарства унутрашњих послова Републике Србије је од 2009. до 31. јануара 2014. године поднело већи број кривичних пријава за кривична дела против **безбедности рачунарских података** (за 7 од 8 кривичних дела), као и одређен број пријава за кривична дела против **привреде** (фалсификовање и злоупотреба платних картица) и кривичних дела против **полне слободе** (приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу). Учиниоци кривичних дела против безбедности рачунарских података су највише извршили дела рачунарске преваре и неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података.

Већина учинилаца cyber криминала у Србији је мушког пола (92,9%), док се жене ређе појављују као извршиоци (7,1%), при томе нешто мање од половине (45,4%) учинилаца женског пола није дела извршавало самостално већ су биле партнерке или познанице неког од чланова групе.

У Србији је, данас, највише учинилаца cyber криминала између 25 и 35 година (40,6%) старости. Ако се њима додају и они од 18 до 25 година (16,1%) добија се да су више од половине (57,6%) млади. Такође, у Србији нема учинилаца cyber криминала млађих од 18 година. Учинилаци дела cyber криминала који су деловали као група, има око две трећине (61,3%) између 25 и 35 година. За дела која су извршена у групи четвртина (25,8%) учинилаца је између 35 и 45 година, при томе ситуација је готово идентична и кад су у питању они који то извршавају самостално (24,5%).

Највише учинилаца дела cyber криминала има пребивалиште у Београду (38%), затим следе они из Војводина (27,7%), Шумадије и Западне Србије (22%), Јужне и Источне Србије (9,7%), са Косова и Метохије била је оптужена само једана особа, али се поступак водио против још неколико грађана те покрајине. Поред њих појавила су се и 3 учиниоца са пребивалиштем у Босни и Херцеговини. Нешто мање од половине (45,2%) учинилаца дела cyber криминала у Србији који су учествовали у групном (организованом) извршењу кривичног дела долазе из градова са више од 200.000 становника, а више од две петине (41,9%) је имало пребивалиште у градовима између 100.000 и 200.000 становника. На учиниоце cyber криминала се још увек не може применити географско профилисање.

У Србији је нешто мање од две трећине учинилаца овог криминала (61%) завршило средњу школу, око 22% има факултет, а највиши ново образовања, докторат, 3%. Само са завршеним основним образовањем је 12,9%, док је без икакве школе 1,9%.

Највише учинилаца cyber криминала (35%) у Србији има неко од занимања које припада техничко-технолошким струкама. На другом месту су учиниоци, четвртина од укупног броја, који уопште немају занимање. Занимања из друштвено-

хуманистичке групације има 18% учинилаца, а најниже учешће, по 4,5%, из области медицинских и природно-математичких занимања.

У Србији учиниоци cyber криминала долазе из свих социјалних група и имају различит радни статус: 58% учинилаца није у радном односу, 34% су стално запослени, 6% повремено ради или их издржава неко други, док пензионисаних лица има 2%. Имовину нема 88% учинилаца cyber криминала. Три четвртине запослених учинилаца нема имовину, док је то код незапослених још израженије. Незапослени учиниоци у 93,3% случајева су без имовине. Што се тиче учинилаца из групе пензионера и оних који раде повремено нико нема имовину. Највећи број кривичних дела која су извршили незапослени су дела против безбедности рачунарских података (33,3%) у односу на друга дела cyber криминала. Код кривичних дела против безбедности рачунарских података највећи број учинилаца није запослен (71,4%), мање од четвртине јесте (23,8%) и мали број ради повремено (4,8%). Нема пензионера у овој групи кривичних дела. Незапослени учиниоци у већем броју су извршавали дела у групи (28,9%) него запослени (9,6%). Ипак, извршење у групи није уобичајено ни за једну категорију учинилаца. Пензионери и учиниоци који повремено раде су кривична дела извршавали искључиво самостално.

Нешто више од половине (57%) учинилаца cyber криминала у Србији нису удати или ожењени. Проценат учинилаца cyber криминала који су у брачној заједници је 32%, они који су разведени 8%, а у ванбрачној заједници живи 3%. Нема удоваца/удовица. Учиниоци cyber криминала у Србији који су у брачној заједници су скоро у једнаком броју запослени (46%) и незапослени (44%), док 10% повремено ради. Велика већина (72%) нема имовину, а само 28% је поседује. Они који су неожењени/неудати су нешто мање од две трећине (65,2%) незапослени и скоро уопште немају имовину (98,9%). Већина учинилаца cyber криминала (62,6%) нема децу, 35,5% има до троје деце, док оних који имају више од је 1,9%. Скоро две трећине учинилаца cyber криминала у Србији који немају децу су незапослени (63,9%) и немају имовину (94,8%). Око половине незапослених учинилаца има до троје деце (49,1%). Нешто мање од половине запослених учинилаца има до троје деце (45,5%). Четвртина оних (25,5%) који имају до троје деце поседују имовину.

Већина учиниоци cyber криминала у Србији (77%) није било раније осуђивано. Од 23% учинилаца који су били раније осуђивани 55,6% је било осуђивано само једном, 19,4% више пута, док за 25% осуђиваних нема података о осуђиваности (не зна се да ли су осуђивани једном или више пута). У већини случајева неосуђиваних је процентуално било више у односу на осуђиване са истим нивоом образовања, изузетак су они са вишом школом којих има више у категорији осуђиваних. Нешто мање од четвртине раније осуђиваних за cyber криминал је завршило само основну школу (22,2%), док нешто више од две трећине има средње образовање (66,7%). У групи са рецидивом јасно је изражен тренд повећања учешћа учинилаца са средњом школом (мада је виши код учинилаца cyber криминала са рецидивом него код других облика криминала). Распоред је исти и кад су у питању учиниоци са основном школом, а разлике су нарочито код учинилаца са факултетом и докторатом, којих нема међу учиниоцима cyber криминала са рецидивом, али их има међу неосуђиваним. У овој групацији највише је са средњом, а најмање са вишом школом, односно без школе. Од оних који нису претходно осуђивани нешто мање од две трећине је са завршеном средњом школом (58,8%) и нешто мање од четвртине са високим образовањем (24,4%).

Нешто мање од трећине (30,6%) осуђиваних за дела cyber криминала у Србији је извршило дело против интелектуалне својине, док је 36,1% извршило дело против безбедности рачунарских података. Највећи део (37,8%) учинилаца који нису претходно осуђивани извршили су дело против полне слободе, а четвртина (24,4%) од укупног броја је извршила дело против безбедности рачунарских података. Нешто више од петине учинилаца ових дела који су раније били осуђивани служили су војни рок. Од неосуђиваних више од половине (55,5%) га је служило. Међу њима су и жене. Иако малобројне (9,24%) ипак их је више него оних који су били ослобођени служења (4,2%). Учиниоци из Београда су најактивнији у односу на рецидивизам (38%:44,4%), слично је и са Шумадијом и Западном Србијом (22%:27,7%). Раскорак се бележи у Војводини (27,74%:11,1%). Учиниоци ових дела, који нису претходно осуђивани, у највећем броју имају пребивалиште у Београду (36,1%), док их је нешто мање са пребивалиштем у Војводини (32,8%).

Начин извршења дела са аспекта броја учинилаца cyber криминала и основних социо-демографских карактеристика учинилаца у Србији показују значајну везу. Старост има ниску, али статистички значајну везу са начином извршења ових кривичних дела. Исто је и са пребивалиштем, односно регионом, величином места, као и са радним статусом, имовином и рецидивизмом.

Однос између броја извршилаца по групама дела указује на доминантност самосталног извршења, једино је код дела против безбедности рачунарских података превага на групном (организованом) извршењу.

Дакле, учиниоци кривичних дела против безбедности рачунарских података су доминантно мушког пола (83%). Скоро две трећине (60%) учинилаца је старости између 25 и 35 година и углавном су из Београда са околином (40,5%) или из градова чији је број становника између 100.000 и 200.000 (36%). Најчешће се њихов степен образовања завршава на средњој школи 57%, док је факултетски образованих 21%. Техничко-технолошким занимањима се бави 29% учинилаца, 26% немају занимање, а за 21% случајева подаци о занимању нису доступни. Запосленост је на ниском нивоу (посао има 24%), док проценат оних који нису у радном односу је вишеструко већи (73%). Брачног друга има 31%, а потомке 9% учинилаца. Војни рок је служило њих 63%. Претходно је осуђивано 31%.

Сва кривична дела против полне слободе као групе дела cyber криминала у Србији извршили су мушкарци. До сада није забележено да је било учинилаца женског пола. Они су углавном преко 45 година (34%) и између 25 и 45 година (30%). Већина је из Војводине (40%), па из Београда и околине (22%). Пребивалиште у местима изнад 200.000 становника има 40% учинилаца. Образовање код ове групе учинилаца је слично као и код осталих, половина их има завршену средњу школу, а факултет има 24%. Забележени су и случајеви у којима учиниоци имају докторат. Са техничко-технолошким занимањима је скоро трећина (30%) учинилаца. Запослених има мање (44%) него незапослених. Имовину поседује 22% учинилаца. Многи учиниоци ових дела имају формирану породицу, у брачној заједници или разведених је 81%, а 9% живе у ванбрачној заједници. Децу има нешто мање од половине (44%) учинилаца. У овој групи 28% учинилаца је ослобођено служења војног рока (болест, инвалидитет), док је 64% одслужило. Осуђивано је 28% учинилаца од којих је 4% осуђивано више пута.

Карактеристике учинилаца дела неовлашћеног искоришћавања ауторског дела и предмета сродног права (члан 199 Кривичног законика) су следеће: 96% су мушког пола, углавном између 25 и 35 година (37,5%) и са пребивалиштем у

великим градовима (67%), средњег су образовани (67%), нису запослени (63%) и ни један нема имовину. У браку је 42%, 37% има до троје деце, а више их има 8%. Војску је служило 65%. Раније је осуђивана скоро половина (46%), од тога: 72% је осуђивано једном, а 28% више пута. Најчешћи мотив извршења дела је новац.

Карактеристике учинилаца дела угрожавања сигурности (члан 138 Кривичног законика) преко интернет сајтова, на друштвеним мрежама (*Facebook*), као и путем електронских порука, чији садржај представља озбиљну претњу појединцима и групама су: 96% мушкарци из Београда и околине; 44% има пребивалиште у градовима са више од 200.000 становника. Већина је завршила средњу школу (72%). Скоро половина је запослена (48%), али нема имовину. Углавном немају брачни статус (76%) и немају децу. Пошто је већина млађа од 25 година нису служили војску. Мало их је претходно осуђивано (16%) и то само једном.

II Ставови према појединим делима cyber криминала у Србији су следећи:

Страх и перцепција криминала у јавности под утицајема медија стварају *perpetum mobile* ефекат проузрокујући моралну панику. Мапирање и мерење страха, односно његовог интензитета и утицаја на перцепцију друштва постало је пратећа појава уз мерење и тумачење самог cyber криминала.

Истраживање које је спроведено у мају 2013. године обухватило је и 23 питања везана за одређене облике злоупотреба интернета и друштвених мрежа, односно дела cyber криминала. Један део питања био је усмерен на добијање одговора о свести (перцепцији) опасности и постојању страха од cyber криминала.

Подаци из истраживања у Србији указују на недовољну упознатост са хакингом као обликом cyber криминала.

На питање шта је хакинг:

А.) 37% испитаника одговорило потврдно од тога је било више из мушке популације (55,2%) од оних из женске (44,8%). При томе је више испитаница од испитаника одговорило да је чуло али да не зна ништа о томе;

Б.) највећи проценат (55%) који о хакингу ништа не зна је оних између 18 и 30 година старости, затим следе они који имају мање од 18 (35%), преко 45 (23%), а од 30 до 45 година свега је 6% оних који не знају. У групи испитаника до 18 година најмањи проценат је оних који не знају шта је хакинг у популацији од 14 до 16 година, али процентуално у целој овој популацији они су и групација која највише зна шта је то (скоро 54%);

В.) преко 44% свих испитаника зна шта је хакинг без обзира на величину места пребивалишта. Најмање знају испитаници из места мањих од 5000 становника (36,1%), највише из места од 5000 до 20.000 становника (52,8%), а ни испитаници из Београда у великом проценту не знају (43,1%);

Г.) 25,4% жена које су одговориле да знају је између 18 и 35 година старости, а мушкараца 29,3% у истој доби.

На питање да ли сте некада били жртва хакинга:

А.) 13,9% је оних који су одговорили да су били жртва;

Б.) жене су у 14,7% одговора потврдиле да су биле жртве и 13% је то био случај са мушкарцима. Доминантан за обе категорије испитаника је негативан одговор (мушкарци 62,7%, а жене 59,7%). За одговор „не

знам“ испитанице су се определиле за 1,3% више него испитаници (25,6% : 24,3%);

В.) 19,8% испитаника који је дало одговор да су били жртве хакинга, било је из групе до 18 година;

Г.) у местима до 5000 становника број испитаника је потврдио да не зна да ли су или не били жртве хакинга (20,9%), што је слично броју испитаника из места од 5000 до 20.000 становника (18,1%). Највећи проценат у свим групама се определио за одричан одговор и креће се између 58,1% (из места до 5000 становника) до 63,9% (из места 5000 до 20.000);

Д.) највећи број жртава хакинга био је у групи од 18 до 30 година, у местима до 5000 становника (23,2%), а 22% је младих испод 18 година у градовима преко 500.000 становника;

Ђ.) испитаници који су били жртве хакинга одговорили су да знају шта је хакинг у 68,7% случајева, а њих 28% су чули. али не знају шта је. За оне који не знају да су били жртве 27,1% зна шта је хакинг, 40,3% је чуло, али не зна ништа о томе и 32,6% не зна шта је то.

На питање шта је *phising*:

А.) испитаници су одговарали у великом проценту да не знају (65,3%) или да су чули, али ипак не знају шта је то (25%). Мали број је оних који тврде да знају шта је то;

Б.) испитаници знају више шта је (13,4%) од испитаница (5,7%);

В.) испитаници различитих година су различито одговарали на питање шта је *phishing*. Дистрибуција се креће од 62,2% (од 18 до 30 година) до 83,9% (преко 45 година). Најмлађи су се у 66,1% случајева изјаснили негативно;

Г.) највише знају они из места између 20.000 и 100.000 (10,63%) и између 100.000 и 500.000 становника. Најмање је код испитаника до 5000 становника. У великим градовима (изнад 500.000 становника) 10% зна. Потпуно негативни одговор дали су испитаници из места свих величина и крећу се између 63,7% (од 100.000 и 500.000) и 72,7% (до 5000);

Д.) 91,3% испитаница преко 45 година не зна уопште, а 28% младих испод 18 година женског пола се определило за овај одговор. 15,28% мушкараца између 30 и 45 година зна, док су најмање позитивних одговора дале су младе испитанице до 18 година, а највише између 30 и 45 година.

На питање о томе да ли су били жртве *phishing*-а:

А.) већина испитаника је одговорило да не зна да ли су или не били жртве (51,8%), а изузетно мали проценат (3,4%) је одговорило да су били;

Б.) највећи проценат испитаника оба пола је одговорло да не знају да су били жртве (жене 55,8%, мушкарци 48%). Испитаници су скоро исто (само за 0,3% разлике) одговорили да не знају и да нису били жртве;

В.) испитаници су више од 50% одговарали да не знају да су били жртве, изузев оних до 18 година чији одговори су минимално били испод овог процента (48,9%);

Г.) доминантни одрични одговори карактеристични су за испитанике из места од 5000 до 20.000 становника јер у местима са више од 20.000 становника највише је одговора да не знају да су били жртва (50% и >%);

Д.) мушкарци до 18 година највише су се изјаснили да су били жртве (6,8%), док се тако изјаснило 6,4% жена од 30 до 45 година*;*

Ђ.) мушкарци из места између 5000 и 20.000 становника (6,5%) и преко 500.000 (6,3%) зна шта је *phishing*.

На питање да ли имају искуства са насиљем преко друштвених мрежа/ cyber малтретирањем (10 понуђених одговора - 8 потврдних и 2 одрична):

А.) скоро 90% испитаника је одговорило да нису били жртве, али знају да су то неки доживели (53,5%) и да никад нису за то чули (35,7%), док 3 одговора који су преко 2% је било: да, гледао/ла сам више пута клипове и фотографије малтретирања (2,9%); да, „шалимо" се често због разних „глупости" које неки постављају (2,5%); и 2,1,% испитаника је одговорило да је учествовало о томе, што је крајње забрињавајуће;

Б.) највећи проценат испитаника оба пола је одговорио да нису били жртве али да знају неке који јесу: испитанице 26,8%, а испитаници 25%. Никад нису чули „подједнако" и мушки (18%) и женски (17,7%) испитаници. У 1,6% случајева испитаници су активно учествовали у овом облику малтретирања и пасивно 2% („шалили ...");

В.) највећи проценат испитаника између 18 и 30 година одговорило је да нису били жртве, али знају неке који јесу (58,3%). Готово половина (49,1%) оних преко 45 година старости није чула, а за све остале одговоре ирелевантне су старосне групе;

Г.) највише испитаника из свих места се определило за одговор да нису били жртве (50 и >%) али да знају неке који су то доживели, једино мање је испитаника из места до 5000 становника који су се за овај одговор определили у 43% случајева. Иста групација је у нешто мањем проценту (40%) одговорила и да није чула за cyber малтретирање. Сви остали испитаници су у мањем проценту изабрали овај одговор;

Д.) највећи проценат који нису доживели/е cyber малтретирање али знају ко јесте су жене између 18 и 30 година (62,8%), а најмањи преко 40 година (52%). Испитаници преко 45 година подједнако су одговорили да знају да су неки други били жртве ове појаве;

Ђ.) преко 50% испитаница је одговорило да то нису никад доживеле али да знају неког ко јесте у свим местима која су праћена по величини, осим из места до 5000 становника (44,2%). Најмањи проценат од свих испитаника који нису чули за електронско малтретирање су испитанице из места од 5000 до 20.000 становника (30,9%). Испитаници из било којих места су просечно необавештенији од испитаница;

Е.) они који никад нису чули за ову појаву су >50% становници места са >500.000 становника у старосној групи од 30 до 45 година (52,8%) и преко 45 година (63%). Најбоље су обавештени (25%) испитаници од 18 до 30 година у местима од 5000 до 20.000 становника;

Ж.) значи, о cyber малтретирању испитаници нису добро обавештени, али и нису често били његова жртва. Неки познају неког ко је то био. У незнатном броју су учествовали у томе; основали групу која је против насиља; гледали више пута клипове и фотографија малтретирања; често се „шалили" због разних „глупости" које је неко други поставио; постављали њихове понижавајуће фотографије и исмејавали их; вређали их и

називали свакаквим именима или добијали претње више пута. Искуства која су стицали не зависе од величине места из којих су, али у неким случајевима зависе од пола и година старости.

На питање „Да сте „налетели“ са говор мржње на интернету да ли бисте?“ (понуђено је 6 одговора):

А.) више од половине испитаника (60,6%) би на ову појаву заборавило јер их не занима;

Б.) 19,2% би то пријавило администратору, 2,2% би оставили похвални коментар, 7,1% би се насмејали и лајковали да се слажу, а мали број би то пријавило полицији (3,9%);

В.) највећи проценат испитаника оба пола би заборавило јер их не занима шта други раде: жене 31,4%, а мушкарци 29,1%, пријавило би администратору 9,2% : 9,8%, најмање су се обе групе испитаника определиле да би оставили похвални коментар (жене 0,5%, мушкарци 1,6%);

Г.) највећи проценат свих старосних група се определио за заборав и пасивност, највише старији од 45 година (69,8%), а најмање млађи од 18 година (54%). Најмлађи највише од свих група би говор мржње пријавили старијима (17,1%), а мали број би пријавило полицији (4,9%), што би урадили и они преко 45 година (4,8%). Старији од 45 година не би уопште остављали позитивне коментаре, док су најмлађи одговорили да би се највише смејали и „лајковали“ такве садржаје. Најчешће би пријавили администратору испитаници између 30 и 45 година (27,6%). Све старосне групе су резервисане у пријављивању полицији;

Д.) испитаници из свих места процентуално најмање би оставили похвални коментар, с тим што се у овој малој групи „истичу“ они из места до 5000 становника (3,6%). Забораву би прибегли највише становници места између 20.000 и 100.000 становника (66,9%), а најмање између 5000 и 20.000 (58,1%). Испитаници из градова већих од 500.000 становника, после пасивности и заборава, највише су се определили за пријаву администратору (21,5%). Пријавили би полицији највише испитаници из места до 5000 (6,4%), а најмање између 100.000 и 500.000 становника (2,7%);

Ђ.) највише мушкараца преко 45 година је одговорило да би заборавило јер их не занима шта други раде, док испитаници преко 45 година оба пола не би оставили похвалне коментаре за поруке које носе cyber мржњу. Припаднице „лепшег“ пола између 30 и 45 година нису бирале овај понуђени одговор;

Е.) жене би највише заборавиле јер их то не занима ако су из места величине између 20.000 и 100.000 становника (71,4%). Ово је домиинантан одговор и за мушкарце из таквих места. Преко 11,5% мушкараца из места до 20.000 становника лајкују говор мржње, а жене из ових места су мање екстремне (око 8,7%);

Ж.) највећи број одговора везаних за заборав, најмањи број остављања похвалних коментара или пријављивања администратору дали су испитаници из места од 5000 до 20.000 становника, старости између 30 и 45 година (50%). 3/4 испитаника старих преко 45 година из градова

> већих од 500.000 становника највише су склони забораву. Млађи од 18 година, поред заборава, највише су се усмерили на пријаву старијима ако су из места између 100.000 и 500.000 становника (22%), односно из места између 20.000 и 100.000 становника (18%).

