Оригинални научни рад 343.13/.14:004.6
doi:10.5937/zrpfns47-3618

*Милана Писарић, асистент*
*Универзитет у Новом Саду*
*Правни факултет у Новом Саду*

# ПОТРЕБНИ НОРМАТИВНИ ОДГОВОР НА ПРОБЛЕМЕ ОТКРИВАЊА И ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА[1]

***Сажетак:*** Одређени аспекти високотехнолошког криминала, представљају суштину проблема са којима се органи откривања и гоњења кривичних дела која су почињена злоупотребом информационих технологија, сусрећу. Сви ови аспекти чине високотехнолошки криминал специфичним обликом криминала и сви морају бити узети у обзир како би се што потпуније разумеле и превазишле тешкоће у откривању и доказивању кривичних дела и суђењу учиниоцима истих. Имајући у виду све наведено, а да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских мрежа и система, разумљиво је настојање држава да прилагоде, односно употпуне постојеће кривичне законе новим одредбама. За стварање одговарајућег правног оквира за супротсављање овој врсти криминала путем кривичног права, потребно је у прописима кривичног материјалног права инкриминисати одређена понашања, односно предвидети кривична дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система, а у прописима кривичног процесног права утврдити одговарајућа овлашћења надлежних органа у циљу откривања извора недозвољене радње, односно прикупљања података о учињеном кривичном делу и учиниоцу који могу бити искоришћени као доказ у кривичном поступку.

***Кључне речи:*** високотехнолошки криминал, нормативни одговор, откривање, доказивање.

---

[1] Овај рад је настао као резултат научно-истраживачког рада на Пројекту „Теоријски и практични проблеми стварања и примене права (ЕУ и Србија)“ чији носилац је Правни факултет у Новом Саду.

## 1. Уводна разматрања

Поједина кривична дела почињена злоупотребом достигнућа информационе и комуникационе технологије донекле су слична условно речено традиционалним кривичним делима – примера ради, крађа, превара, вандализам, неовлашћен приступ приватној сфери појединца, дечја порнографија и кршење ауторских права су проблеми који су постојали и пре појаве рачунара и Интернета. Стога постојећи прописи могу представљати солидну основу за откривање и хватање појединаца и криминалних група који су починили кривична дела коришћењем рачунара и Интернета. Проблеми у вези са откривањем кривичних дела и гоњењем учинилаца настају не толико услед природе недозвољених активности, већ управо због природе информационих технологија. Наиме, глобална мрежа повезаних рачунара и рачунарских система, која обухвата целу земаљску куглу, омогућава појединцима у једној држави да предузму одређене штетне радње у било којој другој држави, докле год постоји рачунар и Интернет конекција на оба места. Огроман домет и готово потпуна анонимност корисника на Интернету отежава задатак органа гоњења да уђу у траг учиниоцима и открију извор криминалне активности, а у случају да то успеју, границе територијалне надлежности могу да их спрече у изношењу оптужбе пред суд.

Одређени аспекти високотехнолошког криминала, представљају суштину проблема са којима се органи откривања и гоњења кривичних дела која су почињена злоупотребом информационих технологија, сусрећу. Пре свега, ради се о релативно новој појави о чијим специфичностима надлежни органи гоњења и суђења нису у довољној мери упознати. Са друге стране, начини и средства која се користе у извршењу кривичних дела се мењају, односно усавршавају са развојем информационе технологије, чиме неминовно долази до повећања разлике између знања извршилаца дела и (не)знања овлашћењних службених лица орагана гоњења, из ког разлога је неопходна специјализација надлежних органа како би супротстављање високотехнолошком криминалу уопште било могуће. Друго, дефиниције ове врсте криминала нису јасно нити униформно одређене и чак постоје недоследности и значајне разлике у кривичним законима појединих држава. Како је транснационална димензија високотехнолошког криминала такође релевантна, потребно је усклађивање дефиниција у прописима држава, јер уколико не постоји правна компатибилност у конкретном случају, истрага и гоњење могу неминовно бити отежани. Треће, за дела високотехнолошког криминала карактерична је просторна удаљеност између учиниоца и оштећеног, при чиму се под местом извршења кривичног дела може сматрати неколико

локација које се чак могу налазити на територији неколико држава. Четврто, вероватноћа пријављивања и откривања кривичног дела су далеко мање него у случају традиционалних кривичних дела. Пето, с обзиром на природу електронских доказа и брзину којом се радња може предузети, а трагови у електронском облику изменити, сакрити или уништити, постојеће радње и мере надлежних органа не представљају основ за делотворно деловање органа откривања и гоњења кривичних дела[2].