Имајући у виду значај друштвених мрежа и савремених облика комуникације путем информационих мрежа, као и наведених карактеристика *cyber* криминала јасно је уочљива чињеница да сви фактори друштва, али и међународна заједница уопште, имају велику одговорност у ефикасном регулисању ове области и правовремене заштите корисника информационо-комуникационих технологија. У том контексту посебно је битно нагласити да је у марту 2012. године, Европски савет Републици Србији доделио званичан статус државе кандидата за чланство у ЕУ, а 28. јуна 2013. године је донео и одлуку о отварању преговора о приступању Републике Србије Европској унији. У Бриселу је јануара 2014. године одржана прва међувладина конференција између Републике Србије и Европске уније, чиме је означен почетак приступних преговора на политичком нивоу.

Почетна фаза преговора – аналитички преглед и оцена усклађености прописа Републике Србије са правним тековинама Европске уније и њихове примене (скрининг), већ је започела у септембру 2013. године и обухватиће сва поглавља преговора, а трајаће до марта 2015. године.

У оквиру преговарачког поглавља 10 – Информационо друштво и медији, обухваћена је и област информационе безбедности.

Сматрамо да је паралелно са преговорима од велике важности што је ово научно истраживање својим резултатима указало на потребу усклађивања правних прописа и организационих решења према моделу који је примењен у Европској унији.

Такође наглашавамо и да је у области cyber криминала потребно усагласити термине, одређења и класификације и ускладити их са свим међународним документима. Од велике је важности припрема и усвајање националне стратегије cyber сигурности која би била усклађена са Стратегијом Европске уније, као и оснивање CERT-а (Computer Emergency Team). У нашој држави још увек није установљен ефикасан *CERT*-тим (*Computep Emepgency Responce Team*) за спречавање ових кривичних дела, нити су одређене институције чији би представници требали да се ангажују у овом правцу. Успостављање *CERT* тима у великој мери би допринело ефикаснијем спречавању ових кривичних дела, бржем и одговорнијем приступу у истраживању ове појаве и обједињеном одговору на изазове и претње које ова појава доноси.

Имајући у виду сталне модификације cyber криминала и усклађивање начина извршења са савременим трендовима у развоју информационо-комуникационих технологија требало би предузети организоване, синхронизоване и институционализоване активности континуираног праћења *modus operandi* учинилаца cyber криминала кроз: с једне стране, дефинисање анализа које је неопходно вршити (прихватањем упитника које треба користити на исти начин као што се користе друге земље), а с друге, усаглашавање са методологијом, критеријумима и показатељима дефинисаним од стране УН и Европске уније. Потребно је размотрити могућност да се у Кривични законик Републике Србије унесу дела која су предвиђена у Конвенцији о cyber (високотехнолошком) криминалу која до сада нису експлицитно предвиђена као посебна кривична дела

као што су незаконито пресретање (члан 3 Конвенције) и компјутерско фалсификовање (члан 7 Конвенције). Препорука је, у скалду са резултатима истраживања које је спроведено, да је потребно посебно инкриминисати дела крађе идентитета и *phishing-a*.

Требало би и боље дефинисати кривична дела из Додатног протокола уз Конвенцију о cyber (високотехнолошком) криминалу која се односе на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, а која нису експлицитно инкриминисана у Кривичном законику.

У Закон о кривичном поступку Републике Србије потребно је унети специфичности као што су: хитна заштита сачуваних рачунарских података, делимично откривање података о саобраћају и прикупљање рачунарских података у реалном времену, а које су дефинисане у Конвенцији.

Истраживање је показало и да је потребно систематски и континуирано пратити учиниоце, дела и жртве cyber (високотехнолошког) криминала по свим социодемографским и другим показатељима. Ради боље организације и ефикасности државних органа против овог вида криминалитета сматрамо да би посебно било добро да се на одговарајућим местима запосле службеници који би на ефикасан начин, а на основу расположивих података анализирали феномен и припремали одговарајуће извештаје који би послужили за ефикасније супротстављање овом виду криминалитета. Од великог значаја је и организација континуираног праћења коришћења информационо комуникационих технологија за извршавање кривичних дела у Републици Србији, посебно ради припреме адекватних анализа, студија, извештаја за надлежне институције, одговарајуће међународне субјекте, јавност и то нарочито научну и стручну.

Искуства Министарства унутрашњих послова Републике Србије у борби против високотехнолошког криминала говоре о томе да се ради о кривичним делима чији се појавни облици мењају у веома кратком року са појавом нових техничко-технолошких решења, као и да се ова кривична дела чине у веома кратком времеском року, готово свуда где постоји интернет - па самим тим и у Републици Србији. Са феноменом вискотехнолошког криминалитета су се, поред Одељења за борбу против високотехнолошког криминала, у оквиру Министарства унутрашњих послова, суочиле и друге организационе јединице, а сузбијање великог броја појавних облика високотехнолошког криминалитета, посебно оних са елементима организованог и транснационалног криминала, на територији Републике Србије данас је веома сложен и тежак задатак, који из дана у дан представља све већи изазов за Министартво унутрашњих послова Републике Србије. Савремене информационе технологије, меморијски капацитети рачунарских мрежа и глобална дистрибуција података и информација додатно отежавају могућност откривања ових кривичних дела и проналажење извршилаца.

Cyber криминал је мултидисциплинарна појава, па зато сматрамо да је потребно формирати мултидисциплинарне и мултиинституционе тимове за изучавање, праћење и анализирање специфичности cyber криминала, учинилаца и жртава. Ради адекватног прикупљања података потребно је испитати јавно мњење о перцепцији опасности од cyber криминала, по узору и уз помоћ усвојене методологије других земаља и међународних организација.

Међународна сарадња у овој области је од пресудног значаја и за превентивне и за репресивне активности, па је значајно размотрити и искористити

могућности за повезивање са истраживачким центрима из других земаља како би се могла радити компаративна анализа резултата добијених истраживањима.

Млади су веома угрожени овим видом криминала, па посебно треба имати у виду потребу њихове адекватне заштите. Зато је стално истраживање облика cyber криминала у образовним институцијама од велике важности, узимајући у обзир чињеницу да се, након добијених резултата могу сачињавати предлози конкретних мера на нивоу друштва, образовних институција, породица, деце/младих. За ове институције би било потребно сачинити програме посебних тренинга (нпр. за директоре школа, професоре, наставнике и учитеље, као и школске одборе, форуме школа, родитеље).

Вршњачко насиље, као друштвено непожељно понашање, најчешће се реализује злоупотребом информационо-комуникационих технологија. Како би се утицало на ту област битно је да се припремају програми за вршњачку едукацију о опасностима везаним за коришћење интернета, друштвених мрежа, мобилних телефона и других уређаја и медија.

Средства јавног информисања имају важну улогу у превенцији cyber криминала. Како би се њихова улога повећала и како би се ресурси ангажовали у пуном капацитету потребно је припремити програме и планове едукације новинара ради одговарајућег извештавања и праћења ових проблема.

Чињеница је и да су последице високотехнолошког криминала врло често за жртве такве да изазивају психичке и друге проблеме, зато сматрамо да је важно да друштво формира посебна саветовалишта за жртве овог вида криминала, која би се посебно бавила младима.

Сматрамо и да је евидентирање недозвољених садржаја на интернету и друштвеним мрежама, који могу угрозити одређене групе корисника и обавештавање државних органа и других заинтересованих страна, посебно важно и да би требало да буде организованије, те да је потребно подстицати посебне „узбуњиваче“ у друштву који би се бавили прегледом садржаја и пријављивањем нелегалних активности.

У прилог наведених препорукама иду и резултати добијени у оквиру анкета које су спроведене у државним органима, а који се баве спречавањем високотехнолошког криминала. У њима је учествовало 48 испитаника оба пола, различитих старосних доби, занимања, економског статуса и друго. У одабиру узорка се водило рачуна да буде довољан број испитаника, али је обраћена пажња и на то да расподела испитаника не буде крајње диспропорцијална по полу и другим критеријумима. Узорак су чинили припадници полиције, Управа граничне полиције и Служба за борбу против организованог криминала - Одељење за борбу против високотехнолошког криминала, Више јавно тужилаштва у Београду, односно Одељење за борбу против високотехнолошког криминала, као и судије. Закључај истраживача је да је узорак према свим анализама свеобухватан по свим критеријумима.

Реултати истраживања указали су да је потребно у првом реду уредити стандардне оперативне процедуре у погледу поступања са дигиталним уређајима, односно предвидети одговорност свих припадника полиције у поступању са оваквим дигиталним траговима, поред постојећих законских и подзаконских аката. Након овога неопходно је прибавити адекватне уређаје и софтвере који у том смислу могу бити коришћени на адекватан начин (почевши од адекватне опреме за безбедан

транспорт привремено одузетих предмета, њихово складиштење у адекватним условима, опреме за форензичка вештачења и слично).

Код кривичног дела из чл. 185б резултати показују да се у овој области криминалитета мора предвидети начин за боље проактивно деловања, односно да треба водити рачуна о примени мера из Маријиног закона на извршиоце овог дела. Само на тај начин и генерална и специјална превенција могу имати смисла.

Код кривичних дела везаних за злоупотребе ауторских и сродних права и дела из чл.198, уочено је да се у моменту истраживања најчешће јављају различити облици искоришћавања ауторског дела путем интернета, али је у највећој заступљеност П2П или *torrent* размена материјала. Сви остали облици се јављају много мање. Проблеми са којима се у овој области сусрећемо везују се и за могућност идентификовања извршилаца у оваквом начину размењивања ауторски заштићених материјала. Иако постоје контакти и жеља да се сарадња продуби и у овој области са произвођачима главних *torrent* клијената, као и простор за бољу полицијску сарадњу, неопходно је да се ова област додатно нормативно уреди и да се дају шира овлашћења органима гоњења у погледу остваривања увида у индивидуалне идентификујуће карактеристике корисника који дистрибуирају недозвољени материјал.

У вршењу кривичних дела из ове области је померен простор у виртуелно окружење, од којих предњаче средства ИКТ, рачунари, интернет, комуникација преко „SAAT“ затворених соба за чет. Један од понуђених одговора (2.08%) веома интересантно позиционира и нека кривична дела извршена преко интернета у дела која се врше путем уцене или принуде. У погледу поступања поводом овог дела, у вези његовог расветљавања и откривања учиниоца, смернице се могу свести на отежавање приступа оваквим средствима и пооштравање казнене политике према учиниоцима. Са друге стране интересантно је размотрити шта су све испитаници понудили као предмете кривичног дела. Једна од група предмета који су објекат дела били су: текстови у часописима, рекламни материјал и публикације. Потребно је у том смислу усмерити рад у области ОСИНТ-а и потпуније регулисати примену алатки у вези окружења отворених извора, а такође и продубити обуке којима би се оперативци и тужиоци упознали са овим оруђима.

У погледу спречавања и сузбијања ове групе кривичних дела веома је интересантно размотрити мере предвиђене у СОПА у САД или Хадопи закон у Француској, којима се веома значајни резултати могу постићи у овој области у погледу спречавања пиратерије која је у нашој земљи дефинитивно узела маха. Суштина мера јесте да се превентивни део активности препусти ИСП–овима и да се њима да оруђе којим би се корисницима њихових услуга ускратиле услуге на одређено време, а да то буде праћено реакцијом државе у смислу санкција према учиниоцу кривичног дела, које иду чак дотле да се одређеном лицу забрани коришћења интернета као вид мере безбедности или алтернативне санкције.

Такође је могуће додати још једну смерницу у вези свих представника носилаца права, где је веома лако од удружења лица која су носиоци права захтевати да се оформи један јаван регистар носилаца права и њихових аступника истих, како би се лако отклањале препреке које би подразумевале њихово проналажење, чиме би се смањило време неопходно за тако нешто. Ова ситуација, такође, не би изискивала више средстава јер се може организовати, а што ми сматрамо легитимним предлогом, на нивоу отвореног и јавног регистра. Њега би користили носиоци права и он би у облику форума могао бити примерен за

изношење проблема, деловање узбуњивача и био би одржаван од стране носилаца права.

У вези са овом групом дела, посебно у погледу члана 200 КЗ РС неопходно је пооштрити казнену политику у погледу неовлашћене продаје и дистрибуције уређаја који се, у овом смислу, могу користити и инкриминисати припремне радње у правцу прављења и прибављања оваквих уређаја.

Код члана 225 КЗ РС треба инкриминисати и само прибављање ових података и њихово нуђење на продају пооштравањем казнене политике у погледу казни за ово дело, а овакав коментар се може дати и за кривична дела из чл. 300, 301 и 302. Посебно је значајно напоменути да је неопходно инкриминисати кривично дело крађе идентитета, посебно крађе он-лајн идентитета.

Анкете спроведене у Привредној комори Србије код интернет сервис провајдера спроведене су на 5 испитаника. У одабиру узорка се водило рачуна да буде довољан број испитаника. Узорак су чинили представници привредних друштава који која се баве пружањем услуга интернета. Узорак је према свим анализама свеобухватан по свим критеријумима. По многим критеријумима он јесте репрезентативан за популацију.

Једна петина испитаних провајдера интернет услуга је учествовала у некој од посебних акција из области ВТК. Као једна од смерница и препорука у овој области могла би се извести потреба да се оваква активност прошири и омасови, с обзиром да је приватно јавно партнерство ИСП и државе у овој области неопходност. Ова сарадња мора бити и институционализована и не сме се догодити да представници било које од страна имају јачу позицију или да се понашају као супротстављене стране, такође мора се препознати обострани интерес у заштити крајњих корисника грађана и у сваком случају морају се поштовати права и слободе грађана. Тежи се да субјекти из јавног и приватног сектора предузму одређене активности у циљу што боље заштите ИКТ система. Очекујемо од провајдера и ИКТ индустрије да се усредсреде на развој сигурности, приватности и употребљивости производа, процеса и сервиса у циљу превенције и борбе против крађе идентитета и других напада на приватност. Такође је неопходно да мрежни оператори, провајдери и приватни сектор деле и примењују добре безбедносне праксе и да негују културу анализе ризика и управљања у организацијама и пословању организовањем одговарајуће обуке, као и да успоставе безбедна решења доступна корисницима.

Са обзиром да је ова област у одређеним државама, које су познате по својим залагањима за примену и неограничавање слобода и права човека и грађанина, регулисана и на начин да се у одређеним случајевима оваква права и слободе могу ограничити (већ поменути Хадопи закон и СОПА), није невероватно да се и код нас, у некој блиској будућности, уведе некакав облик ограничења права и слобода у погледу приступа интернету. У нашој анкети сви представници ИСП су изнели да никада нису блокирали приступ корисницима услуга.

Ови резултати су управо значајни зато што је у савременим друштвима тенденција да се овим путем промовише сигурност ИКТ система и одговорност за њихову заштиту. Такође, жеља нам је била да се овим омогуће адекватне едукационе активности у овој облати и да се шири свест о значају проблема ИКТ веза са ВТК и ирегуларним миграцијама и трговином људима, поготово међу младим људима, као носиоцима промена у држави, највећих корисника ИКТ и могућих будућих жртава. Такође сматрамо и да би било потребно да се предузму одговарајуће мере како бисмо реаговали на сигурносне инциденте нарочито кроз:

континуирано побољшање метода идентификације и утврђивања безбедносних проблема, примену адекватне контроле, успостављања ефективне комуникације у са вези сарадњом свих заинтересованих страна у овом процесу, размену информација о најбољим праксама земаља чланица, подстицање сарадње између академске заједнице и привреде како би се развиле технологије и услуге у складу са прихваћеним стандардима. Управо ово и јесте био циљ овог истраживања. Наша тежња је и да сви релевантни субјекти у држави предузму мере које ће допринети очувању безбедности ИКТ система у Републици Србији, у циљу унапређења стања у овој области. Позивамо и да се подрже обуке и подигне свест у области безбедности ИКТ система, повећају контрибуције намењене научно-истраживачком раду и унапреде приступачност и ширење добијених резултата. Жеља је и да се подстакне развој сарадње у циљу раста ИКТ индустрије. Циљ који промовишемо и покушавамо да остваримо је да се обрати посебна пажња на превенцију и борбу против нових и постојећих безбедносних претњи електронским комуникационим мрежама. Да се формира Национални ЦЕРТ тим. Наша препорука је и да се подстакну и обавежу провајдери и мрежни оператери да обезбеде адекватан ниво безбедности ИКТ система. Наш је предлог и да се предузму мере да јавни сектор буде пример добре праксе тако што ће се омогућити сигурне услуге електронске управе. Наш предлог је и да привредни субјекти развијају позитиван однос према безбедности ИКТ система како би производили унапређеније и сигурније производе. Такође подстичемо произвођаче и провајдере да испуне захтеве за заштиту приватности, безбедност и поузданост својих производа и сервиса у циљу превенције незаконитих активности њихових корисника. Подстичемо заинтересована лица да сарађују и покрену експериментална окружења за развој нових технологија и сервиса; да усвоје нове технологије и сервисе за производе који су у комерцијалној употреби. Наша смерница иде и ка томе да сва заинтересована лица трба да учествују у борби против спама и других лоших пракси.

Заштита приватности на интернету широм света заузима велику пажњу јавности и покренуте су многе расправе о овој актуелној теми. Застарела регулатива у области заштите података о личности, у којој нису препознате специфичности прикупљања, обраде, чувања и дељења података на интернету, захтева хитну измену и допуну. Предлози Европске комисије за свеобухватну реформу Директиве за заштиту података 1995 ЕУ имају за циљ да ојачају права на приватност и регулишу европску дигитална економију. Постоји јасна потреба да се затвори растући јаз између појединаца и компанија које обрађују податке о личности. Тек усвојена Директива захтева нови приступ заштити података о личности. Канцеларија Повереника за информације од јавног значаја и заштиту података о личности припрема нови Закон у овој области који ће пратити савремене токове и прилагодити се понашању појединца, штитећи једно од основних људских права - право на приватност. Након пуних пет година примене Закона и даље нису донети бројни подзаконски акти који би ближе уредили ову област. Иницијатива Повереника да се Закон мора мењати како би примена била адекватна, још увек није наишла на подршку надлежних органа. У Централни регистар уписано је свега неколико стотина база података иако их има на десетине хиљада. То потврђује наводе експерата и бројних удружења који инсистирају на бољем регулисању права на приватност и озбиљнијем бављењу овим проблемом.

Кључно је да се за сва наведена дела, којом је инкриминисана повреда приватности и неки вид злоупотребе података о личности, поступак покреће по приватној тужби, сем када то учине службена лица у обављању службе када се гоњење предузима по предлогу. Тиме је држава препустила појединцу да се за остварење овог права сам бори. Поставља се питање да ли је тежина ових дела адекватно регулисана јер је за остале слободе и права човека (равноправност, право на употребу језика и писма, изражавање националне или етничке припадности, слобода кретања, исповедања вере и друга) предвиђено да држава мора да интервенише. Изменом одредби Кривичног законика порука свима који су спремни да занемаре право да „вас оставе на миру“ би била јаснија. Крађа идентитета и разни видови преузимања података о личности на интернету (нпр. *phishing*) нису посебно инкриминисана Кривичним закоником Републике Србије, већ се третирају као превара. У складу са развојем информационо-комуникационих технологија неопходно је осавременити Кривични законик у складу са појавом нових кривичних дела.