Сви ови аспекти чине високотехнолошки криминал специфичним обликом криминала и сви морају бити узети у обзир како би се што потпуније разумеле и превазишле тешкоће у откривању и доказивању кривичних дела и суђењу учиниоцима истих. Имајући у виду све наведено, а да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских мрежа и система, разумљиво је настојање држава да прилагоде, односно употпуне постојеће кривичне законе новим одредбама.

## 2. Потреба прилагођавања кривичне процедуре специфичностима високотехнолошког криминала

За стварање одговарајућег правног оквира за супротављање овој врсти криминала путем кривичног права, осим што се у прописима кривичног материјалног права одређена понашања инкриминишу, те предвиђају као кривична дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система, неопходно је да прописи кривичног процесног права садрже одговарајућа овлашћења надлежних органа у циљу откривања извора недозвољене радње, односно прикупљања података о учињеном кривичном делу и учиниоцу који ће бити искоришћени као доказ у кривичном поступку, а водећи рачуна о специфичностима високотехнолошког криминала и окружења у оквиру ког се недозвољене активности предузимају. При томе, одређене карактеристике савремених рачунарских система и мрежа представљају озбиљну препреку за обезбеђивање доказа потребних за оптужење и вођење кривичног поступка за дела високотехнолошког криминала[3]. На структурном нивоу, с обзиром на то да се ради о својеврсној рачунарској мрежи на глобалном нивоу, сама конфигурација Интернета превазилази границе држава, док према традиционалним принципима међународног јавног права државе имају надлежност само у оквиру својих суверених граница, па је самим тим и место предузимања радњи и мера надлежних органа у откривању, гоњењу и вођењу кри-

[2] F. Cassim, „Formulating specialized legislation to address the growing spectre of cybercrime: a comparative study“, *Potchefstroom electronic law journal*, 12/2009, 55.

[3] B. Maier, „How Has the Law Attempted to Tackle the Borderless Nature of the Internet?“, *International Journal of Law and Information Technology* 2/2010, 153.

вичног поступка за дела високотехнолошког криминала ограничено на територију државе. На техничком нивоу, операције у оквиру рачунарских система и мрежа карактерише одређена непостојаност и брз проток података који могу бити измењени, премештени, прикривени или избрисани за неколико секунди, што у принципу, значи да спровођење радњи и мера ради проналажења и обезбеђења доказа криминалних активности може бити, најблаже речено, отежано.

Што се тиче проблема непостојаности података на Интернету, могуће решење јесте предвиђање обавеза пружаоцима интернет услуга и других телекомуникационих услуга да за одређени временски период задржавају све одређене податке и да их на захтев надлежних органа учине доступним за потребе вођења кривичног поступка. Прописи би требало да садрже овлашћења органа гоњења у циљу откривања извора недозвољене радње, те идентификовање починиоца кривичног дела, односно да би се омогућило прикупљање података о учињеном кривичном делу и учиниоцу који ће бити искоришћени као доказ у кривичном поступку[4]. У том смислу, поставља се питање да ли је регулиаања тих овлашћења приступити реактивно или проактивно. Осим тога поставља се питање у односу на која кривична дела се специфична овлашћења у вези са предузимањем посебних доказних радњи предузимају: да ли у односу на кривична дела која су у кривичним законима одређена као дела против рачунарских система, дела чије радње су предузете злоупотребом рачунара или у сваком конкретном случају када је потребно обезбедити доказ у електронском облику без обзира о ком кривичном делу се ради. Другим речима, потребно је поћи од основне премисе да подаци у дигиталном облику имају вредност у кривичном поступку и доказну снагу која је идентична снази материјалних доказа који постоје у физичком свету.

Сходно томе, одредбама кривичног процесног права би требало омогућити да се ове две тешкоће превазиђу на одговарајући начин и у складу са принципа и интересима кривичне процедуре. Бројни и разноврсни су изазови у откривању и доказивању дела високотехнолошког криминала које треба превазићи одговарајућим одредбама кривичног процесног права, а односе се на превазилажење ограничења у ситуацији када више држава има надлежност над гоњењем, задржавање и очување података који могу бити употребљени као доказ, давање одговарајућих овлашћења надлежним органима, проналажење одговарајућег механизма за пријављивање кривичних дела, координирање радом и размену информација и података између надлежних органа, декодирање енкрипције и утврђивање идентите-

[4] I. Brown, „Communications Data Retention in an Evolving Internet“, *International Journal of Law and Information Technology* 2/2010, 100.

та учиниоца, одговорајућа обука запослених у органима гоњења и суђења на свим нивоима и слично.

Међутим, приликом одређивања сврхе и околности под којима се процесна овлашћења могу применити, неопходно је водити рачуна о правним принципима домаћег кривичне процедуре. Кривично процесно право представља неопходну спону између кривичног дела и изрицања одређене кривичне санкције од стране суда, те у том смислу прописује одређена овлашћења надлежним органима ради остварења кривичноправног захтева а у исто време треба да спречи примену кривичног закона према лицима за које се утврди да нису учинили претпостављено кривично дело, а уз очување претпоставке невиности[5]. Из тог разлога приликом прописивања овлашћења надлежним органима у вези са кривичним поступком постоје одређена ограничења, чији је смисао спречавање самовоље у поступању од стране тих органа. Како би се постигла неопходна равнотежа између интереса кривичног поступка и интереса (и права) оптуженог и других лица у поступку, релевантна су не само ограничавање обима у прописивању овлашћења него и начин остваривања тих овлашћења, те врста радњи које су органи овлашћени да предузму.

## 3. Транснационална природа и надлежност за откривање и доказивање дела високотехнолошког криминала

Веома важна, али изузетно сложена питања у вези са процесурирањем дела високотехнолошког криминала односе се одређивање принципа надлежности који ће се примењивати у конкретном случају. Приступ који је у теорији најзаступљенији јесте залагање за стварањем посебних принципа за одређивање надлежности с обзиром на то да је виртуелни, кибер простор специфичан и у потпуности одвојен од реалног простора, у ком корисници рачунара и рачунарских мрежа комуницирају електронски и преко граница надлежности држава[6]. Надлежност у кибер простору можемо одредити као право одређене државе и државних органа да уређују односе у електронском окружењу и примењују правне норме у односу на правне субјекте на њеној територији а што произилази из суверенитета државе. У погледу кривичног материјалног и процесног права важи прицип да судови примењују само норме ове две гране права које је прописала национална држава али не и норме страног права (осим у случају одређених облика међународне правне помоћи, односно на основу ратификације одређених међународних уговора).

[5] S. Brenner, „Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law“, *Murdoch University Electronic Journal of Law* 2/2001, 40.

[6] S. Brenner, B. Koops, „Approaches to cybercrime jurisdiction“, *Journal of High Technology Law* 1/2004, 36.

Ако се у обзир узме могући транснационални карактер високотехнолошког криминала, поставља се питање да ли примена традиционалних принципа, који почивају на заштити интереса државе (територијални, заштитни, ограничени персонални принцип), односно на солидарности међународне заједнице (неограничени персонални, универзални принцип), може довести до сукоба надлежности када се више држава сматра надлежном? У том смислу требало би имати у виду одредбу члана 22. Конвенције о компјутерском криминалитету, која полазећи од територијалног и персоналног принципа предвиђа консултације између држава чланица за постизање споразума о одговарајућој надлежности у конкретном случају а ради превазилажења проблема сукоба надлежности у вези са кривичним поступком и поштовањем принципа *ne bis in idem* установљеним међународним правним документима. С обзиром на препреку транснационалне природе Интернета, могуће решење би се састојало у формирању међународне полицијске односно тужилачке организације или давање националним судовима универзалне надлежности, на који начин би се сва ограничења територијалне надлежности државих органа превазишле и била би омогућена ефикасна борба против овог облика прекограничног криминала. Међутим, овакав радикалан приступ није прихваћен јер већина држава не жели да се одрекне свог суверенитета и прихвати да надлежни органи друге државе предузимају одређене истражне радње на њиховој територији[7]. Како, дакле, надлежни органи предузимају радње само у оквиру територије државе, неопходно је користити одговарајуће механизме међународне правне помоћи у кривичним стварима. Међутим, постојећи механизми су у недовољној мери ефикасни, с обзиром да су процедуре пружања помоћи и сарадње, уопште, дуготрајни, а ради обезбеђења доказа за оптужење учинилаца у кибер простору неопходно је хитно реаговање, па би требало предвидети могућност екстериторијалног деловања надлежних органа у одређеним случајевима под одређеним условима. У складу са принципом територијалног суверенитета једне државе, физичко присуство и активности органа једне државе на територији друге државе, а без претходне сагласности те државе представљају повреду територијалног суверенитета. С тим у вези је и дилема да ли је и под којим условима могуће да органи једне државе применом техничких средстава предузимају радње и мере у циљу прикупљања података за потребе кривичног поступка за дела високотехнолошког криминала, односно да ли приступ рачунару и рачунарским системима који се налазе на територији друге државе а коришћењем међународне комуникационе инфраструктуре, какав је Интернет, представља кршење принципа територијалног суверенитета или превазилажењу овог проблема треба присту-

[7] M. Goodman, S.Brenner, „The emerging Consensus in on Criminal Conduct in Cyberspace“, *International Journal of Law and Information Technology* 2/2002, 178.