Усклађивање правних мера заштите мора пратити и измена у наставним плановима и програмима који ни на који начин не обрађују питања информационе приватности и генерално понашања корисника на интернету. Наравно, не треба чекати да се надлежне институције одазову и предузму одговарајуће мере. Постоје разни видови неформалног учења који у великој мери могу утицати на подизање свести корисника.

У контексту истраживања које је спроведено изузетно је било интересантно сагледати злоупотребу информационо-комуникационих технологија од стране жртава трговине људима и ирегуларним мигрантима, као и тражилаца азила.

На основу статистичких података из истраживања о жртвама трговине људима може се констатовати да су међу жртвама трговине људима знатно заступљенија лица женског него лица мушког пола, и то особе између 19 и 33 година. Велика већина испитаника је пореклом са ових простора, и то српске или ромске националности. Образовање испитаника који чине овај узорак је на прилично ниском нивоу, што се може посматрати као фактор виктимизације, јер отежава проналажење регуларног запослења, те је особа „принуђена“ да пронађе извор прихода и обезбеди себи егзистенцију на неки други начин. Ипак, треба имати у виду да је у питању мали узорак, ограничен на жртве испитане у одређеном временском периоду, што не допушта да се из њега изведе генерални закључак о томе да су жртве трговине људима у нашој земљи по правилу ниског степена образовања.

Међу жртвама су најзаступљенија незапослена лица. Такође, највећи број испитаника оценио је свој економски статус као лош или чак веома лош и то како садашњи тако и у тренутку врбовања, што јасно показује у коликој мери незапосленост, низак ниво образовања и негативан став о сопственој економској ситуацији доприносе виктимизацији. Однос броја испитаника који знају и који не знају да користе рачунар није статистички значајан, будући да је разлика само 10% у корист првих. Велика већина испитаника поседује мобилни телефон, док је број оних који поседују рачунар знатно мањи. Податак о односу броја жртава које користе и које не користе друштвене мреже нема статистичку значајност, јер је њихов однос скоро 50-50.

Највећи број жртава регрутован је 2012. године, а највише њих потражило је помоћ током 2013. године и то од полиције. У највећем броју случајева радило се о сексуалној експлоатацији.

Најзаступљенији начин успостављања првог контакта са жртвама из испитаног узорка био је личним, директним, непосредним путем и то без употребе било каквих информационо-комуникационих технологија. Наиме, иако укупно 23 испитаника има налог на *Facebook*-у, први контакт са трафикером је у највећем броју случајева остварен лично или преко познаника, што показује да, упркос поседовању налога на друштвеним мрежама трговац људима ипак није одабрао тај начин за ступање у први конатакт са њима.

Само један испитаник, са којим је трговац људима први контакт остварио путем интернета, користи друштвене мреже и има налог на *Facebook-у*, што указује на могућност да је *Facebook* том приликом злоупотребљен у сврху вербовања жртава трговине људима. То показује да на конкретном узорку приступ информационо-комуникационим технологимјама од стране жртве није имао знатнијег утицаја на њену виктимизацију. Будући да је први контакт у највећем броју случајева остварен лично или преко познаника, дакле без ослањања на информационо-комуникационе технологије. Лични контакт је и најзаступљенији начин на који је трговац одржавао контакт са жртвом, с тим што он понекад комбинован са употребом мобилног телефона, а само ретко и са интернетом.

То, међутим не може бити основ за извођење закључка да у Србији нема случајева вербовања жртава трговине људима путем злоупотребе информационо-комуникационих технологија. Наиме, наведени подаци представљају само пресек тренутне ситуације и слика су једног веома малог узорка који се не може третирати као репрезентативан. Због тога би требало размотрити спровођење оваквих истраживања и у будућности и то редовно и на различитим узорцима, јер би се тек онда, након дуготрајног праћења могла креирати реална слика о заступљености и доприносу информационо-комуникационих технологија у процесу трговине људима и њиховом доприносу виктимизацији. Посебно треба имати у виду и тамну бројку криминалитета у овој области, када је тумачење узорка и његових импликација на општу слику о жртвама трговине људима у питању.

Анализирани подаци о ирегуларним мигрантима и тражиоцима азила, добијени су на основу интервјуа спроведених од 24.4. до 20.6.2013. године, на узорцима које је чинило 53 тражиоца азила, 45 ирегуларних миграната, те 92 лица која имају оперативна сазнања у области везе између ВТК и ирегуларних миграција. Подаци су обрађени у програмима Microsoft Excel и SPSS. Резултати истраживања указују на постојање везе између ирегуларних миграција и употребе високих технологија. Популација тражилаца азила више користи високе технологије у процесу миграција у односу на ирегуларне мигранте. Оно што је заједничко за обе популације јесте чињеница да су рачунар/мобилни телефон у већој мери коришћени за комуникацију са другим мигрантима или кријумчарима него за самостално путовање. Такође, степен употребе високих технологија зависи од демографских и социоекономских карактеристика испитаника, те мушкарци, лица са вишим степеном образовања и они који говоре неки од страних језика више користе високе технологије у процесу ирегуларне миграције.

Приметна је веза између ирегуларних миграција и употребе високих технологија и од стране испитаника запослених у државним и невладиним организацијама, међу којима су и припадници полицијских установа широм Србије

и припадници граничне полиције, који о овоме говоре на основу стечених кооперативних искустава. Међутим, како би они могли да делују превентивно потребна је много боља техничка опремљеност њихових јединица. Транснационални карактер ирегуларних миграција, те висок удео секундарних кретања у структури токова тражилаца азила према територијалном пореклу, намећу потребу за даљом и бољом међународном сарадњом по питању ирегуларних миграција.

Веома значајни резултати добијени су и истраживањем употребе информационо-комуникационих технологија од стране кријумчара људи и трговаца људима. Иако је евидентно да полицијски службеници, у свом досадашњем раду, нису у довољној мери истраживали околности од значаја за утврђивање у којој се мери поједине савремене информационо-комуникационе технологије злоупотребљавају у процесу кријумчарења људи, оперативна сазнања која су предочили у упитницима основ су за констатацију да се савремене информационо-комуникационе технологије злоупотребљавају у процесу кријумчарења људи. Ово се нарочито односи на рачунаре, интернет, поједине друштвене мреже и мобилне телефоне. Притом, потврђено је да већина кријумчара који користе интернет користе и друштвене мреже у процесу кријумчарења миграната (нарочито *Facebook*, *Twitter*, *Google+* и *LinkedIn*).

Резултати истраживања показују значајну учесталост злоупотребе информационо-комуникационе технологије од стране трговаца људима у свим фазама извршења кривичног дела трговине људима (врбовање, транспортовање и експлотација). У значајној мери полицијски службеници су, током свог оперативног рада, пажњу посветили проналажењу, одузимању и експертизи средстава савремених комуникационих технологија коришћених од стране трговаца људима.

ПОЈМОВНИК

Адреса је низ знакова (слова, бројеви, цифре, сигнали и специјални знакови) који је намењен за одређивање одредишта везе[864].

Апликативни програмски интерфејс (АПИ) је софтверски интерфејс између апликација пружалаца медијских садржаја и уређаја за пријем тих садржаја[865].

Азил је право на боравак и заштиту које има странац у другој држави.

У Србији **азил** је право на боравак и заштиту које има странац коме је на основу одлуке надлежног органа, који је одлучивао о његовом захтеву за азил у Републици Србији, одобрено уточиште или други облик заштите; Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Азилант је странац коме је на основу одлуке надлежног органа који је одлучивао о његовом захтеву за азил у Републици Србији, одобрено уточиште или други облик заштите предвиђен законом.

Базе података су добро структуирана колекција података која постоји релативно дуго и коју користи и одржава више корисника, односно програма (апликација).[866]

Блокирање садржаја представља онемогућавање приступа интернет садржајима, неким рачунарима или мрежама[867].

Ботнет је мрежа заражених рачунара, која настаје тако што се, помоћу одређеног малициозног софтвера, остварује контрола над великим бројем рачунара.

Веб-сервер - на веб-серверима се налазе веб-објекти до којих се долази навођењем њихове URL адресе. Када корисник затражи неку веб-страницу веб-читач шаље серверу HTTP поруке са захтевом за објекте са одговарајуће странице. Сервер прима ове захтеве и одговара HTTP порукама у којима се налазе тражени објекти.[868]

Високотехнолошки криминал Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала[869] (ЗОНДОВТК), који је ступио на снагу 25.7.2005. године (и уз измене 2009. год. објављене у Службеном гласнику Републике Србије број 104-09), први пут је и у домаћем законодавству дефинисан појам високотехнолошког криминала и то као "вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или

---

864 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010) и допуњено од стране МД & РД, ПИТАЊЕ ШТА СУ ОДРЕДИШТА ВЕЗА?;

865 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

866 Бранислав Лазаревић, Зоран Марјановић, Ненад Аничић, Слађан Бабарогић (2012) „Базе података";

867 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

868 James F. Kurose, Keith W. Ross (2008) "Умрежавање Рачунара - Од врха ка дну", http://www.webopedia.com/TERM/W/Web_server.html, www.wikipedia.org

869 Службени гласник Републике Србије број 61/05" од 15.7.2005. године;

електронском облику. Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала успостављени су законски оквири за успостављање институција за борбу против високотехнолошког криминала и у њихову надлежност поверено је спречавање кривичних дела против безбедности рачунарских података, као и кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. Законом о изменама и допунама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[870], створени су и додатни услови за ефикаснију борбу против високотехнолошког криминала проширењем надлежности на друга кривична дела. У члану 2 овог закона о изменама и допунама наведено је да се члан 3 мења и наводи се да се закон примењује ради откривања, кривичног гоњења и суђења за: 1) кривична дела против безбедности рачунарских података одређена Кривичним закоником; 2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара; 3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2 став 1 овог закона." Изменом се ишло ка повећању броја примерака ауторских дела (новим изменама је број примерака ауторских дела прелази 2000, а према старом закону 500, измене су извршене и у материјалној штети која је, по новим изменама преко 1.000.000 динара, а била је 850.000 динара). Додат је и трећи став, чиме је надлежност проширена и на друга наведена кривична дела.

2013. године дошло је до изменама и допунама Кривичног законика, уведени су појмови „рачунарски системи" и „рачунари", па су ти појмови унети и у одредбе овог закона (члан 2 и 3).

Изменама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, прецизирана је и проширена примена закона и на кривична дела против привреде (члан 3 тачка 2 Закона), односно на друга кривична дела (код којих се због начина извршења или употребљених средстава могу сматрати кривичним делима), па су у том смислу проширене надлежности државних органа за борбу против овог криминала (додата тачка 3 члану 3 Закона).

Извршена су и усклађивања (углавном терминолошка – на пр. "окружно" у "више", "непосредно виши суд" у "Апелациони суд" ...) са новодонетим законима (Закон о јавном тужилаштву, Закона о уређењу судова и Закон о седиштима и подручјима судова и јавних тужилаштава).

870 Службени гласник Републике Србије број 104/09 од 11.12.2009. године;

Временски жиг је званично време придружено електронском документу или групи електронских докумената, којим се потврђује садржај електронског документа у то време, односно садржај сваког документа у групи[871].

Врбовање је појава чији су обим и садржај ужи од појма регрутовања и његова је поткатегорија. То је акт придобијања сагласности воље потенцијалне жртве са легендираном понудом регрутера и манифестује се као обмана жртве апсолутним неистинама или полуистинама. Гледано кроз кривично-правну призму, врбовање подразумева наговарање неког лица да предузме неке делатности, односно да се стави у одређени положај и овај облик радње се најчешће може односити на чињење криминалних активности, проституцију, просјачење и друго[872].

Дела компјутерског криминала, као типична дела извршена помоћу и против рачунара појављују се: 1) немарно коришћење информационих система и кршење безбедносне политике; 2)он-лајн преваре, крађа идентитета; 3) хакинг; 4) вируси; тројанци, црви или adware/spyware програми; 5) дигитална пиратерија музике, филма и/или софтвера, посебно преко P2P мрежа; 7) сајбер малтретирање; (8) трговина људима; 9) организовани криминал; 10)шпијунирање; 11) сајбер–тероризам[873].

Дете је било која особа млађа од осамнаест година[874].

Генетска приватност - развој биомедицине и биоинформатике омогућиће да се телесним прегледом поједине особе анализира њен генетски материјал, а на тај начин могуће је установити не само садашње или прошло стање, него и предиспозиције или евентуално будуће здравље особе. Потенцијални послодавци тако ће увидом у те податке моћи да виде колико је неко склон оболевању и тако одлучити кога ће запослити, што отвара потпуно нову грану генетске дискриминације. Осим тога, нека осигуравајућа друштва већ данас одбијају да осигурају особе које имају генетске предиспозиције за наследне или опасне болести.

Такве злоупотребе су заправо негативна последица развоја биоинформатике и проблем који треба што пре решити. Најбољи начин за то биће доношење посебног закона о генетској приватности, који ће строго ограничавати доступност и могућност манипулације генетским информацијама појединца, што ће спречити, али и врло строго санкционисати све злоупотребе.

Гранична полиција је организациона јединица МУП-а која непосредно обавља послове граничне контроле и друге послове заштите државне границе. Закон о странцима, Службени гласник Републике Србије, бр. 97/08.

---

871 преузето из Закона о електронском документу, члан 3 (Службени Гласник РС бр. 51/2009);

872 Лазаревић, Љ. *Коментар Кривичног законика Републике Србије*, Савремена администрација, Београд, 2011, стр. 1123;

873 http://www.scribd.com/doc/24908486/Encyclopedia-of-Cyber-Crime, датум последњег приступа 25.3.2014;

874 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала *усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/200;*

Дигитализација је преношење докумената из других облика у електронски облик[875].

Под појмом **друштвене мреже** сматра се специјалан веб-сајт који представља социјалну структуру коју чине актери (чланови који су регистровани на том сајту и имају своје налоге) и везе између тих актера. Садрже простор за остављање порука, текстове или било који други садржај, простор за приватно ћаскање и могућност дељења садржаја са другима[876].

ДОС напад - одбијање пружања услуга (енг. *Denial of service*)[877]. У случају када је у питању велики број захтева усмерених од стране више рачунара заражених малициозним програмима, реч је о дистрибуираном ДОС-у (енг. *Distributed denial of service*)[878]. Резултат DDoS напада је прекид услуга који, као резултат ,има нестабилност система или његово обарање. Управо ови DDOS напади[879] представљају најактуелнију претњу која долази кроз ботнетове (велики броја зомби-рачунара, такозваних зомби-мрежа). PDOS напади (енг. *Permanent denial of service*) могу да трајно оштете хардвер на серверима са даљинским приступом. Напад се заснива на искоришћавању „firmware apdejta“[880] који се серверима шаље преко мреже или интернета, а који је способан да превари хардвер и флешује (енг. *flash*) било који део система, што би могло довести до трајног и потпуног хардверског пада TDoS напади телекомуникациона одбијања пружања услуга у којима су извршиоци компромитовали рачуне корисника, након чега контактирају финансијске институције и мењају податке о датим корисницима, добијајући на тај начин прикривену анонимност – потпуно нови дигитални идентитет. Ови напади су коришћени да друге жртве приморају путем безбројних позива упућених према одређеним лицима (телефонским бројевима или контактима) на промену бројева.

Довођење у заблуду је стварање погрешне или непотпуне представе код другог лица. Та се радња може извршити на два начина: лажним приказивањем чињеница и прикривањем чињеница. Лажно приказивање је тврђење да постоји нека чињеница која у стварности не постоји и обрнуто. Прикривање чињеница је

875 преузето из Закона о електронском потпису, члан 3 (Службени гласник РС бр. 135/2004);

876 Boyd, Danah; Ellison, Nicole (2007) "Social Network Sites: Definition, History, and Scholarship", Journal of Computer-Mediated Communication 13;

877 Рачунару се шаље огроман број захтева којим се комуникациони канали загушују, па рачунар или систем није у могућности да оствари спољну комуникацију;

878 Основни критеријум за разликовање је постојање дистрибуираног – усмереног напада, у којем велика мрежа рачунара-зомбија – ботова (ботнет) напада комуникације једног (или више) рачунара;

879 У Великој Британији покушали су инкриминацију оваквих аката (Computer Misuse (Amendment) Bill 2002 HL: House of Lords Bills 2001-2002, p.79) кроз „одбијање пружања услуга чини оно лице које изазове или у намери изазивања директно или посредно, кроз деградацију, опструкцију или неки други облик нефункционисања рачунарског система или неког његовог дела. Лице ће се сматрати одговорним и у случају када није имало намеру изазивања оваквог случаја у границама свесног нехата;

880 Термин фирмвер (енг. firmware) означава скуп програма, фабрички уграђених у хардверске уређаје и компоненте. Временом произвођачи опреме проналазе боља софтверска решења за функционисање тих уређаја. Поступак замене постојећег фирмвера новим назива се флешовање;

прећуткивање чињеница од лица које је дужно да их саопшти или стварање неке ситуације да неко лице не може само да сазна за одређене чињенице[881].

Држава порекла је држава чије држављанство има странац или држава у којој је лице без држављанства имало стални боравак, а уколико странац има више од једног држављанства, држава порекла је свака држава чије држављанство има странац. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Електронска комуникациона мрежа представља системе преноса и, тамо где је то примењено, уређаје за комутацију и усмеравање и друге ресурсе, укључујући пасивне мрежне елементе, који омогућавају пренос сигнала помоћу жичних, радио, оптичких или других електромагнетских средстава, укључујући сателитске мреже, фиксне (са комутацијом кола и пакета, укључујући интернет) и мобилне мреже, енергетске кабловске системе, у делу који се користи за пренос сигнала, мреже које се користе за дистрибуцију и емитовање медијских садржаја, без обзира на врсту података и информација који се преносе[882].

Електронска комуникациона мрежа за посебне намене је електронска комуникациона мрежа органа одбране, унутрашњих послова и Безбедносно-информативне агенције (у даљем тексту: органи одбране и безбедности), органа државне управе надлежних за заштиту и спасавање, као и служби за хитне интервенције (у даљем тексту: службе за хитне интервенције), која се користи за намене за које су наведени органи основани, не користи се у комерцијалне сврхе и не даје се на коришћење трећим лицима[883].

Електронска комуникациона опрема је опрема која се употребљава за обављање делатности електронских комуникација[884].

Електронска комуникациона услуга је услуга која се по правилу пружа уз накнаду, а састоји се у целини или претежно од преноса сигнала у електронским комуникационим мрежама, укључујући телекомуникационе услуге и услуге дистрибуције и емитовања медијских садржаја, али не обухвата услуге пружања медијских садржаја или обављања уредничке контроле над медијским садржајима који се преносе путем електронских комуникационих мрежа и услуга, нити обухвата услуге информационог друштва које се у целини или претежно не састоје од преноса сигнала електронским комуникационим мрежама[885].

Електронска порука је сваки текстуални, гласовни, звучни или сликовни запис, послат преко јавне комуникационе мреже, који се може похранити у мрежи или у терминалној опреми примаоца све док је прималац не преузме или јој приступи[886].

Електронски документ јесте скуп података састављен од слова, бројева, симбола, графичких, звучних и видео-записа садржаних у поднеску, писмену, решењу,

881 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 502;

882 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

883 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

884 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010):

885 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010):

886 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

исправи или било ком другом акту који сачине правна и физичка лица или органи власти, ради коришћења у правном промету или у управном, судском или другом поступку пред органима власти, ако је електронски израђен, дигитализован, послат, примљен, сачуван или архивиран на електронском, магнетном, оптичком или другом медију[887].

Експлоатација обухвата, као минимум, експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа[888].

Жртва је лице које је појединачно или колективно претрпело штету, укључујући физичко или ментално повређивање, емотивну патњу, материјални губитак или груб напад на своја основна права, услед чињења или нечињења која представљају кршење кривичних закона држава, што се односи и на законе који забрањују злоупотребу власти. Жртвом се може сматрати свако ко испуњава наведене услове, без обзира на то да ли је учинилац дела идентификован или није, да ли је ухапшен, да ли се против њега води судски поступак, да ли је проглашен кривим и без обзира на степен његовог сродства са жртвом. Термин „жртва“ обухвата по потреби и блиску породицу и лица која жртва директно издржава, као и лица која су претрпела штету помажући жртвама које су се нашле у невољи[889].

Жртва трговине људима је свако физичко лице подвргнуто трговини људима. Центар за заштиту жртава трговине људима утврђује статус жртве трговине људима[890].

Збирка података је скуп података који се аутоматизовано или неаутоматизовано воде и доступни су по личном, предметном или другом основу, независно од начина на који су похрањени и места где се чувају[891].