пити прагматично прописивањем могућности екстериторијалног деловања државних органа под одређеним условима. Правила међународног јавног права налажу да се у таквим случајевима користе механизми пружања међународне правне помоћи у кривичним стварима (мултилатерални или билатерални уговор[8]), међутим, с обзиром на неефикасност таквих механизама, с једне стране, и природу података који се обрађују, складиште и преносе путем Интернета, с друге стране, било би оправдано, чак и уколико не постоји међународни уговор који би омогућио међународну сарадњу у предузимању радњи прикупљања доказа, надлежним органима дати овлашћење да под одређеним условима и у одређеним случајевима приступе и претраже рачунарске системе и мреже која се налази на територији друге државе, односно да предузимају одређене радње и мере ради прикупљања података за потребе кривичног поступка за дела високотехнолошког криминала чак и ван граница њихове територије.

Поједини правни системи имају различите приступе регулисању одговора државе на претњу високотехнолошког криминала и не постоји јединствен став о томе које се то неовлашћене активности злоупотребом информационих технологија сврставају под овим појмом[9]. У том смислу од изузетног значаја је концензус постигунт у оквиру Савета Европе у виду Конвенције о високотехнолошком криминалу[10]. Ратификовањем или приступањем Конвенцији, држава се обавезује да имплементацијом одредаба материјалне и процесне природе обезбеди да у домаћем законодавству предвиди као кривична дела одређена понашања, те да пропише одређена овлашћења надлежним органима неопходна за истрагу и кривично гоњење таквих кривичних дела[11]. Конвенција представља свеобухватан оквир за

---

[8] На међународном нивоу постоје два правна инструмента која пружају солидну основу за суштинску прекограничну сарадњу у супротстављању сајбер криминалу. Први од ових инструмената, Конвенција Савета Европе о високотехнолошком криминалу иако усвојена као регионални механизам има глобални значај, а друга је Конвенција Уједињених нација против транснационалног организованог криминала, која од индиректног значаја за борбу против високотехнолошког криминала када је исти резултат деловања криминалних група у прекограничним оквирима.

[9] N. Foggetti, „Transnational Cyber crime, differences between national laws and developments of European legislation: by repression?“, *Masaryk University journal of Law and technology* 2/2008, 37.

[10] *Convention on Cybercrime,* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[11] Што се тиче структуре, Конвенција садржи четири поглавља. У *првом поглављу* дефинисани су основни појмови (рачунарски систем, рачунарски подаци, провајдери услуга, проток података). *Друго поглавље* садржи законодавне мере које треба предузети на националном нивоу, а односе се на кривично материјално право и кривично процесно право. У оквиру одељка 1. Конвенције кривична дела су сврстана у четири групе: прву групу чине кривична дела усмерена против поверљивости, интегритета и доступности података и информационих

прилагођавање кривичног материјалног и процесног законодавства и одредаба за међународну сарадњу у борби против компјутерског криминала, а с обзиром на неадекватност традиционалних истражних овлашћења и одсуство у већини земаља посебних процедуралних правила која се примењују у кибер простору, Конвенција има за циљ да се у домаћем кривичном процесном праву обезбеде овлашћења надлежним органима која су неопходна за истрагу кривичних дела учињених у вези са рачунарским системима као и других кривичних дела за гоњење којих је неопходно прикупити податке у електронском облику[12]. Ова овлашћења, од којих су нека посебно иновативна, одговарају различитим циљевима, као што су прикупљање доказа, лоцирање извора и идентификовање учинилаца кривичних дела али сва имају за циљ да се прикупе подаци за потребе конкретне кривичне ствари и нису проактивне у погледу свог ефекта или обима и не служе стварању „орвелијанског" система електронског надзора у телекомуникационом окружењу. Конвенција предвиђа могућност да се подаци прикупљају, те обавезује оне који поседују релевантне податке да их учине доступним, односно да их сачувају за потребе вођења истраге, али не садржи захтев нити оправдава свеобухватни и неселективни надзор комуникација појединаца од стране пружалаца телекомуникационих услуга нити полиције, осим ако се предузимају радње ради откривања конкретног кривичног дела и учиниоца. Осим тога, предвиђена су значајне процедуралне гаранције, што представља један од главних доприноса Конвенције[13].