Информациона приватност је право појединца да контролише који, за кога и како подаци о њему могу постати доступни другима[892].

Издавалац временског жига је правно лице пружалац услуга од поверења које поседује систем за формирање временског жига и које издаје временски жиг. Издавалац временског жига обезбеђује услове за поуздано пружање услуга, а нарочито: 1) доступност својих услуга свим корисницима чије су активности у складу са објављеном Политиком издавања временског жига; 2) заштиту података о личности корисника; 3) ресурсе потребне за издавање временског жига у складу с Политиком издавања временског жига; 4) ефикасно поступање у решавању

887 Појам електронског документа у Закону о електронском документу (Службени гласник Републике Србије бр.) – члан 2.

888 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала *усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001;*

889 Декларација о основним принципима правде за жртве злочина и злоупотребе власти, усвојена Резолуцијом Генералне скупштине Уједињених нација број 40/34 од 29. новембра 1985. године;

890 Стратегија борбе против трговине људима у Републици Србији, Службени гласник РС, бр. 111/2006;

891 преузето из Закона о заштити података о личности, члан 3 (Службени гласник РС бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012;

892 Мирјана Дракулић,1996, „Основи комјутерског права“;

рекламација и спорова са корисницима или другим заинтересованим странама у вези издавања временског жига [893].

Интелектуална својина обухвата ауторско и сродна права, жиг, географску ознаку порекла, дизајн, патент, мали патент и топографију интегрисаних кола.[894]

Интероперабилност је својство два или више система или њихових компоненти да размењују податке и користе податке који су размењени[895].

Интерфејс је физичка или логичка веза између два или више уређаја, два или више делова истог уређаја или медијума преноса, дефинисана функционалним карактеристикама, карактеристикама сигнала или другим одговарајућим карактеристикама[896].

Информациони посредник је правно или физичко лице које у име пошиљаоца или примаоца врши пријем, пренос, достављање и чување електронских докумената[897].

Информациони систем је интегрисани скуп компоненети за сакупљање, снимање, чување, обраду и преношење **информација**. Омогућава брз приступ великом броју информација и брзо и ефикасно тумачење великог броја података[898].

Избеглица је лице које се, због оправданог страха од прогона због своје расе, пола, језика, вероисповести, националне припадности или припадности некој групи или због својих политичких уверења, не налази у држави свог порекла и није у могућности или због тог страха не жели да се стави под заштиту те државе, као и лице без држављанства које се налази изван државе свог претходног сталног боравка и које не може или због тог страха не жели да се врати у ту државу. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Иррегуларни мигрант је лице које је прекршило закон о уласку страних држављана у земљу или које нема законски статус у земљи боравка.

Јавна комуникациона мрежа јесте електронска комуникациона мрежа која се, у целини или претежно, користи за пружање јавно доступних електронских комуникационих услуга и омогућава пренос података између терминалних тачака мреже[899].

Компјутерски криминал је вршење кривичних дела код којих се рачунар и рачунарска технологија појављују као оруђе за чињење кривичног дела или као објект заштите. Овај криминал је специфично понашање кога карактерише[900]:

---

893 преузето из Закона о електронском документу, члан 3 (Службени гласник РС бр. 51/2009), Правилник о издавању временског жига, члан 6 (Службени гласник РС бр. 112/2009);

894 Преузето из Закона о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, члан 3 (Службени гласник РС бр. 46/2006 и 104/2009);

895 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

896 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

897 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

898 Rainer, Turban (2009), "Introduction to information systems";

899 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

900 Дракулић М, Основи компјутерског права, Београд, ДОПИС, стр.400 – 487;

1) понашање које је противправно, неетичко и неауторизовано, а усмерено је на аутоматску обраду података и/или њихов пренос, што значи да је у питању дело човека, да је предвиђено и описано у својим битним обележјима у закону као кривично дело и да је друштвено опасно;

2) за постојање овог криминала неопходно је постојање рачунара, односно знања вазених за компјутерске технологије. Рачунари се појављују у у четворострукој улози: објекта, „субјекта“, инструмента/оружја и симбола;

3) код ових кривичних дела изузетно је велики проблем откривање и спровођење кривичних поступака пошто су то дела за чије је откривање и процесуирање неопходно специфично знање, што постоји масовност оружја и што је отежано откривање и праћење последица одређених околности: велике способности прерушавања, скривености трагова, невидљивости доказа и тешкоћа у њиховом дешифровању и приказивању, њихово лако брисање, неискуство истражитеља и тужиоца и правна несигурност и празнине;

4) овај криминал не зна за границе, лагано прелази из једне државе у другу и са једног континента на други.

Комуникација означава размену или преношење информација између одређеног броја особа путем јавно доступних електронских комуникационих услуга, изузев информација које се преносе у склопу услуга јавног емитовања програма преко електронских комуникационих мрежа и које се не могу повезати са одређеним претплатником или корисником, односно примаоцем[901].

Корисник је физичко или правно лице које користи или захтева јавно доступну електронску комуникациону услугу[902].

Корисник података је физичко или правно лице, односно орган власти, који је законом или по пристанку лица овлашћен да користи податке (у даљем тексту корисник) [903].

Крађа идентитета обухвата лажно представљање особе при чему се преузима идентитет неке друге особе, ради неовлашћеног приступа рачунима, локацијама и власништву особе чији је идентитет украден[904].

Кривично дело трговине људима је дефинисано на начин на који је то учињено у члану **388** Кривичног законика Републике Србије[905], као и у Стратегији борбе против трговине људима у Републици Србији[906]. Ово дело чини лице које силом или претњом, довођењем у заблуду или одржавањем у заблуди, злоупотребом

901 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

902 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

903 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр.44/2010);

904 http://www.consumer.ftc.gov/features/feature-0014-identity-theft, датум последњег приступа 4.12.2013;

905 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005,72/2009, 111/2009 и 121/2012;

906 Стратегија борбе против трговине људима у Републици Србији, Службени гласник РС, бр. 111/2006;

овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи, врбује, превози, пребацује, предаје, продаје, купује, посредује у продаји, сакрива или држи друго лице, а у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима, казниће се затвором од три до дванаест година (члан 388 став 1). За дело из става 1 овог члана, учињено према малолетном лицу учинилац ће се казнити казном прописаном за то дело и кад није употребио силу, претњу или неки други од наведених начина извршења (члан 388 став 2). Ако је дело из става 1 овог члана учињено према малолетном лицу, учинилац ће се казнити затвором најмање пет година (члан 388 став 3). Ако је услед дела из ст. 1 и 2 овог члана наступила тешка телесна повреда неког лица, учинилац ће се казнити затвором од пет до петнаест година, а ако је наступила тешка телесна повреда малолетног лица услед дела из става 3 овог члана, учинилац ће се казнити затвором најмање пет година (члан 388 став 4). Ако је услед дела из ст. 1 и 3 овог члана наступила смрт једног или више лица, учинилац ће се казнити затвором најмање десет година (члан 388 став 5). Ко се бави вршењем кривичног дела из ст. 1 до 3 овог члана или је дело извршено од стране групе, казниће се затвором најмање пет година (члан 388. став 6.). Ако је дело из ст. 1 до 3 овог члана извршено од стране организоване криминалне групе, учинилац ће се казнити затвором најмање десет година (члан 388 став 7). Ко зна или је могао знати да је лице жртва трговине људима, па искористи њен положај или другоме омогући искоришћавање њеног положаја ради експлоатације предвиђене ставом 1 овог члана, казниће се затвором од шест месеци до пет година (члан 388 став 8). Ако је дело из става 8 овог члана учињено према лицу за које је учинилац знао или је могао знати да је малолетно, учинилац ће се казнити казном затвора од једне до осам година (члан 388 став 9). Пристанак лица на експлоатацију или на успостављање ропског или њему сличног односа из става 1овог члана не утиче на постојање кривичног дела из ст. 1, 2 и 6 овог члана (члан 388 став 10)[907].

Кривично дело трговина малолетним лицима ради усвојења из члана 389 став 1 чини лице које одузме лице које није навршило шеснаест година ради његовог усвојења противно важећим прописима или ко усвоји такво лице или посредује у таквом усвојењу или ко у том циљу купи, прода или преда друго лице које није навршило шеснаест година или га превози, обезбеђује му смештај или га прикрива. За овај основни облик тог кривичног дела прописана је казна затвора у трајању од 1 до 5 година.

Ако се неко лице бави вршењем делатности које чине основни облик кривичног дела трговине малолетним лицима ради усвојења или уколико је то дело извршено од стране групе, учинилац се може казнити затвором у трајању од најмање 3 године (члан 389 став 2). Ако је основни облик овог кривичног дела извршен од стране

907 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005,72/2009, 111/2009 и 121/2012, члан 388;

организоване криминалне групе, учинилац ће се казнити затвором у трајању од најмање 5 година[908].

Кривично дело заснивање ропског односа и превоз лица у ропском односу, прописано чланом 390 Кривичног законика Републике Србије чини лице које кршећи правила међународног права, стави другог у ропски или њему сличан однос или га држи у таквом односу, купи, прода, преда другом лицу или посредује у куповини, продаји или предаји оваквог лица или подстиче другог да прода своју слободу или слободу лица које издржава или о којем се стара. За ово кривично дело прописана је казна затвора од 1 до 10 година. Лице које превози лица која се налазе у ропском или њему сличном односу из једне земље у другу, казниће се затвором од 6 месеци до 5 година (члан 390 став 2). Уколико је кривично дело заснивања ропског односа и превоза лица у ропском односу учињено према малолетном лицу, учинилаца ће се казнити затвором у трајању од 5 до 15 година (члан 390 став 3)[909].

Комерцијална је сексуална експлоатација жртава трговине људима ради задовољења сексуалних прохтева, нагонских и патолошких потреба неодређеног броја „власнику" познатих и непознатих лица, при чему се остварује извесна противправна корист[910].

Кријумчари људи су особе које свесно (из користољубља) другом лицу омогуће неовлашћени прелазак државне границе, као и оне које странцу омогуће неовлашћени транзит или боравак.

Лице које тражи азил је странац који поднесе захтев за азил на територији Републике Србије о чијем захтеву није донета коначна одлука. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Малвер (енг. *Malware*) представља различите облике штетног софтвера који је програмиран од стране нападача са циљем да угрози рад система, прикупи поверљиве информације или придобије неовлашћен приступ рачунарским системима[911].

Медицинска приватност је право пацијента да контролише који, коме и како медицински подаци о њему могу постати доступни другима. Оно је релативног карактера, што значи да постоје, само у строго законски предвиђеним условима, ситуације када се други интереси стављају испред интереса појединца, пацијента. Подаци који су обухваћени медицинском приватношћу су медицински подаци под којима се подразумева посебна категорија података о личности везаних за здравље појединца[912].

---

908 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009. и 121/2012, члан 389;

909 Кривични законик Републике Србије, Службени гласник РС, бр. 85/2005, 88/2005,107/2005, 72/2009, 111/2009. и 121/2012, члан 390;

910 Мијалковић, С. Жарковић, М. 2012, Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 158-159;

911 http://technet.microsoft.com/en-us/library/dd632948.aspx, датум последњег приступа 3.12.2013;

912 Дракулић М. 2006, "Правни и етички аспекти модерне медицине - права пацијената";

Медијски садржаји обухватају радијске и телевизијске програме, односно аудиовизуелне садржаје, као и са њима повезане интерактивне услуге, који се дистрибуирају и емитују, односно пружају корисницима путем електронских комуникационих мрежа, на основу програмске шеме или на захтев корисника[913].

Миграција је облик просторне покретљивости становништва, унутар граница државе или између две државе, који укључује промену места пребивилашта.

Малолетник без пратње је странац који није навршио осамнаест година живота и који приликом уласка у Републику Србију нема или је након уласка у њу, остао без пратње родитеља или старатеља. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Недопуштени податак је информација, порука и документ који је у супротности са прописима и моралом или који је законом одређен као поверљив[914].

Некомерцијална је сексуална експлоатација жртава трговине људима од стране лица које их је „купило“ ради задовољења личних или/и сексуалних прохтева њему блиских лица, без намере да њиховом експлоатацијом остварује противправни приход[915].

Обрада података је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин (у даљем тексту: обрада). Пуноважан пристанак за обраду може дати лице, након што га руковалац претходно обавести. Пуноважан пристанак лице може дати писмено или усмено на записник. У случају опозива, лице које је дало пристанак дужно је да руковаоцу надокнади оправдане трошкове и штету, у складу са прописима који уређују одговорност за штету. Могућа је и обрада без пристанка[916].

Обрађивач података је физичко или правно лице, односно орган власти, коме руковалац на основу закона или уговора поверава одређене послове у вези са обрадом (у даљем тексту: обрађивач) [917].

Оператер је лице које обавља или је овлашћено да обавља делатност електронских комуникација[918].

---

913 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

914 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

915 Мијалковић, С. Жарковић, М. 2012, Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 158;

916 Преузето из Закона о заштити података о личности, члан 10 и 11, (Службени гласник РС бр. 97/2008);

917 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

918 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

Одржавање у заблуди је активна радња, активно подржавање погрешне или непотпуне представе код другог лица која код њега већ постоји[919].

Подаци су елементарни описи ствари, догађаја, активности и трансакција који су забележени, класификовани и сачувани, али нису организовани и не носе никакво конкретно значење[920].

Податак о личности је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и слично), по чијем налогу је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и слично, односно посредно, путем увида у документ у којем је информација садржана и слично) или без обзира на друго својство информације (у даљем тексту: податак)[921].

Податак о личности директива

Подаци о саобраћају се односе на податке који се обрађују приликом преноса и тарифирања комуникације унутар електронске комуникационе мреже[922].

Подаци о локацији су подаци који означавају тренутни или стални географски положај терминалне опреме корисника унутар електронске комуникационе мреже[923].

Потрошач је физичко лице које на тржишту прибавља робу или услуге у сврхе које нису намењене његовој пословној или другој комерцијалној делатности[924].

Пошиљалац је правно или физичко лице, односно орган власти који је послао или у чије име се примаоцу шаље електронски документ; **прималац** је правно или физичко лице, односно орган власти коме је намењен и упућен електронски документ и који је тај документ примио[925].

Пресретање електронске комуникације[926] је једна од четири категорија напада на рачунарске системе. Пресретање или прислушкивање је пасиван напад и у овом случају пошиљалац шаље поруку која стиже до одредишта. Најчешће прималац не може детектовати овакву врсту напада[927].

---

919 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 502;

920 Rainer, Turban (2009), "Introduction to information systems";

921 преузето из Закона о заштити података о личности, члан 3 (Службени ласник РС бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012);

922 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

923 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

924 преузето из Закона о заштити потрошача, члан 5 (Службени гласник РС бр.73/2010);

925 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

926 Овај облик дела у нашем законодавству је веома палијативно регулисан чл. 143, гони се по приватној тужби (осим у ст. 3 када то чини службено или војно лице), чл. 301 КЗ, чл. 302 (уз постојање неког облика заштите), чл. 304 (без заштите), посредно и 304а евентуално чл. 315 тек се неким подзаконским актима и предлозима закона покушава подробније и конкретније регулисати ова материја о чему ће бити речи касније;

927 Дејан Симић, (2011), "Основе информационо комуникационих технологија";

Претплатник је физичко или правно лице које је закључило уговор са оператором јавно доступних електронских комуникационих услуга о пружању тих услуга[928].

Претраживач је рачунарски програм који тражи специфичну информацију помоћу кључне речи и обавештава корисника о резултатима претраге. Претраживач садржи индекс са потписом више милијарди веб-страница и користи тај индекс да би пронашао странице које садрже скуп кључних речи помоћу којих корисник претражује интернет[929].

Приватност се појављује као вишезначна категорија: као право појединца који се појављује као субјект података и као приватност корисника. Приватност корисника обухвата: 1) приватност тзв. "информација за укључивање одређеног терминала у систем" (нпр. позивни број, тип захтеване услуге и слично); 2) приватност говора (онемогућавање пресретања усмених комуникација); 3) приватност података (онемогућавање пресретања података у било ком облику они били); 4) приватност корисникове локације; 5) приватност корисникове идентификације; 6) приватност посебних начина укључивања и 7) приватност његових финансијских трансакција (нарочито трансмисије података о кредитним картицама). Право на приватност је једно од основних, неотуђивих и апсолутних људских права сваког појединца којим се обезбеђује интегритет и дигнитет људске личности, а ради очувања тајности и слободе његовог приватног живота[930].

Приступ подразумева давање на коришћење средстава или услуга другим операторима, под одређеним условима, било на ексклузивној или неексклузивној основи, ради пружања електронских комуникационих услуга, укључујући услуге путем којих се пружају услуге информационог друштва или медијски садржаји, што, између осталог, обухвата: приступ елементима мреже и припадајућим средствима, што може обухватати прикључење опреме путем фиксних или бежичних веза (нарочито приступ локалној петљи, те средствима и услугама неопходним за пружање услуга преко локалне петље), приступ физичкој инфраструктури (укључујући зграде, кабловску канализацију и антенске стубове), приступ одговарајућим софтверским системима (укључујући системиме за оперативну подршку), приступ информационим системима и базама података за наручивање, пружање, одржавање, обрачун и наплату услуга, приступ системима за превођење бројева или системима са истоветном функционалношћу, приступ фиксним и мобилним мрежама (посебно за потребе роминга), приступ системима условног приступа, као и приступ виртуелним мрежним услугама[931].

Пружалац услуга информационог друштва је правно лице или предузетник који пружа услуге информационог друштва (у даљем тексту: пружалац услуга)[932].

Пристанак жртве трговине људским бићима на намеравану експлоатацију је без значаја у случајевима у којима је коришћена било која од наведених мера. Врбовање, превожење, пребацивање, скривање или примање детета за сврхе

928 преузето из Закона о електронским комуникацијама, члан 4 (Службени ласник РС бр. 44/2010);

929 Rainer, Turban (2009), "Introduction to information systems";

930 Дракулић М. (1996), "Основи компјутерског права";

931 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

932 преузето из Закона о електронским комуникацијама, члан 4 (Службени гласник РС бр. 44/2010);

експлоатације сматра се "трговином људским бићима" чак и ако не обухвата било које од набројаних средстава[933].

Продаја жртава другоме, односно **„препродаја људи“** је доминантни вид експлоатације жртава. Наиме, жртву може да експлоатише појединац или криминална група која је регрутовала, али она може да буде продата другом лицу или групи који ће је даље експлоатисати. У другом случају, даља продаја жртве представља облик њене експлоатације, односно зараду трговаца људима на разлици прихода од продаје жртве и трошкова њеног регрутовања, транспортовања и издржавања[934]. Осим тога, жртва може да буде продата и пошто је неко време била експлоатисана. Због тога се овај вид експлоатације назива трговина људима у ужем смислу, јер представља „трговину ради даље трговине“[935].

Принудна проституција је један од најзаступљенијих појавних облика експлоатације жртава трговине људима[936]. Под **проституцијом** се подразумева сексуални однос који карактеришу плаћање (најчешће у новцу), екстреман промискуитет и емоционална равнодушност према партнеру и самом сексуалном чину. Битне одлике проституције су: повезивање сваког сексуалног односа са новцем или каквом другом користи; екстреман сексуални промискуитет, односно везаност за велики број различитих, али и непознатих партнера и емотивна равнодушност не само према сексуалном задовољству већ и према партнеру[937].

Пороногрaфија се одређује као приказ еротског понашања (у виду визуелних садржаја или у писаној форми) који има за циљ изазивање сексуалног узбуђења. При овом виду експлоатације принудне сексуалне активности у којима жртва учествује бележе се у аудио-визуелном облику (фотографија или тонфилмско снимање), а потом репродукују или дистрибуирају. Други облик подразумева принуду жртве на извођење представа са порнографским садржајем.

Принудно вршење криминалних радњи. Према степену друштвене опасности ових незаконитих радњи, може се разликовати принудно вршење прекршаја и принудно вршење кривичних дела[938].

Принуда на вршење кривичних дела је тип експлоатације при коме се жртве приморавају на вршење одређених противправних радњи, а са циљем прибављања противправне имовинске користи за лице које примењује принуду.

---

933 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала *усвојен у Палерму, децембра 2000. године,* Службени гласник РС – Међународни уговори*, бр. 6/2001;*

934 Голубовић, С. Голубовић, Н. Примена теорије рационалног избора у анализи трговине људима, *Наука, безбедност, полиција,* вол. 16, бр. 2, Београд, 2011, стр. 87–100;

935 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 97;

936 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, (2012), стр. 159;

937 Јефтовић, М, Милашиновић, С. (2002), *Самоугрожавање друштва – социјално-патолошке девијације*, Синекс, Београд, 2002, стр. 143;

938 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 172;

Принуда на просјачење - Просјачење је дефинисано 2004. године, када је Међународна организација рада усвојила дефиницију просјачења које се утврђује као „низ активности којима појединац тражи новац од непознате особе, а на основу свог сиромаштва или у потрази за добротворним донацијама, позивајући се на здравствене или верске разлоге. Просјаци исто тако могу продавати мање предмете, као што су крпе за чишћење или цвеће, заузврат тражећи новац чији износ није утемељен вредношћу предмета који се продаје.“[939] Принуда на просјачење представља облик принуде на вршење прекршаја. Просјачење може бити индивдуално или у оквиру организоване мреже за просјачење, на локацијама са великом фреквенцијом људи[940].

Принудно учешће у оружаним сукобима подразумева да се жртве приморавају да непосредно или посредно учествују у ратним, терористичким, диверзантским, герилским и сличним акцијама[941].

Принуда подразумева навођење неког лица силом или претњом да нешто учини, не учини или трпи. Сила подразумева употребу физичке, механичке или друге снаге са циљем сламања отпора неког лица, као и примену хипнозе или омамљујућих средстава како би се оно довело у несвесно стање и принудило на одређено понашање. Сила може бити примењена као апсолутна или компулзивна, посредно или непосредно, али у интензитету који је подобан да утиче на вољу пасивног субјекта. Претња је зло које се ставља у изглед пасивном субјекту или њему блиском лицу ако не поступе по захтеву лица које врши принуду[942].

Принуда на закључење брака је тип експлоатације при коме се жртва експлоатише улогом брачног партнера у браку који је склопљен принудно. У оваквим ситуацијама жртва се експлоатише кроз наметнуту улогу брачног друга – супружника, јер брак није закључен сагласном изјавом воља обе, већ само једне особе. Може имати следеће облике: с обзиром на пол брачних партнера - принудни хетеросексуални брак и принудни хомосексуални брак; с обзиром на пол и узраст жртве - принудни брак са женом, принудни брак са дететом, принуђени дечји брак, принудни брак са мушкарцем; с обзиром на број жртава које су експлоатисане - принудни моногамни брак, принудни полигамни брак, принудни моноандни или полиандни брак[943].

Заблуда је непостојање представе о некој околности или постојање погрешне или непотпуне представе о некој околности[944].

---

939 Save the Children (2011), Регионални извјештај о просјачењу дјеце, распрострањеност, превенција и сузбијање дјечјег просјачења, Save the Children, Сарајево, стр. 12;

940 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, (2012), стр. 172;

941 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 173;

942 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 518;

943 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 167;

944 Јовашевић, Д. (2006), Лексикон кривичног права, Јавно предузеће Службени гласник, Београд, стр. 733;

Повратник по основу Споразума о реадмисији је држављанин Републике Србије за чији повратак је надлежни орган дао сагласност по основу Споразума о реадмисији које је закључила Република Србија. Закон о управљању миграцијама, Службени гласник Републике Србије, бр. 107/ 2012.

Поступак азила је поступак за стицање и престанак права на азил и других права лица која траже азил. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Превозник је физичко или правно лице регистровано за јавни превоз путника у ваздушном, друмском, водном или железничком саобраћају. Закон о странцима, Службени гласник Републике Србије, бр. 97/08

Прихватилиште за странце је објекат за смештај странаца којима није дозвољен улазак у земљу или којима је изречено протеривање или удаљење из земље, али их није могуће тако удаљити и којима је, у складу са законом, одређен боравак под појачаним полицијским надзором. Закон о странцима, Службени гласник Републике Србије, бр. 97/08;

Рачунар је сваки електронски уређај који на основу рачунарских програма аутоматски обрађује и размењује податке[945].

Рачунарски вирус је рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података[946].

Рачунарски податак је свако представљање чињеница, информација или концепт у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију[947].

Рачунарским програмом сматра се уређени скуп наредби које служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара[948].

Рачунарски систем је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података[949].

Рачунарском мрежом сматра се скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке[950].

---

945 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012 и 104/2013)

946 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013);

947 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013);

948 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013)

949 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013)

Регрутовање жртава трговине људима обухвата скуп метода, поступака и средстава чијом се појединачном или комбинованом применом неко лице „увлачи“ у мрежу кријумчарења или трговине људима[951].

Радна експлоатација је тип експлоатације који подразумева принудни рад жртве. Принудни рад је дефинисан Конвенцијом број 29 о присилном раду Међународне организације рада из 1930. године[952] и Конвенцијом број 105 о укидању принудног рада из 1957. године. Принудни рад се односи на било који рад или службу који су изнуђени од стране неког лица под претњом било какве казне и за које се то лице није добровољно пријавило. Услови принудног рада укључују употребу физичког или сексуалног насиља, претњу насиљем, дужничко ропство, обустављање исплате примања или неплаћање, ограничење слободе кретања, задржавање пасоша и личних исправа и претњу пријавом властима. Радна експлоатација може укључивати: експлоатацију у пољопривредном сектору и шумарству, експлоатацију у индустријском сектору, експлоатацију у услужном сектору, експлоатацију у домаћинству (тзв. кућно ропство) и комбиновану експлоатацију[953].

Сигурна држава порекла је држава са листе коју утврђује Влада, чији је држављанин лице које тражи азил, а ако се ради о лицу без држављанства, држава у којој је то лице имало претходно стално боравиште, која је ратификовала и примењује међународне споразуме о људским правима и основним слободама, у којој не постоји опасност од прогањања из било ког разлога који представља основ за признавање права на уточиште или доделу субсидијарне заштите, чији држављани не напуштају своју државу из тих разлога и која дозвољава међународним телима увид у поштовање људских права. Закон о азилу, Службени гласник Републике Србије, бр.109/07.

Сигурна трећа држава је држава са листе коју утврђује Влада, која се придржава међународних начела о заштити избеглица садржаних у Конвенцији о статусу избеглица из 1951. године и Протоколу о статусу избеглица из 1967. године (у даљем тексту: Женевска конвенција и Протокол), у којој је тражилац азила боравио или кроз коју је пролазио, непосредно пре доласка на територију Републике Србије и у којој је имао могућност подношења захтева за азил, у којој не би био изложен прогону, мучењу, нељудском или понижавајућем поступку или враћању у државу у којој би његов живот, безбедност или слобода били угрожени. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Субсидијарна заштита је облик заштите који Република Србија одобрава странцу, који би у случају повратка у државу порекла био изложен мучењу, нечовечном или понижавајућем поступању или би његов живот, безбедност или слобода били

---

950 преузето из Кривичног законика Републике Србије, члан 112 (Службени гласник РС бр. 85/2005, 88/2005 - испр. 107/2005 - испр. 72/2009, 111/2009, 121/2012 и 104/2013)

951 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 86;

952 Convention (No. 29) concerning Forced Labor, Adopted on 28 June 1930 by the General Conference of the International Labor Organization at its 14th session, at: Human Rights - A Compilation of International Instruments Volume I, Universal Instruments, United Nations, New York and Geneva, 1994;

953 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 156-157;

угрожени насиљем општих размера које је изазвано спољном агресијом или унутрашњим оружаним сукобима или масовним кршењем људских права. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Странац је свако лице које није држављанин Републике Србије, било да је страни држављанин или лице без држављанства. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Споразум о реадмисији је међународни споразум који регулише поступак враћања и прихватања лица која не испуњавају или више не испуњавају услове за улазак или боравак на територији друге државе. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Сајбер криминал је такав облик криминалног понашања код кога је сајбер простор – окружење у коме се рачунарске мреже појављују као средство, циљ, доказ и/или симбол или окружење извршења кривичног дела. При томе се под сајбер простором подразумева или врста "заједнице" сачињене од мреже рачунара у којој се елементи традиционалног друштва налазе у облику бајтова и битова или "простор који креирају рачунарске мреже"[954].

Систем за формирање временског жига је софтверско-хардверски систем за формирање временског жига који има приступ тачном времену у складу са законом[955].

Софтвер представља компјутерске програме, датотеке и пратећу (њему припадајућу) документацију (као што су менјуели и приручници) који служе корисницима. У Моделу закона за заштиту компјутерског софтвера Светске организације за заштиту интелектуалне својине (WIPO – World Intellectual Property Organization) софтвер је дефинисан као целина која обухвата компјутерски програм и то онај који је материјално фиксиран на тракама, дисковима и сличним медијумима; пратеће материјале, као што су приручници за коришћење програма или за њихово опслуживање и опис програма садржаног у менјуелима програмске логике. Дакле, софтвер је комплексан појам под којим се подразумева целина састављена од два дела: 1. компјутерских програма (и подпрограма) и 2. пратеће (софтверу припадајуће) документације (приручници и упутства) за коришћење програма, њихово опслуживање и/или разумевање. У одређеним случајевима под пратећом документацијом се подразумевају и описи програма, као потпуни процедурални прикази података у вербалној, шематској или некој другој форми, који су довољни да се на основу њих изради низ инструкција, које представљају одговарајући рачунарски програм (један или више, са и без подпрограма) са пратећом документацијом, што чини софтверски пакет, а готово никада или изузетно ретко, и опис програма[956].

Сексуална експлоатација (*sex trafficking*) је најзаступљенији облик експлоатације жртава трговине људима. То је експлоатација њиховог тела, полног и сексуалног идентитета и интегритета. Реч је о виду експлоатације жртава оба пола, различитог

954 Дракулић, М. Дракулић, Р. "Cyber kриминал", доступан на Интернету на адреси: http://www.bos.rs/cepit/idrustvo/sk/c yberkriminal.pdf последњи пут приступљено 20.7.2010. год;

955 преузето из Закона о електронском документу, члан 3 (Службени гласник РС бр. 51/2009);

956 Дракулић М.(1996), "Основи компјутерског права";

узрасног доба, који се манифестује као некомрецијална и комерцијална сексуална експлоатација[957].

Транзит је прелазак преко територије Републике Србије. Закон о странцима, Службени гласник Републике Србије, бр. 97/08.

Трговина људима дефинисана је на начин на који је то учињено у члану 4 Конвенције Савета Европе о борби против трговине људима[958], односно у члану 3 Протокола за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године[959].

Трговина људима значи вербовање, превоз, премештање, скривање или прихват лица, уз примену претње или силе или других облика принуде, отмице, преваре, обмане, злоупотребе овлашћења или стања угрожености или давање или примање новчаних средстава или друге користи ради добијања пристанка лица које има контролу над другим лицем у циљу експлоатације[960].

Трговина децом ради усвојења је вид експлоатације који се успоставља над дететом и може се манифестовати као „неправо" и право. Неправо експлоатисање илегалним усвојењем детета постоји у случајевима када је усвојење извршено на незаконит начин, након тога дете живи са новим родитељима без икаквих додатних облика експлоатације. Сам положај жртве, због начина на који је у њега доведена, сматра се експлоатацијом. „Право" експлоатисање илегално усвојеног детета постоји у случајевима када је, поред тога што је „неправо", дете и додатно експлоатисано другим видовима и облицима: сексуално, радно, приморавањем на вршење одређених криминалних радњи или трговином људима у ужем смислу.

Трговина органима или *одузимање људских органа и делова тела* је вид експлоатације где су жртве експлоатисане на тај начин што им је узет орган из организма, или део тела. У овом случају може постојати неколико облика експлоатације. С обзиром на врсту људског ткива које се узима: узимање људских органа и узимање делова људских тела; у односу на то да ли постоји сагласност даваоца органа, односно дела тела: добровољно давање људских органа или делова тела и насилно узимање људских органа или делова тела; с обзиром на то да ли је лице од кога се орган узима живо или не: узимање органа или делова тела од живог лица, узимање органа или делова тела од „свеже умрлог" лица и узимање органа

957 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 158;

958 Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009;

959 Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори бр. 6/2001;

960 Закон о потврђивању Конвенције Савета Европе о борби против трговине људима, Службени гласник РС – Међународни уговори, бр. 19/2009. члан 4 и Протокол за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминала усвојен у Палерму, децембра 2000. године, Службени гласник РС – Међународни уговори, бр. 6/2001, члан 3;

или делова тела од давно мртвог лица; с обзиром на циљ, односно сврху одузимања органа или дела тела: узимање органа или делова тела ради задовољења здравствених потреба лица и узимање органа или делова тела у научно–истраживачке сврхе[961].

Трговци људима су сва лица која су укључена у процес трговања људима (учествују у врбовању жртава, њиховом спровођењу, превожењу, чувању, обезбеђењу смештаја, контролисању или експлоатацији)[962]. То су особе које су регрутовањем (врбовањем), спровођењем, превожењем, чувањем, обезбеђењем смештаја, контролисањем или експлоатицијом људи, укључене у процес трговања њима. Према дефиницији Уједињених нација, сви трафикери се могу класификовати као регрутери или врбовници (*recruiters)*, превозници (*transporters*), контролори жртава (*controlers*), они који врше трансфер и/или одржавају лица у експлоататорском положају, они који су умешани у криминал у вези с тим и они који профитирају, било директно било индиректно, од трговине људима, појединих њених облика или сродних прекршаја[963].

Услуга информационог друштва је услуга која се пружа на даљину уз накнаду путем електронске опреме за обраду и складиштење података, на лични захтев корисника услуга, а посебно продаја робе и услуга путем интернета, нуђење података и рекламирање путем интернета, електронски претраживачи, као и омогућавање тражења података и услуга које се преносе електронском мрежом, обезбеђивање приступа мрежи или складиштење података корисника услуга[964].

Уточиште је право на боравак и заштиту која се даје избеглици на територији Републике Србије за кога надлежни орган утврди да је његово страховање од прогона у држави порекла основано. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Својство члана породице може се изузетно признати и другим лицима при чему се посебно узима у обзир чињеница да су била издржавана од стране лица коме је одобрено уточиште или субсидијарна заштита. Закон о азилу, Службени гласник Републике Србије, бр. 109/07.

Фејсбук[965] (енг. *Facebook*) је једна од највећих светских комерцијалних интернет друштвених мрежа. Састоји се од веб-сајта који служи као сервис корисника који регистрацијом добијају налог и везом између тих људи. Сваки корисник може затражити од другог корисника да постане његов пријатељ тиме што му шаље захтев на који предходни мора да одговори да ли одобрава или не. Корисници могу придруживати у мреже које су организоване по разним критеријумима: градовима, даним местима, школама, универзитетима и слично.

---

961 Мијалковић, С. (2005). Облици и видови трговине људима. *Темида*, 8 (1), стр. 41;

962 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, (2012) стр. 133;

963 Смерница 2, *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, United Nations High Commisissioner for Human Rights to the Economic and Social Council, E/2002/68/Add.1, New York, 2002;

964 преузето из Закона о електронским комуникацијама, члан 4. (Службени Гласник РС бр. 44/2010)

965 "Key Facts". *Facebook Newsroom*. Facebook. Retrieved May 2, 2013., "Is Facebook the New MySpace?". *PC World* (San Francisco). Retrieved April 30, 2008;

Физичко лице је човек као правни субјект, тј. ималац правне способности[966].

Фишинг[967] (енг. *Phishing*) представља чин покушаја преваре како би се украле вредне информације као што су бројеви кредитних картица и социјалног осигурања, као и корисничка имена и шифре. Овај термин је познат и под називом "Brand spoofing", јер се потенцијалним жртвама шаље е-пошта званичног изгледа са потписом њихове банке. Ове поруке могу да се шаљу људима на одабраним листама, или на било којим листама, уз очекивање да ће одређени проценат људи којима је е-пошта послата заиста имати рачун у тој банци.

Форум представља он-лајн дискусију која је представљена на неком веб-сајту и у којој учесници форума могу да одржавају разне конверзације у форми написаних порука. Предност форума у односу на собе за ћаскање је у томе што су поруке дискусије сачуване на дуг временски период и не бришу се. Конверзације су груписане по теми, теме су груписане у категорије. Свако регистрован на форуму може остављати поруке у конверзацији дате теме или може покретати нову тему[968].

Фазе трговине људима могу укључивати: фазу „порекла“, фазу „транзита“, фазу „дестинације“ и фазу „елиминације“.

Фаза порекла је прва фаза кријумчарења мигранта и трговине људима која се одвија на међународном нивоу. Одвија се у земљи порекла и неретко је одликује деловање организоване криминалне групе са адекватном структуром, стварање злочиначког плана и регрутовање мигранта, односно жртава трговине људима[969].

Фаза транзита жртава трговине људима је друга фаза у процесу трговине људима и подразумева транспортовање жртава до места њихове дестинације, а када је реч о међународној трговини људима одвија се у тзв. земљама порекла, транзита и/или дестинације жртава и обухвата планирање и организовање транспорта и логистичке подршке, транспортовање лица и прелажење државне границе. Ова фаза може да подразумева не само пребацивање са једног места на друго, већ и скривање жртве и озбиљно кршење људских права (кроз нехумане услове транспорта и сакривања, физичко и психичко злостављање)[970].

Фаза дестинације је трећа фаза кријумчарења мигранта и трговине људима која се одвија у земљи дестинације жртава. Судбина прокријумчарених мигранта и жртава трговине људима у овој фази је различита. Над *жртвама трговине људима* заснива се ропски однос и оне су сурово експлоатисане. Смештају их у одређене објекте из којих не могу својевољно да оду (високе ограде, постављене камере, физичко обезбеђење и слично) или их контролишу на други начин. Жртве тзв. добровољне трговине људима добијају фалсификоване идентификационе исправе (путне

966 Обрен Станковић, Владимир Водинелић (2007) „Увод у грађанско право”;

967 http://www.pcmag.com/encyclopedia/term/49176/phishing, датум последњег приступа 26.3.2014;

968 "Glossary Of Technical Terms". Green Web Design. 2008-04-28., "Forum Software Timeline 1994 - 2010". Forum Software Reviews. 2010-12-24., "vBulletin Community Forum - FAQ: What is a bulletin board?"

969 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 81;

970 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 91;

исправе, личне карте, пријаве боравка и слично) или задржавају лична документа и укључују се у процес експлоатације[971].

Као што је истакнуто, **експлоатација** обухвата, као минимум, експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа. Експлоатација жртава је кључни моменат трговине људима: то је основно средство за остваривање енормно високог противправног профита, што је и њен главни узрок.

Операционализацијом датих дефиниција и уважавањем видова и облика намераване, односно извршене експлоатација који њима нису предвиђени, могу се идентификовати следећи *доминантни видови експлоатације жртава трговине људима*: продаја жртве другом лицу, тз. „препродаја људи"; радна експлоатација; сексуална експлоатација; илегално усвојење деце; принудно склапање бракова; трговина људским органима или деловима тела; принудно учешће у оружаним сукобима; принудно вршење одређњих криминалних радњи и остали, неспецифични облици експлоатације[972].

Хостинг[973] представља било какву врсту поседовања, дељења и дистрибуције садржаја, сервиса и услуга на рачунарским мрежама.

Хакер у оригиналном значењу означава свакога ко је веома заинтересован да научи све о компјутерским системима и њиховом коришћењу на нови и "паметан" начин, те многи компјутерски ентузијасти себе зову хакерима у, овом, непежоративном значењу[974]. Хакери су и појединци или групе које пробијају заштиту окружења компјутерског система, специјалног он-лајн сервиса, чинећи то из малициозности или нетрпељивости, али често и из политичких разлога[975]. Хакер означава и сваког програмера који експлоатише, проверава или доводи компјутерске и комуникационе системе до крајњих граница, без обзира на последице. Понекад то може довести и до уништења или саботаже вредних података, као и великих штета[976]. Слично је и одређење да је то неауторизовани приступ систему или бази података од стране неауторизоване особе[977]. *Хакинг* је неауторизовани, насилни приступ, односно покушај приступа систему (компјутерском, комуникационом), а хакер је особа која има знање,способности и

971 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 92-93;

972 Мијалковић, С. Жарковић, М. (2012), Илегалне миграције и трговина људима, Криминалистичко-полицијска академија, Београд, 2012, стр. 153-154;

973 http://en.wikipedia.org/wiki/Internet_hosting_service, датум последњег приступа 5.12.2013; http://www.webopedia.com/TERM/H/hosting_server.html, датум последњег приступа 5.12.2013;

974 Denning D., (1990), "A Dialog on Hacking and Security, Edicija: Computers Under Attack, Intruders, Worms, and Viruses", New York, ACM Press;

975 Peckitt R.,(1989), Computers In General Practice, Wilmslow, Sigma Press;

976 Grupa autora, (1990), Organizing for Computer Crime: Investigation and Prosecuting, National Institute of Justice USA;

977 Peckitt R., op. cit., str. 136;

жеље да у потпуности неовлашћено користи туђе компјутерске и комуникационе системе[978].

Црв је облик штетног софтвера који се реплицира и шири на различите рачунаре преко мреже[979]. За разлику од вируса црв функционише независно од неког постојећег програма. Црв оптерећује саобраћај мреже, оштећује и модификује податке или омогућава неовлашћеног приступа неком рачунару.

Центар за азил је објекат за смештај лица која су поднела захтев за азил на територији Републике Србије.

Члан породице је супружник ако је брак закључен пре доласка у Републику Србију, малолетно дете, усвојеник, односно пасторак, као и родитељ и усвојитељ који су по закону дужни да га издржавају.

978 Дракулић М.,(1996), оп.цит., стр. 433;

979 http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm
http://www.microsoft.com/security/pc-security/worms-remove.aspx, датум последњег приступа 4.12.2013;

ПРИЛОЗИ

Прилог бр.1
Анкета за високотехнолошки криминал

Напомена: Пажљиво прочитајте свако питање и заокружите слово испред Вашег одговора (на затвореним питањима) или допишите одговор (на отвореним питањима). Хвала на уложеном времену.

1. **Пол:**
   а. женски
   б. мушки

2. **Године старости:**
   а. од 6 – мање од 10
   б. од 10 – мање од 14
   в. од 14 – мање од 16
   г. од 16 – мање од 18
   д. од 18 – мање од 30
   ђ. од 30 – мање од 45
   е. од 45 – мање од 60
   ж. преко 60

3. **Држава рођења:**
   а. СФРЈ
   б. СРЈ
   в. РС
   г. друга _____
   д. не знам / не желим да одговорим

4. **Националност:**
   а. српска
   б. не знам / не желим да одговорим
   в. друга _____

5. **Место** (Напомена: могу попунити и анкетари у зависности од места у коме спроводе истраживање):
   а. боравка у Србији _____
   б. пребивалишта у Србији: _____

6. **Место у коме сада живите има** (Напомена: могу попунити и анкетари у зависности од места у коме спроводе истраживање):
   а. до 5.000 становника
   б. 5.000 до 20.000 становника
   в. 20.000 до 100.000 становника
   г. 100.000 до 500.000 становника
   д. преко 500.000 становника

7. **Брачни статус** (Напомена: не попуњавају деца у основној школи):
   а. неожењен/неудата
   б. ожењен/удата
   в. разведен/разведена
   г. удовац/удовица

8. **Стамбени статус:**
   а. у стану / кући
   б. у изнајмљеном стану
   в. у ученичком / студентском / другом дому
   г. у кампу за азиланте / имигранте
   д. у привременом боравишту који ми је обезбедила Влада Србије

9. **Завршен ниво образовања** (Напомена: могу попунити и анкетари у зависности институције у којој спроводе истраживање):
   а. без школе
   б. основно
   в. средње
   г. више
   д. високо

10. **Област образовања** (Напомена: могу попунити и анкетари у зависности институције у којој спроводе истраживање):
    а. опште образовање
    б. друштвено-хуманистичка
    в. медицинско-биолошка
    г. природно-математичка
    д. техничко-технолошка
    ђ. уметност
    е. остало _____

11. **Радни статус** (Напомена: не попуњавају деца у основној и средњој школи):
    а. запослен/а
    б. незапослен/а
    в. привремено запослен/а
    г. повремено запослен/а
    д. пензионер

12. **Где сте запослени, а за незапослене и пензионере где сте били запослени** (Напомена: не попуњавају деца у основној и средњој школи)?

а. пољопривреда, лов, шумарство, рибарство	једноставни послови стручни послови
б. рударство	једноставни послови стручни послови
в. снабдевање електричном енергијом	једноставни послови стручни послови

г. снабдевање водом, управљање отпадним водама,контролисање процеса уклањања отпада једноставни послови
стручни послови

д. грађевинарство једноставни послови
стручни послови

ђ. трговина једноставни послови
стручни послови

е. саобраћај и складиштење једноставни послови
стручни послови

ж. услуге смештаја и исхране једноставни послови
стручни послови

з. информисање и комуникације једноставни послови
стручни послови

и. финансијске делатности и делатности осигурања
једноставни послови
стручни послови

ј. пословање са некретнинама једноставни послови
стручни послови

к. стручне, научне, иновационе и техничке делатности
једноставни послови
стручни послови

л. административне и помоћне услужне делатности
једноставни послови
стручни послови

љ. јавна управа (државна управа, локална самоуправа, агенције, друго)
једноставни послови
стручни послови

м. одбрана, полиција једноставни послови
стручни послови

н. образовање једноставни послови
стручни послови

њ. здравствена и социјална заштита једноставни послови
стручни послови

о. Уметност, забава и рекреација једноставни послови
стручни послови

п. друге делатности: _____
једноставни послови
стручни послови

13. Оцените Ваш економски статус (Напомена: не попуњавају деца у основној и средњој школи):

а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

14. Да ли знате неки страни језик?

а. да, наведите које _____

б. не

15. Да ли знате да користите рачунар?

а. да

б. не

16. Да ли имате рачунар? (Напомена: могуће је заокружити више одговора):

а. да, код куће имам десктоп

б. да, лаптоп / ноутбук / таблет

в. не

17. Да ли имате могућност коришћења рачунара у школи / на факултету / на послу?

а. да, имам „свој“ рачунар који свакодневно користим

б. да, имамо информатички кабинет / рачунарски центар који могу стално да користим

в. да, имамо информатички кабинет / рачунарски центар који могу повремено да користим

г. не, немам приступ рачунарима

18. Где и колико користите рачунар?

а. код куће	увек	често	понекад	ретко	никад
б. на факултету/ у школи	увек	често	понекад	ретко	никад
в. на послу	увек	често	понекад	ретко	никад
г. у интернет-кафеу	увек	често	понекад	ретко	никад
д. у играоници	увек	често	понекад	ретко	никад
ђ. на јавним местима (wирелесс / хотспот)	увек	често	понекад	ретко	никад

19. За које сврхе користите рачунар?

а. учење	увек	често	понекад	ретко	никад
б. посао	увек	често	понекад	ретко	никад
в. информисање	увек	често	понекад	ретко	никад
г. комуникацију	увек	често	понекад	ретко	никад
д. забаву	увек	често	понекад	ретко	никад
ђ. играње игрица	увек	често	понекад	ретко	никад
е. коцкање	увек	често	понекад	ретко	никад
ж. остало	увек	често	понекад	ретко	никад

20. Да ли имате мобилни телефон?

а. да, обичан

б. да, смарт

в. не

21. Да ли користите интернет?

а. да
б. не

22. Ако користите интернет, колико је то често?

а. неколико пута месечно
б. једном недељно
в. неколико пута недељно
г. свакодневно до једног сата
д. свакодневно од једног до пет сати
ђ. свакодневно преко пет сати

23. Ако користите интернет, коју врсту везе углавном користите? (Напомена: заокружите само везу коју најчешће користите):

а. диал уп
б. АДСЛ
в. кабловску
г. 3G / 4G
д. не знам

24. Које сајтове посећујете на интернету?

а. образовне	увек	често	понекад	ретко	никад
б. информативне	увек	често	понекад	ретко	никад
в. музичке/ филмске	увек	често	понекад	ретко	никад
г. за поруке	увек	често	понекад	ретко	никад
д. chat роом-ове	увек	често	понекад	ретко	никад
ђ. друштвене мреже	увек	често	понекад	ретко	никад
е. за игрице	увек	често	понекад	ретко	никад
ж. за игре на срећу	увек	често	понекад	ретко	никад
з. за преуз. филм/муз	увек	често	понекад	ретко	никад
и. за упознавање	увек	често	понекад	ретко	никад
ј. за тражење посла	увек	често	понекад	ретко	никад
к. нешто друго	увек	често	понекад	ретко	никад

25. Коју од наведених сервиса користите за комуникацију путем интернета?

а. *webmail*	увек	често	понекад	ретко	никад
б. *web to sms service*	увек	често	понекад	ретко	никад
в. *чет апликације*	увек	често	понекад	ретко	никад
г. друштвене мреже	увек	често	понекад	ретко	никад
д. *VoIP*	увек	често	понекад	ретко	никад

26. Да ли четујете преко телефона или рачунара?

а. да, свакодневно
б. да, често
в. понекад
г. пробала/о сам али ми се није свидело
д. не
ђ. не знам шта је то

27. Заокружите *чет апликације* које користите (Напомена: могуће је заокружити више одговора):

а. IRC
б. MSN
в. YAHOO! Messenger
г. Facebook Messenger
д. SKYPE
ђ. G-Talk
е. WhatsApp
ж. користим неку андроид апликацију
з. ништа од наведеног

28. Да ли сте некоме доставили он-лајн своје податке? (Напомена: могуће је заокружити више одговора)

а. да, име и презиме
б. да, адресу
в. да, број телефона
г. да, број личне карте
д. да, матични број
ђ. да, број пасоша
е. да, број кредитне картице
ж.да, број индекса
з. да, нешто друго
и. да, лозинку
ј. не

29. Ако јесте, наведите коме (Напомена: могуће је заокружити више одговора):

а. особи коју не познајем
б. на сајту приликом регистровања
в. продавници на њиховм сајту приликом наручивања
г. органу управе
д. страној амбасади
ђ. банци / школи / факултету
е. здравственим установама
ж.невладиним организацијама
з. туристичкој агенцији
и. мобилном оператеру
ј. интернет провајдеру
к. члану породице
л. пријатељу
љ.познанику

30. На који начин сте доставили личне податке? (Напомена: могуће је заокружити више одговора)

а. попуњавањем он-лајн формулара
б. е-поштом
в. преко друштвене мреже
г. преко апликације

д. попуњавањем шерованих докумената
ђ. на други начин _____

31. Да ли читате услове под којим остављате Ваше податке?
а. да, пажљиво
б. да, само информативно
в. да, понекад
г. не, не разумем их
д. не, само их прихватим
ђ. не, не знам ни да постоје

32. Да ли мислите да се мобилни уређај/рачунар може злоупотребити? (Напомена: могуће је заокружити више одговора)
а. да, за крађу идентитета на разним мрежама
б. да, за „скидање" филмова и музике
в. да, за пословну шпијунажу
г. да, за преузимање података о личности
д. да, за злоупотребу картица
ђ. да, за „упаде у рачунаре"
е. да, за насиље
ж. не, није могуће

33.Познајете ли некога ко користи рачунар у те сврхе?
а. да, познајем неколико особа
б. да, познајем једну особу
в. не познајем никога

34. Какво је Ваше мишљење о тим особама (Напомена: не попуњавају деца у основној и средњој школи)?
а. то је супер, и ја бих се тиме бавио/ла
б. то је ОК, али ја то никада не бих урадио/ла
в. то је његова/њена ствар
г. знам да је то забрањено и никада то не бих урадио/ла
д. пријавио/ла бих га да знам коме

35. Да ли знате шта је *phishing*?
а. да, то је _____
б. чуо/ла сам, али не знам ништа о томе
в. не

36. Да ли су потребна специфична информатичка знања да би неко то радио?
а. да
б. не
в. не знам

37. Поседујете ли Ви та знања?

а. да
б. не
в. не знам

38. Да ли сте некада били жртва *phishing*-а?

а. да
б. не
в. не знам

39. Да ли знате шта је *hacking*?

а. да, то је _____
б. чуо/ла сам, али не знам ништа о томе
в. не

40. Да ли су потребна специфична информатичка знања да би неко био хакер?

а. да
б. не
в. не знам

41.Поседујете ли Ви та знања?

а. да
б. не
в. не знам

42. Да ли сте некада били жртва *хакинг*-а?

а. да
б. не
в. не знам

43. Да ли Вам је некада неко преузео идентитет на некој друштвеној мрежи?

а. да
б. не
в. не знам

44.Да ли је неко злоупотребио Вашу платну картицу (Напомена: не попуњавају деца у основној и средњој школи)?

а. да
б. не
в. не знам

45.Можете ли да замислите живот без рачунара / мобилног телефона?

а. да, радо бих се одрекао/ла свега тога
б. да, али би ми тешко пало
в. не

На питања наредна питања одговарате само ако користите друштвене мреже

46. Заокружите друштвену мрежу на којој поседујете налог (Напомена: могуће је заокружити више одговора):

а. Facebook
б. Twitter
в. YoyTубе
г. LinkedIn
д. Google +
ђ. Foursquare
е. Tumblr
ж. друге _____
з. немам налог ни на једној друштвеној мрежи

47. Како сте сазнали за друштвене мреже које користите? (Напомена: могуће је заокружити више одговора)

а. од пријатељ
б. случајно претражујући интернет
в. путем медија
г. нисам чуо/ла за њих

48. Са ким комуницирате путем друштвених мрежа?

а. са члановима породице	увек	често	понекад	ретко	никад
б. са најближим пријатељима	увек	често	понекад	ретко	никад
в. са дечком/ девојком	увек	често	понекад	ретко	никад
г. са он-лајн пријатељима	увек	често	понекад	ретко	никад
д. са познаницима	увек	често	понекад	ретко	никад
ђ. са колегама и сарадницима	увек	често	понекад	ретко	никад
е. са непознатима	увек	често	понекад	ретко	никад

49. У које сврхе користите ове сајтове?

а. за зближав.са чл.породице	увек	често	понекад	ретко	никад
б. за зближав.са пријатељима	увек	често	понекад	ретко	никад
в. за проналажење „изгубљених“ рођака, пријатеља и познаника	увек	често	понекад	ретко	никад
г. за упознавање више особа	увек	често	понекад	ретко	никад
д. за повезивање са особама сличних/ истих интересовања	увек	често	понекад	ретко	никад
ђ. за посредовање	увек	често	понекад	ретко	никад
е. за остварење емотивних веза	увек	често	понекад	ретко	никад
ж. за проналажење посла	увек	често	понекад	ретко	никад
з. то је део мог посла	увек	често	понекад	ретко	никад
и. за „убијање времена“	увек	често	понекад	ретко	никад

50. Како одржавате контакт са он-лајн пријатељима? (Напомена: могуће је заокружити више одговора):

а. преко интернета
б. путем мобилног телефона
в. личним контактима

51. Да ли сте се физички срели са неким кога сте упознали путем интернета?

а. да
б. не

52. Ако јесте, са колико?

а. мање од 3
б. 3 – 20
в. преко 20

53. Како сте након физичког сусрета наставили контакт са он-лајн познаницима? (Напомена: заокружите само један одговор):

а. виђамо се интезивно
б. виђамо се ретко
в. чујемо се
г. само он-лајн
д. прекинули смо контакт

54. Колико пријатеља имате на Facebook-у/Twitter-у/Google+/Tumbrl

(Напомена: заокружите одговор само за мрежи коју највише користите)?

а. до 100
б. 101 - 500
в. 501 – 1000
г. 1001 - 2000
д. преко 2000

55. Колико сте он-лајн пријатеља раније познавали?

а. све
б. већину
в. неколико
г. никога

56. Ваш профил на друштвеној мрежи могу да виде:

а. сви
б. пријатељи пријатеља
в. пријатељи
г. лажно се представљам
д. нико, кријем се

57. Које податке приказујете? (Напомена: могуће је заокружити више одговора):

а. име, презиме, датум рођења
б. интересовања
в. фотографије
г. адресу
д. контакт телефон
ђ. е-пошту
е. статус (сам/а, у вези, ожењен/удата ...)
ж. измишљам податке

58. Да ли сте покушали да деактивирате Ваш налог?

а. да
б. не

59. Да ли Вас брине могућност злоупотребе података које сте оставили?

а. да
б. не, није ми битно
в. не, мислим да то није могуће

60. Да ли добијате он-лајн понуде?

а. да
б. не

61. Ако добијате, какве су садржине:

а. запошљавање
б. туристичка путовања
в. школовање
г. лечење
д. уручивање новчаних награда
ђ. помоћ за добијање боравишне / радне дозволе
е. брачне
ж. пословне
з. заједничка летовања/зимовања
и. позив за чланство у групу / организацију
ј. заједнички викенди
к. остало _____

62. Колико често Вам стижу овакве понуде?

а. веома често
б. често
в. повремено
г. ретко, једанпут
д. никада

63. Како сте реаговали на овакве поруке?

а. одговорио/ла сам
б. прочитао/ла сам, али нисам реаговао/ла
в. прочитао/ла сам и обрисао/ла
г. обрисао/ла без читања
д. пријавио/ла _____

64. Да ли сте имали проблема са злоупотребом Ваших података?

а. да
б. не

65. Ако јесте, каквих?

а. крађа идентитета
б. крађа платних картица

в. дистрибуција података о личности
г. добијање нежељених порука (*спам*)
д. он-лајн узнемиравање
ђ. физичко узнемиравање
е. сексуално узнемиравање
ж. остали видови узнемиравања _____

66. Да ли сте се на друштвеној мрежи суочили са:

а. неко ми је преузео профил
б. неко је отворио лажан профил представљајући се као ја
в. постављају моје фотографије без питања и тагују ме
г. непознати ме зову на број телефона који сам оставио/ла на профилу
д. добијао/ла сам разне „сексуалне“ понуде
ђ. добијао/ла сам пословне понуде
е. нешто друго _____

67. Да ли имате искуства са насиљем преко друштвених мрежа?

а. да, учествовао/ла сам у томе
б. да, основао/ла сам групу која је против _____
в. да, учлањен/а сам у групу која мрзи _____
г. да, гледао/ла сам више пута клипове и фотографије малтретирања
д. да, "шалимо" се често због разних "глупости" које неки постављају
ђ. да, постављали су понижавајуће фотографије мене и исмејавали ме
е. да, вређају ме и називају свакаквим именима
ж. да, претили су ми више пута
з. не, али знам да су неки то доживели
и. не, никада нисам чуо/ла за то

68. Ако "налетите" на "говор мржње" на интернету да ли бисте?

а. пријавили администратору случај
б. пријавили неком старијем кога познајете
в. пријавили полицији
г. заборавили на то јер вас не занима шта други раде
д. насмејали се и лајковали ако се слажете са тим
ђ. оставили похвални коментар

69. На који начин су друштвене мреже утицале на Ваш живот? (Напомена: могуће је заокружити више одговора)

а. нашао/ла сам посао
б. преселио/ла сам се у иностранство
в. нашао/ла сам животног партнера
г. упознао/ла сам више партнера
д. интензивнији ми је емотивни живот
ђ. више комуницирам са пријатељима
е. упознао/ла сам више људи
ж. све мање се виђам са пријатељима
з. прекинуо/ла сам неке контакте
и. нешто друго _____

Прилог бр.2
Анкета за припаднике одељења за борбу против ВТК СБПОК, УКП, МУП РС и УГП, тужилаштво и суд

Као фокус-групе ове анкете и могућих питања интервјуа, који се могу из овог текста извести, јављају се припадници полиције, конкретно одељења за борбу против ВТК СБПОК, УКП, МУП РС и УГП, тужилаштво и суд.

Напомена: На сва питања анкете могуће је заокружити више одговора.

1. **Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију као кривично дело из чл.185 КЗ према Вашим сазнањима обухвата:**
   а. лица до 14 година,
   б. лица од 14 до18 година,
   в. лица од 14 до 16 година,
   г. лица од 18 до 21 година,
   д. не знам.

2. **Ово дело се може чинити и у оквиру:**
   а. илегалних миграција,
   б. трговине људима,
   в. класичних кривичних дела,
   г. кривичних дела организованог криминала,
   д. корупције,
   ђ. других тешких кривичних дела,
   е. _____
   ж. не знам.

3. **Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:**
   а, продајом, приказивањем или јавним излагањем или на други начин чињење доступним текстова, слика, аудио-визуелних или других предмета порнографске садржине малолетнику или приказивањем порнографске представе малолетнику;
   б. искоришћавањем малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу;
   в. дело из ст. 1 и 2 овог члана учињено према детету;
   г. прибављањем за себе или другог, поседовањем, продајом, приказивањем, јавним излагањем или електронски или на други начин чињењем доступним слика, аудио-визуелних или других предмета порнографске садржине настале искоришћавање ммалолетног лица;
   д. није их било.

4. Да ли има оних појавних облика који нису обухваћени законом?

а. да _____
б. не,
в. не знам.

5. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела?

_____
_____

6. Да ли сте били на посебним обукама и тренинзима за примену ИКТ у области којом се бавите и наведите којим?

_____
_____

7. Уколико сте на питање бр. 4 одговорили са ДА објасните да ли се и на који начин недоследности злоупотребљавају:

а. злоупотребљавају се _____
б. не
в. не знам

8. Навођење малолетног лица на присуствовање полним радњама (члана 185а, КЗ РС)односи се на:

а. малолетна лица увек често понекад ретко никад
б. децу увек често понекад ретко никад
в. примену силе или претње увек често понекад ретко никад
г. посредно присуство кажњивим радњама путем интернета малолетног лица или детета увек често понекад ретко никад
д. нешто друго _____

9. Ово дело се према Вашим сазнањима може вршити и у оквирима:

а. илегалних миграција увек често понекад ретко никад
б. трговине људима увек често понекад ретко никад
в. класичних кривичних дела увек често понекад ретко никад
г. кривичних дела организованог криминала, корупције и других тешких кривичних дела увек често понекад ретко никад
д. нешто друго _____

10. Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

а. навођењем малолетника да присуствује силовању, обљуби или са њом изједначеним чином или другој полној радњи;
б. дело учињено употребом силе или претње или према детету;
в. не знам.

11. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____

12. Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из члана 185б се према Вашем искуству вршило следећим средствима ИКТ:

а. различитим уређајима за аудио-визуелно снимање
увек често понекад ретко никад
б. смарт телефонима увек често понекад ретко никад
в. таблетима увек често понекад ретко никад
г. лаптоповима увек често понекад ретко никад
д. друго

13. Ово дело се може вршити и у оквирима:

а. илегалних миграција увек често понекад ретко никад
б. трговине људима увек често понекад ретко никад
в. класичних кривичних дела увек често понекад ретко никад
г. кривичних дела организованог криминала
увек често понекад ретко никад
д. корупције и других тешких кривичних дела
увек често понекад ретко никад
ђ. _____

14. Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

а. у намери извршења кривичног дела из чл. 178 став 4, 179 став 3, 18. ст. 1 и 2, 181 ст. 2 и 3, 182 став 1, 183 став 2, 184 став 3, 185 став 2. и 185а КЗ, користећи рачунарску мрежу или комуникацију другим техничким средствима, договори са малолетником састанак и појави се на договореном месту ради састанка;
б. ко дело изврши према детету;
в. не знам.

15. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____
_____

16. Повреда моралних права аутора и интерпретатора из члана 198 КЗ врши се у ком облику:

а. када извршилац под својим именом или именом другог у целини или делимично објави, стави у промет примерке туђег ауторског дела или интерпретације или на други начин јавно саопшти дело или интерпретацију;
б. без дозволе аутора измени или преради туђе ауторско дело или измени туђу снимљену интерпретацију;
в. не знам.

17. Ово дело се према Вашим сазнањима може вршити и у оквирима:

а. илегалних миграција увек често понекад ретко никад
б. трговине људима увек често понекад ретко никад
в. класичних кривичних дела увек често понекад ретко никад
г. кривичних дела организованог криминала, корупције и других тешких кривичних дела
увек често понекад ретко никад
д. нешто друго _____

18. Наведите посебна средства извршења овог кривичног дела на које сте наилазили у свом раду:

_____
_____
_____

19. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____
_____
_____

20. Према Вашем искуству са прибављањем предлога за кривично гоњење оваквих кривичних дела?

а. лако се прибављају увек често понекад ретко никад
б. постоје одређенин проблеми увек често понекад ретко никад
в. најчешће се не добијају увек често понекад ретко никад
г. _____

21. Неовлашћено искоришћавање ауторског дела или предмета сродног права према члану 199, према Вашем искуству најчешће се гоне:

а. основни облици кривичног дела увек често понекад ретко никад
б. тежи облик увек често понекад ретко никад
в. посебни облик увек често понекад ретко никад
г. припремне радње за извршење овог дела
увек често понекад ретко никад
д. _____

22. Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

а. списак из закона и
б. не знам.

23. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____
_____
_____

24. Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (члан 200 КЗ РС), најчешће се врше:

а. посебним уређајима _____

б. посебним рачунарским програмима _____

в. друго _____

25. Наведите начине извршења овог кривичног дела и његове облике на које сте наилазили у свом раду:

а. неовлашћено уклањање или измена електронске информације о ауторском или сродном праву;

б. стављањем упромет, увозом, извозом, емитовањем или на други начин јавним саопштавањем ауторског дела или предмета сродно правне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена;

в. на други начин: _____

26. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____

_____

_____

27. Како се утврђују носиоци ових права, која се штите овим делом (чл. 200 КЗ РС)?

_____

_____

_____

28. Наведите начине извршења кривичног дела превара (члан 208 КЗ), а које не спадају у кд. из чл.301КЗ и његове облике на које сте наилазили:

а. ко у намери да себи или другом прибави противправну имовинску корист доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини;

б. дело учињено само у намери да другог оштети;

в. када је делом из ст. 1 и 2 овог члана прибављена имовинска корист или је нанета штета у износу који прелази 450 хиљада динара;

г. када је делом из ст. 1 и 2 овог члана прибављена имовинска корист или је нанета штета у износу који прелази милион и петсто хиљада динара;

д. не знам

29. Које информационо-комуникационе технологије би требало користити у сузбијању и спречавању овог дела:

_____

_____

_____

У ком обиму се ова дела врше само у циљу наношења штете другоме као привилегованом облику овог дела?

а. увек,
б. често,
в. понекад,
г. ретко,
д. никад.

Наведите начине извршења кривичног дела Фалсификовање и злоупотреба платних картицаиз члана 225, и његове облике на које сте наилазили:

_____

_____

У ком обиму се појављује облик овог кривичног дела из ст. 4 којим се инкриминише неовлашћена употреба туђе картице или података о личности власника картице и шифара које иду уз исте:

а. увек,
б. често,
в. понекад,
г. ретко,
д. никад.

У ком обиму облик из ст. 5 инкриминише набављање лажне платне картице у намери њене употребе као праве или прибављање података у намери да се исти искористе за прављење лажне платне картице:

а. увек,
б. често,
в. понекад,
г. ретко,
д. никад.

Наведите начине извршења кривичног дела Оштећење рачунарских података и програма из члана 298 КЗ и његове облике на које сте наилазили:

а. неовлашћено брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма;
б. уколико је делом из става 1 овог члана проузрокована штета у износу који прелази 450 хиљада динара;
в. уколико је делом из става 1 овог члана проузрокована штета у износу који прелази 1.500.000 динара;
г. неки други

Инкриминација овог дела (чл. 298 КЗ) оправдана је у тежем облику за износ штете који прелази 450 000 динара?

а. јесте,
б. није оправдана,
в. могла је бити и у мањем износу,
г. могла је бити и у већем износу,
д. не знам.

Наведите начине извршења кривичног дела Рачунарска саботажа из члана 299 КЗ и његове облике на које сте наилазили:

а. уношењем, уништењем, брисањем, изменом, оштећењем, прикривањем или на други начин чињењем неупотребљивим рачунарског податка или програма;
б. уништењем или оштећењем рачунара или другог уређаја за електронску обраду и пренос података
в. не знам

У којој мери је ово дело различито од кривичног дела прописаног делом оштећење рачунарских података и програма?

_____

Наведите начине извршења кривичног дела Прављење и уношење рачунарских вируса члан 300 и његове облике на које сте наилазили:

а. прављење рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу;
б. уношење рачунарског вируса у туђ рачунар или рачунарску мрежу и тиме проузроковањем штете;
в. не знам.

Колико је прављење рачунарских вируса у намери уношења у рачунар и рачунарску мрежу:

а. увек,
б. често,
в. понекад,
г. ретко,
д. никад.

Наведите начине извршења кривичног дела Рачунарска превара члан 301 и његове облике на које сте наилазили:

а. уношење нетачног податка, пропуштање уношења тачног податка или на други начин прикривање или лажно приказивање података и тиме утицање на резултате електронске обраде и преноса података;
б. ако је делом из става 1 овог члана прибављена имовинска корист која прелази износ од 450 хиљада динара;
в. уколико је делом из става 1 овог члана прибављена имовинска корист која прелази износ од 1.500.000, учинилац ће се казнити затвором од две до десет година;
г. када дело учини само у намери да другог оштети.

Колико је у практичном раду заступљено ово дело у свом облику који се састоји у вршењу основног облика у намери наношења штете другоме?

а. увек,
б. често,
в. понекад,
г. ретко,
д. никад.

Наведите начине извршења кривичног дела Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података члан 302 и његове облике на које сте наилазили:

а. кршењем мера заштите, неовлашћеним укључивањем у рачунар или рачунарску мрежу;
б. неовлашћено приступање електронској обради података;
в. снимањем или употреба података добијених на начин предвиђен у ставу 1;
г. ако је услед дела из става 1 овог члана дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мрежеили су наступиле друге тешке последице;
д. не знам.

Наведите начине извршења кривичног дела Спречавање и ограничавање приступа јавној рачунарској мрежи члан 303 и његове облике на које стенаилазили:

а. неовлашћено спречавање или ометање приступа јавној рачунарској мрежи;
б. ако дело из става 1 овог члана учини службено лице у вршењу службе
в. не знам.

Наведите начине извршења кривичног дела Спречавање и ограничавање приступа јавној рачунарској мрежи безбедности рачунарских података члан 304а и његове облике на које сте наилазили:

а. поседовањем,
б. прављењем,
в. набављањем,
г. продајом,
д. давањем другом на употребу рачунара, рачунарских система, рачунарских података и програма ради извршења кривичногдела из чл. 298 до 303 овог законика.

Прилог бр.3
Жртве трговине људима - интервју за припаднике владиних и невладиних организација

Основни подаци о интервјуу

Датум интервјуисања_____

Место интервјуисања_____

Организација за коју ради:
а. владин сектор
б. невладин сектор

Назив организације за коју ради _____

Опишите природу свог поступања према жртви трговине људима:
а. у циљу откривања КД- извршиоца
б. превентивно
в. хуманитарно
(могуће је заокружити више опција)

Питања која се односе на коришћење савремених технолигија у идентификацији потенцијалне жртве-жртве трговине људима и откривању кривичног дела Трговина људима

1. **Да ли имате сазнања да су извршиоци кривичног дела Трговина људима користили неки облик савремених начина комуникација у некој од фаза извршења кривичног дела?**
   а. да
   б. не

2. **Који облик савремених начина комуникације је коришћен:**
   а. мобилни телефон
   б. рачунар
   в. други облик

3. **Који начин савремене комуникације је коришћен?**
   а. Друштвене мреже (Facebook, Twitter, LinkedIn, MySpace...)
   б. Skype
   в. Viber
   г. електронска пошта - e-mail
   д. путем интернета
   ђ. путем мобилног телефона

4. Да ли имате сазнања да жртве користе друштвене мреже?

а. да
б. не

5. Ако имате таква сазнања, заокружите друштвене мреже на којима су активни кријумчари из ваше праксе? (могуће је заокружити више одговора)**:**

а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. нема налог ни на једној друштвеној мрежи

6. Да ли су извршиоци кривичног дела Трговина људима на чијим сте случајевима радили користили рачунар/мобилни телефон у некој од фаза трговине људима?

а. да
б. не
Ако јесу, у којој?_____

7. Колико је рачунар/мобилни телефон помогао трговцу у контакту са жртвом и успостављању контаката са другим трговцима?

а. није му помогло
б. веома мало
в. доста му је помогао
г. није ми познато

8. Да ли сматрате да би трговци успели да ступе у контакт без помоћи рачунара/мобилног телефона?

а. да
б. не
в. можда

9. Да ли су вам у досадашњој пракси са жртвама познати случајеви коришћења мобилних рачунара/телефона на јавним местима, у циљу врбовања жртве (интернет-кафе, парк, шопинг- центар, трг или друго јавно место)?

а. да
б. не
в. није ми познато

10. На који начин је трафикер одржавао контакт са жртвом?

а. лично
б. путем фиксног телефона
в. путем мобилног телефона
г. путем интернета
д. преко посредника
ђ. на други начин_____

11. Да ли мислите да су грађани упознати са ризицима које са собом носи употреба информационо-комуникационих технологија?

а. да
б. не

12. Ако мислите да утиче, опишите на који начин.

13. Ако јесте, опишите те начине.

Прилог бр. 4
Интервју за жртве трговине људима

Основни подаци о интервјуу

Датум интервјуисања _____

Место интервјуисања _____

Која организација је интервјуисала жртву трговине људима_____

Подаци о жртви

1. Пол
- а. женски
- б. мушки

2. Године старости:
- а. 6 – 14
- б. 15 – 16
- в. 17 – 18
- г. 19 – 33
- д. 34 – 49
- ђ. 50 – 65
- е. преко 65

3. Држава рођења:
- а. СФРЈ
- б. СРЈ
- в. РС
- г. друга _____

4. Место рођења _____

5. Националност _____

6. Место боравка у Србији (за домаће и стране држављане):
- а. урбано подручје
- б. рурално подручје

7. Садашњи брачни статус:

а. неожењен/неудата
б. ожењен/удата
в. разведен/разведена
г. удовац/удовица
д. у ванбрачној заједници

8. Садашњи услови становања

а. код родитеља
б. у ученичком / студентском дому
в. у привременом боравишту који ми је обезбедила Влада Србије
г. у изнајмљеном стану
д. у свом стану

9. Школска спрема:

а. без школе
б. уписана али незавршена основна школа
в. завршена основна школа
г. уписана али незавршена средња школа/гимназија
д. завршена средња школа/гимназија
ђ. уписана али незавршена виша школа
е. завршена виша школа
ж. уписан али незавршен факултет
з. завршен факултет

10. Област образовања:

а. друштвено-хуманистичка
б. медицинско-биолошка
в. природно-математичка
г. техничко-технолошка
д. уметност
ђ. остало _____

11. Садашњи радни статус:

а. запослен/а
б. незапослен/а
в. привремено запослен/а
г. повремено запослен/а
д. пензионер/ка

12. Где сте запослени, а за незапослене и пензонере где сте били запослени?

_____

13. Оцените Ваш садашњи економски статус:

а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

14. Да ли говорите неки страни језик?

а. да, наведите које _____
б. не

15. Да ли знате да користите рачунар?

а. да
б. не

16. Да ли имате рачунар? (Напомена: могуће је заокружити више одговора):

а. да, код куће десктоп
б. да, лаптоп/ноутбук
в. не

17. Да ли имате мобилни телефон?

а. да
б. не

18. Да ли користите интернет?

а. да
б. не

19. Да ли користите друштвене мреже?

а. да
б. не

20. Ако користите друштвене мреже заокружите друштвену мрежу на којој поседујете налог (могуће је заокружити више одговора):

а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
г. немам налог ни на једној друштвеној мрежи

Подаци о ситуацији трговине људима

21. Година када је трафикер ступио у контакт са Вама _____
22. Година када сте укључени у трговину људима (година регрутације) _____
23. Година када сте се некоме обратили за помоћ _____

24. Коме сте се обратили:

а. полицији
б. другом државном органу (наведите ком) _____
в. невладиној организацији (наведите којој) _____

г. члану породице
д. пријатељу
ђ. неком другом (наведите коме) _____

25. Година изласка из трговине људима _____

26. Место смештаја након прекида експлоатације:
а. у породици порекла
б. у сигурној кући
в. самостално _____
г. у новој породици _____
д. нешто друго _____

27. Тип трговине људима (могуће је заокружити више одговора)
а. сексуална експлоатација
б. радна експлоатација
в. принуда на закључење брака
г. принуда на просјачење
д. принуда на вршење кривичних дела
ђ. трговина органима
е. друго (наведите шта) _____

Контекст регрутације и трафикинга

28. Радни статус када је трафикер ступио у контакт са Вама:
а. запослен/а
б. незапослен/а
в. привремено запослен/а
г. повремено запослен/а
д. пензионер/ка

29. Ако сте били запослени, молимо Вас наведите где сте били у радном односу када је трафикер ступио у контакт са Вама?
_____

30. Оцените Ваш економски статус када је трафикер ступио у контакт са Вама:
а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

31. Место врбовања:
а. на радном месту
б. у сопственој кући
в. у јавном објекту са доступношћу интернета
г. на одмору
д. на другом јавном месту

32. Брачни статус када је трафикер ступио у контакт са Вама:

а. неожењен/неудата
б. ожењен/удата
в. разведен/разведена
г. удовац/удовица
д. у ванбрачној заједници

33. Услови становања када је трафикер ступио у контакт са Вама

а. код родитеља
б. у ученичком / студентском дому
в. у привременом боравишту који ми је обезбедила Влада Србије
г. у изнајмљеном стану
д. у свом стану

34. Начин остваривања првог контакта са трафикером:

а. лично
б. преко познаника
в. путем фиксног телефона
г. путем мобилног телефона
д. путем интернета
ђ. на други начин _____

35. Да ли сте имали приступ информационо–комуникационим технологијама у време врбовања и одакле?

а. да, од куће
б. да, са другог места
в. не

36. Ако јесте, којој сте информационо-комуникационој технологији тада имали приступ?

а. фиксном телефону
б. мобилном телефону
в. интернету

37. Да ли сте тада користили друштвене мреже?

а. да
б. не

38. Ако јесте, заокружите друштвену мрежу на којој сте поседовали налог (могуће је заокружити више одговора):

а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. нисам имао/ла налог ни на једној друштвеној мрежи

39. На који начин је трафикер одржавао контакт са Вама?

а. лично
б. путем фиксног телефона
в. путем мобилног телефона
г. путем интернета
д. преко посредника
ђ. на други начин_____

Мишљење о ризицима и могућности превенције

40. Да ли мислите да сте упознати са ризицима које са собом носи употреба информационо-комуникационих технологија?

а. да
б. не

41. Ако мислите да утиче, опишите на који начин.

42. Ако јесте, опишите те начине.

ПРИЛОГ БР.5
Интервју за азиланте

Основни подаци о интервјуу

Датум интервјуисања _____

Место интервјуисања_____

Подаци о азиланту

1. Пол

а. женски
б. мушки

2. Датум рођења

а. 6 – 14
б. 15 – 16
в. 17 – 18
г. 19 – 33
д. 34 – 49
ђ.50 – 65
е. преко 65

3. Држава рођења _____
4. Место рођења _____
5. Држава у којој је лице живело пре доласка у Србију _____
6. Место боравка_____

7. Тип насеља у коме је лице живело:

а. град
б. село

8. Националност _____
9. Брачно стање _____

а. ожењен/удата
б. неожењен/неудата
в. удовац/удовица

10. Школска спрема:

а. без школе
б. уписана али незавршена / непотпуна основна школа (уписати број завршених разреда)
в. основна школа

г. средња школа
д. виша школа
ђ. висока школа
8. Област образовања:
а. друштвено-хуманистичка
б. медицинско-биолошка
в. природно-математичка
г. техничко-технолошка
д. уметност
ђ. остало _____

11. Садашња економска активност (радно-издржавано становништво):

а. запослен/а
б. незапослен/а
в. бави се пољопривредом (индивидуални пољопривредник)
г. пензионер/ка
д. школује се (уписати да ли је реч о похађању основне, средње школе или факултета)

12. Оцените Ваш садашњи економски статус:

а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

13. Да ли говорите неки страни језик?

а. да, наведите које _____
б. не

14. Жељена држава азила _____

15. Да ли имате родбину или пријатеље у некој европској држави?

а. да (унети назив државе)
б. не

16. Да ли је неко од људи које познајете боравио у Србији?

а. да
б. не

Питања која се односе на коришћење савремених технологија у остваривању процеса миграције-кријумчарења

17. Да ли знате да користите рачунар?

а. да
б. не

18. Да ли имате рачунар? (Напомена: могуће је заокружити више одговора)**:**

а. да, код куће десктоп
б. да, лаптоп/ноутбук
в. не

19. Да ли користите интернет?

а. да
б. не

20. Да ли користите друштвене мреже?

а. да
б. не

21. Ако користите друштвене мреже заокружите друштвену мрежу на којој поседујете налог (Напомена: могуће је заокружити више одговора):

а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. немам налог ни на једној друштвеној мрежи

22. Да ли имате мобилни телефон?

а. да
б. не

23. Колико вам је рачунар/мобилни телефон помогао у доношењу одлуке да мигрирате из земље порекла?

а. није ми помогло
б. веома мало
в. доста ми је помогло

24. Колико вам је рачунар/мобилни телефон помогао у одређивању земље дестинације?

а. није ми помогло
б. веома мало
в. доста ми је помогло

25. Колико вам је рачунар/мобилни телефон помогао у одређивању руте кретања?

а. није ми помогло
б. веома мало
в. доста ми је помогло

26. Колико вам је рачунар/мобилни телефон помогао да самостално, без помоћи других лица пређете до овог места?

а. није ми помогло
б. веома мало
в. доста ми је помогло

27. Колико вам је рачунар/мобилни телефон помогао у контактима са другим мигрантима - кријумчарима?

а. није ми помогло
б. веома мало
в. доста ми је помогло

28. Да ли сте са мигрантима-кријумчарем комуницирали уз помоћ рачунара/ мобилног телефона за време остваривања миграције-кријумчарења и на који начин?

а. да: _____
б. не

29. Да ли бисте успели да дођете у Србију без помоћи рачунара/мобилног телефона?

а. да
б. не
в. можда

30. Да ли бисте другим, потенцијалним мигрантима препоручили да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације?

а. да
б. не
в. можда

Прилог бр. 6
Интервју за мигранте

Основни подаци о интервјуу

Датум интервјуисања _____
Место интервјуисања _____

Подаци о мигранту

1. Пол

а. женски
б. мушки

2. Године старости

а. 6 – 14
б. 15 – 16
в. 17 – 18
г. 19 – 33
д. 34 – 49
ђ. 50 – 65
е. преко 65

3. Држава рођења _____

4. Место рођења _____

5. Националност _____

6. Место боравка

а. урбано подручје
б. рурално подручје

7. Школска спрема:

а. без школе
б. уписана али незавршена основна школа
в. завршена основна школа
г. уписана али незавршена средња школа/гимназија
д. завршена средња школа/гимназија
ђ.уписана али незавршена виша школа
е. завршена виша школа
ж. уписан али незавршен факултет
з. завршен факултет

8. Област образовања:

а. друштвено-хуманистичка
б. медицинско-биолошка
в. природно-математичка
г. техничко-технолошка
д. уметност
ђ. остало _____

9. Садашњи радни статус:

а. запослен/а
б. незапослен/а
в. привремено запослен/а
г. повремено запослен/а
д. пензионер/ка

10. Оцените Ваш садашњи економски статус:

а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

11. Да ли говорите неки страни језик?

а. да, наведите које _____
б. не

Питања која се односе на коришћење савремених технолигија у остваривању процеса миграције – кријумчарења:

12. Да ли знате да користите рачунар?

а. да
б. не

13. Да ли имате рачунар? (напомена: могуће је заокружити више одговора**):**

а. да, код куће десктоп
б. да, лаптоп/ноутбук
в. Не

14. Да ли користите интернет?

а. да
б. не

15. Да ли користите друштвене мреже?

а. да
б. не

16. Ако користите друштвене мреже заокружите друштвену мрежу на којој поседујете налог (могуће је заокружити више одговора):

а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. немам налог ни на једној друштвеној мрежи

17. Да ли имате мобилни телефон?

а. да
б. не

18. Колико вам је рачунар/мобилни телефон помогао у доношењу одлуке да мигрирате из земље порекла?

а. није ми помогло
б. веома мало
в. доста ми је помогло

19. Колико вам је рачунар/мобилни телефон помогао у одређивању земље дестинације?

а. није ми помогло
б. веома мало
в. доста ми је помогло

20. Колико вам је рачунар/мобилни телефон помогао у одређивању руте кретања?

а. није ми помогло
б. веома мало
в. доста ми је помогло

21. Колико вам је рачунар/мобилни телефон помогао да самостално, без помоћи других лица пређете до овог места, како, на који начин?

а. није ми помогло
б. веома мало
в. доста ми је помогло

22. Колико вам је рачунар/мобилни телефон помогао у контактима са другим мигрантима - кријумчарима?

а. није ми помогло
б. веома мало
в. доста ми је помогло

23. Да ли сте са мигрантима - кријумчарем комуницирали уз помоћ рачунара/мобилног телефона за време остваривања миграције – кријумчарења и на који начин?

а. да: _____
б. не

24. Да ли би све ово успели да урадите без помоћи рачунара/мобилног телефона?

а. да
б. не
в. можда

25. Да ли би сте другим, потенцијалним мигрантима препоручили да се самостално, уз помоћ рачунара/мобилног телефона, пребаце из земље порекла у земљу дестинације?

а. да
б. не
в. можда

Прилог бр.7
Интервју за припаднике државног/цивилног сектора у вези са ирегуларним мигрантима

Ирегуларни мигранти

Основни подаци о интервјуу

Датум интервјуисања _____

Место интервјуисања _____

Организација за коју ради:
а. владин сектор
б. невладин сектор

Назив организације за коју ради _____

Опишите природу свог поступања према ирегуларном мигранту:
а. репресивно
б. превентивно
в. хуманитарно
(могуће је заокружити више опција)

Предлог питања која се односе на коришћење савремених технолигија у остваривању процеса миграције - кријумчарења

1. Да ли имате сазнања да ирегуларни мигранти користе интернет у процесу илегалних миграција?
а. да
б. не

2. Да ли имате сазнања да ирегуларни мигранти користите друштвене мреже у процесу илегалних миграција?
а. да
б. Не

3. Ако имате таква сазнања, заокружите друштвене мреже на којима су активни ирегуларни мигранти из ваше праксе? (могуће је заокружити више одговора):
а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare

ђ. друге _____
е. нема налог ни на једној друштвеној мрежи

4. Да ли су ирегуларни мигранти на чијим сте случајевима радили користили рачунар/мобилни телефон током илегалног преласка/боравка?

а. да
б. не

5. Да ли су ирегуларни мигранти на чијим сте случајевима радили користили посебне апликације на рачунарима/мобилним телефонима приликом одређивања руте кретања (GPS)?

а. да
б. не
Ако јесу, које?_____

6. Да ли су ирегуларни мигранти на чијим сте случајевима радили користили рачунаре/мобилне телефоне за контакт са породицом (за обезбеђивање новца за даљи ток кријумчарења)?

а. да
б. не
в. није ми познато

7. Колико је рачунар/мобилни телефон помогао мигранту да самостално, без помоћи других лица пређе до овог места, како, на који начин?

а. није му помогло
б. веома мало
в. доста му је помогло
г. није ми познато

8. Колико је рачунар/мобилни телефон помогао мигранту у контактима са другим мигрантима или са кријумчарима?

а. није му помогло
б. веома мало
в. доста му је помогао
г. није ми познато

9. Да ли сматрате да би ирегуларни мигранти успели да постигну досадашњи ток на путу илегалних миграција без помоћи рачунара/мобилног телефона?

а. да
б. не
в. можда

10. Да ли су вам у досадашњој пракси са ирегуларним мигрантима познати случајеви коришћења мобилних телефона/рачунара на јавним местима, у циљу самосталног организовања и креирања даље руте кретања (интернет-кафе, парк шопинг-центар, трг или друго јавно место)?

а. да
б. не
в. није ми познато

Прилог бр.8
Интервју за припаднике државног сектора/цивилног сектора у вези са кријумчарењем људима

Кријумчари

Интервју за припаднике државног сектора / цивилног сектора

Основни подаци о интервјуу

Датум интервјуисања _____

Место интервјуисања_____

Организација која је извршила интервјуисање:
а. државни сектор
б. цивилни сектор

Назив организације за коју ради: _____

Опишите природу свог поступања према кријумчару мигранта:
а. репресивно
б. превентивно
в. хуманитарно
(могуће је заокружити више опција)

Предлог питања која се односе на коришћење савремених технолигија у остваривању процеса кријумчарења:

1. Да ли имате сазнања да кријумчари користе интернет у процесу кријумчарења мигранта?
   а. да
   б. не

2. Да ли имате сазнања да кријумчари користе друштвене мреже у процесу илегалних миграција?
   а. да
   б. не

3. Ако имате таква сазнања, заокружите друштвене мреже на којима су активни кријумчари из ваше праксе? (могуће је заокружити више одговора)
   а. Facebook
   б. Twitter
   в. LinkedIn
   г. Google+
   д. Foursquare
   ђ. друге _____
   е. нема налог ни на једној друштвеној мрежи

4. Да ли су кријумчари на чијим сте случајевима радили користили рачунар/мобилни телефон током кријумчарења мигранта?
   а. да
   б. не

5. Да ли су кријумчари на чијим сте случајевима радили користили посебне апликације на рачунарима - мобилним телефонима приликом одређивања руте кретања (GPS) у процесу кријумчарења?
   а. да
   б. не
   Ако јесу, које?_____

6. Колико је рачунар/мобилни телефон помогао кријумчару у контакту са другим кријумчарима и у успостављању контаката са илегалним мигрантима?
   а. није му помогло
   б. веома мало
   в. доста му је помогао
   г. није ми познато

7. Да ли сматрате да би кријумчари успели да постигну досадашњи ток кријумчарења мигранта без помоћи рачунара/мобилног телефона?
   а. да
   б. не
   в. можда

8. Да ли су вам у досадашњој пракси са кријумчарима познати случајеви коришћења мобилних телефона/рачунара на јавним местима, у циљу организовања и креирања даље руте кријумчарења илегалних мигранта (интернет-кафе, парк, шопинг-центар, трг или друго јавно место)?
   а. да
   б. не
   в. није ми познато

Прилог бр. 9
Интервју у вези са извршиоцима кривичног дела трговина људима

Основни подаци о интервјуу

Датум интервјуисања_____

Место интервјуисања_____

Која организациона јединица МУП је имала контакт са извршиоцем КД Трговина људима: _____

Подаци о трговцу

1. Пол
а. женски
б. мушки

2. Године старости:
а. 14 – 18
б. 18 – 21
в. 21 – 35
г. 35 – 55
д. 55– 65
ђ. преко 65

3. Држава рођења:
а. СФРЈ
б. СРЈ
в. РС
г. друга _____

4. Место рођења _____

5. Националност _____

6. Место боравка у Србији (за домаће и стране држављане):
а. стварна адреса
б. фиктивна адреса

7. Садашњи брачни статус:
а. неожењен/неудата
б. ожењен/удата

в. разведен/разведена
г. удовац/удовица
д. у ванбрачној заједници

8. Садашњи услови становања
а. код родитеља
б. у ученичком / студентском дому
в. у привременом боравишту који ми је обезбедила Влада Србије
г. у изнајмљеном стану
д. у свом стану

9. Школска спрема:
а. без школе
б. уписана али незавршена основна школа
в. завршена основна школа
г. уписана али незавршена средња школа/гимназија
д. завршена средња школа/гимназија
ђ.уписана али незавршена виша школа
е. завршена виша школа
ж. уписан али незавршен факултет
з. завршен факултет

10. Област образовања:
а. друштвено-хуманистичка
б. медицинско-биолошка
в. природно-математичка
г. техничко-технолошка
д. уметност
ђ. остало _____

11. Садашњи радни статус:
а. запослен/а
б. незапослен/а
в. привремено запослен/а
г. повремено запослен/а
д. пензионер/ка

12. Где је запослен, а за незапослене и пензонере где су били запослени?
_____

13. Садашњи економски статус:
а. веома добар
б. добар
в. осредњи
г. лош
д. веома лош

14. Да ли говори неки страни језик?
а. да, наведите које _____
б. не

15. Да ли зна да користите рачунар?
а. да
б. не

16. Да ли има рачунар? (напомена: могуће је заокружити више одговора):
а. да, код куће десктоп
б. да, лаптоп/ноутбук
в. не

17. Да ли има мобилни телефон?
а. да
б. не

18. Да ли користи интернет?
а. да
б. не

19. Да ли користи друштвене мреже?
а. да
б. не

20. Ако користи друштвене мреже заокружите друштвену мрежу на којој поседује налог (могуће је заокружити више одговора):
а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. нема налог ни на једној друштвеној мрежи

Подаци о криминалној прошлости за трговца

21. Да ли се лице налази у оперативним евиденцијама МУП ?
22. Да ли је лице осуђивано и за која кривична дела?
23. Да ли је лице повратник за кривично дело Трговина људима?
24. Да ли је конкретно кривично дело извршено самостално или у групи?
25. Да ли је лице директан извршилац или подстрекач, помагач или саизвршилац?

Подаци о кривичном делу

26. Време када је ступио у контакт са жртвом
27. Да ли је познавао жртву пре извршења кривичног дела?
28. На који начин је ступио у контакт са жртвом ?
29. На који начин је врбовао/довео у заблуду жртву?
30. На који начин је жртву држао у заблуди?
31. Да ли је ограничавао кретање жртви?
32. Да ли је одузимао лична документа жртви?
33. Да ли је према жртви употребљавао силу или претњу?
34. Да ли је претио члановима породице жртве или њој блиским лицима?
35.Да ли је имао контакте са полицијом или неким другим државним службеницима, којим?
36.Временски период контакта са жртвом

Експлоатација жртве

37. Врста експлоатације
38. Место експлоатације
39. Временски период у ком је вршена експлоатација
40. Прибављена средства (врста, количина)

Коришћење савремених технологија у извршењу кривичног дела

41. Да ли је у време извршења кривичног дела користио информационо-комунакационе технологије?
а. да, од куће
б. да, са другог места
в. не

42. Ако јесте, којој је информационо-комуникационој технологији имао приступ у време извршења кривичног дела?
а. фиксном телефону
б. мобилном телефону
в. интернету

43. Ако је користио савремене информационо-комуникационеј технологије у којој фази кривичног дела их је користио?
а. фаза врбовања
б. фаза транспорта
в. фаза експлоатације
г. више фаза (које)

44. Да ли ли је у време извршења кривичног дела користио друштвене мреже?
а. да
б. не

45. Ако јесте, заокружите друштвену мрежу на којој је поседовао налог (могуће је заокружити више одговора):
а. Facebook
б. Twitter
в. LinkedIn
г. Google+
д. Foursquare
ђ. друге _____
е. нисам имао/ла налог ни на једној друштвеној мрежи

46. На који начин је трговац одржавао контакт са жртвом?
а. лично
б. путем фиксног телефона
в. путем мобилног телефона
г. путем интернета
д. преко посредника
ђ.на други начин_____

47. Да ли су средства савремених технологија пронађена и одузета од трговца?
48. Да ли је вршена експертиза средства савремених комуникација?
49. Да ли се привремено одузета средства савремених комуникација користе као доказ у кривичном поступку?

Прилог бр.10: Интервју за YUTA

1. Да ли је било случајева фалсификованих докумената код путника?
   а. да, било је, колико _____
   б. не

2. Да ли је нека туристичка агенција изгубила лиценцу због везе са трговином људима?
   а. да, која _____
   б. не

3. Да ли је нека туристичка агенција изгубила лиценцу због илегалних миграција?
   а. да, која _____
   б. не

4. Да ли је неко лице запослено у туристичкој агенцији кажњено за трговину људима?
   а. да, колико пута _____
   б. не

5. Да ли је неко лице запослено у туристичкој агенцији кажњено због илегалних миграција?
   а. да, колико пута _____
   б. не

6. Да ли је било случајева да су поједини путници остали ван земље приликом путовања?
   а. да, било је, колико _____
   б. не

7. Да ли је било случајева организовања путовања у иностранство ради тзв. секс туризма?
   а. да, често се организују такви аранжмани
   б. да, било је неколико случајева
   в. не

8. Да ли је било случајева да су организована превоз малолетних лица ради криминалних радњи?
   а. да, било је, колико _____
   б. не

9. Да ли је било случајева путовања у иностранство због нуђења незаконитих медицинских услуга?
   а. да, често се организују такви аранжмани
   б. да, било је неколико случајева
   в. не

Прилог бр. 11: ИСП провајдери

1. Да ли сте учествовали у посебним акцијама из области високотехнолошког криминала?
   а. да, у акцији
   б. не

2. Да ли сте корисницима Ваших услуга блокирали приступ интернет садржајима?
   а. да, којим
   б. не, никада

3. Да ли је било случајева пријаве сајтова због нуђења лажних послова у иностранству?
   а. да
   б. не

4. Ако је било таквих случајева, шта је предузето?

5. Да ли је било случајева пријаве сајтова због посредовања при запошљавању у иностранству?
   а. да
   б. не

6. Ако је било таквих случајева, шта је предузето?

7. Да ли је било случајева пријаве сајтова за услуге посредовања при усвајању деце?
   а. да
   б. не

8. Ако је било таквих случајева, шта је предузето?

9. Да ли је било случајева пријаве сајтова због организовања путовања за секс туризам?
   а. да
   б. не

10. Ако је било таквих случајева, шта је предузето?

11. Да ли је било случајева пријаве сајтова због нуђења сексуалних услуга?
    а. да
    б. не

12. Ако је било таквих случајева, шта је предузето?

13. Да ли је било случајева пријаве сајтова због нуђења незаконитих медицинских услуга?
    а. да
    б. не

14. Ако је било таквих случајева, шта је предузето?

15. Да ли је било случајева пријаве сајтова због трговине органима на интернету?
    а. да
    б. не

16. Ако је било таквих случајева, шта је предузето?

17. Да ли је било случајева пријаве сајтова због трговине органима на интернету?
    а. да
    б. не

18. Ако је било таквих случајева, шта је предузето?

19. Да ли је било случајева пријаве сајтова организованих криминалних група?
    а. да
    б. не

20. Ако је било таквих случајева, шта је предузето?

Прилог бр. 12: Транспортери

1. Да ли је било случајева задржавања путника на граничним прелазима због нерегуларности личних докумената?
   Да, било је, колико _____
   Не

2. Да ли је било случајева фалсификованих докумената код путника?
   Да, било је, колико _____
   Не

3. Да ли је приликом транспорта робе било случајева превоза илегалних мигранта?
   Да, било је, колико _____
   Не

4. Ако је било таквих случајева, да ли је било?
   Смртних исхода, колико_____
   Тежих телесних повреда, колико_____
   Лакших телесних повреда, колико_____

5. Да ли су се приликом транспорта робе превозиле жртве трговине људима?
   Да, било је, колико _____
   Не

6. Ако је било таквих случајева, да ли је било:
   Смртних исхода, колико_____
   Тежих телесних повреда, колико_____
   Лакших телесних повреда, колико_____

7. У случајевима трговине људима, да ли је нека од жртава трговине људима имала средство комуникације (мобилни телефон, рачунар, лаптоп, таблет)
   Да, имала је_____
   Не

Прилог бр.13: Друштво картичара

Друштво картичара

1. Да ли су Ваши корисници пријављивали злоупотребу платних картица?
   а. да
   б. не

2. Ако јесте, каквих?
   а. крађа картица
   б. крађа идентитета у случају остављања података трећим лицима (путем телефона или интернета)
   в. *phishing*-ом
   г. преузимањем података преко лажних сајтова за он-лајн куповину
   д. преузимањем података на сајтовима банака
   ђ. фалсификовањем картица
   е. преко лажних читача на банкоматима и наплатним местима
   ж. друго

3. Да ли је било пријављених случајева упада у систем банака?
   а. да
   б. не

4. Да ли примењујете страндардизоване процедуре информационе безбедности?
   а. да, које
   б. не
   в. не знам

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004(0.034.2)
343.85:343.431(0.034.2)
343.431-058.64(0.034.2)

ВЕЗЕ Cyber криминала са ирегуларном миграцијом и трговином људима [Електронски извор] / [уредник Владимир Урошевић]. - Београд : Министарство унутрашњих послова Републике Србије, 2014 (Београд : Макарије). - 1 електронски оптички диск (CD-ROM) : текст ; 12 cm

Системски захтеви: Нису наведени. - Насл. са насловног екрана. - Тираж 300.

ISBN 978-86-83397-15-0

a) Рачунари - Злоупотреба b) Трговина људима - Сузбијање c) Жртве трговине људима - Међународна заштита
COBISS.SR-ID 209539596

Овај пројекат финансира Европска унија.
Пројекат вредан милион еура ће повећати способност српске полиције да спречава и сузбија ирегуларне миграције, нарочито када су потпомогнуте високотехнолошким криминалом и злоупотребом информационо-комуникационих технологија

Пројекат спроводи Министарство унутрашњих послова Велике Британије у сарадњи са Полицијским президијумом Републике Чешке.
Ставови изнесени у овој публикацији не одражавају нужно ставове Европске комисије.

Пројекат се спроводи у Министарству унутрашњих послова Републике Србије, у Одељењу за борбу против високотехнолошког криминала-СБПОК и Управи граничне полиције (2012-2014)

Научно истраживање спроведено је у сарадњи са:

Факултет организационих наука

Криминалистичко полицијска академија

Центар за заштиту жртава трговине људима

Институт за криминолошка и социолошка истраживања

Институт друштвених наука

Привредна комора Србије