---

система; другу групу чине кривична дела у вези са рачунарима (*computer-related crimes*) у извршењу којих се рачунар појављује као средство; трећу групу чине кривична дела у вези са садржајем; четврту групу чине повреде ауторских и сродних права. У вези са овим кривичним делима, Конвенција пред потписнице поставља захтев за увођењем истражних овлашћења, а ради модернизације алата који стоје на располагању органима истраге и гоњења у вези са са компјутерским криминалом. Наиме, у оквиру одељка 2. (чланови 14-21.) су одредбе које се односе на процесно право, а садрже одређене смернице за поступак, који се води у вези са кривичним делом које извршено путем рачунарских система, као и смернице за прикупљање доказа у електронском облику о извршеном кривичном делу (па и о кривичном делу које не спада у компјутерски криминал у смислу Конвенције). Успостављање, спровођење и примена овлашћења и поступака наведених у делу који се односи на процесно право захтева од државе да обезбеди адекватну заштиту људских права и слобода – првентсвено права на приватност. При том треба да се поштују уобичајени стандарди, тј. минималне мере заштите, укључујући међународне инструменте о људским правима. *Треће поглавље* тиче се међународне сарадње и садржи принципе који се односе на надлежност, екстрадицију, основне принципе међународне помоћи- процедуре које се односе на међусобне захтеве за помоћ у недостатку важећих међународних споразума, узајамну помоћ у вези са привременим мерама, те узајамну помоћ у вези истрагом. *Четврто поглавље* садржи завршне одредбе.

[12] M. Gercke, „Europe's legal approaches to cybercrime", *ERA forum* No. 10/2009, 58.

[13] Miquelon-Weismann, M., "The convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process?" *John Marshall Journal of Computer & Information Law* 2/2005, 333.

## 4. Мере и радње за откривање и доказивање дела високотехнолошког криминала

Подаци који се складиште, обрађују и преносе у рачунарским мрежама и системима су непостојани и подложни изменама, а како би се створио основ да се захтева очување ових података, сматрамо да је у национално законодавство потребно увести **хитно очување ускладиштених рачунарских података** као нову доказну радњу, која би могла бити од пресудног значаја за успех кривичних истрага у рачунарским мрежама. Смисао ове радње је својеврсно "замрзавање података" у циљу да се спречи губитак или измена постојећих података који би могли бити од вредности као доказ у кривичном поступку, а коју по налогу надлежних органа извршавали пружаоци телекомуникационих услуга. Ова радња би се предузимала да би се одређени подаци очували а њихов интегритет одржао, без обзира да ли се ради о подацима о саобраћају или о садржају комуникације, уколико би постојала опасност од губитка или измене. Спровођење мере би основ имало у наредби за хитно очување података која би се издавала пружаоцима услуга електронских комуникација са захтевом да сачувају податке на одређени временски период и при томе би се радило се о тајној мери. Како би у погледу чувања и откривања података о саобраћају могли настати одређени проблеми из чињенице да су више провајдера укључени у пренос комуникације, добро решење је предвидети могућност да се захтева хитно очување података у читавом ланцу комуникације у смислу одређивања извора и одредишта, без обзира на број оператера који су укључени у пренос комуникације. При томе би било могуће захтев упутити само пружаоцима у оквиру територијалних граница једне државе, а ако би се порука преносила посредством провајдера из стране земље, неопходно би било покретање одговарајућих механизама за пружање узајамне правне помоћи.

У ситуацији када је потребно рачунар ком се приступило прегледати, односно остварити увид у то који се подаци у њему налазе, поставља се питање да ли је могуће аналогно применити правила која уређују традиционалне мере процесне принуде према стварима у форми претреса и привременог одузимања физичких предмета. Полазећи од претпоставке да је неопходно посебно регулисати предузимање радње **претраге рачунара, рачунарског система и мрежа** и прикупљање података који се у њима створени, обрађени и преношени, пажњу је потребно посветити начину уређења следећих питања: јасном утврђивању разлике између претраге аутоматски обрађених података и прикупљања аутоматски преношених података и података које је корисник створио; обавези обавештавања лица које је држалац рачунара о томе да је систем био предмет претраге и који подаци су прибављени у одговарајућем моменту; обиму и условима за

претрагу рачунарског система који је са рачунаром који је предмет претраге повезан преко рачунарске мреже. Да би се прегледао рачунарски систем, те да би се утврдило присуство података неопходних за кривичну истрагу, неопходно је утврдити ко је, под којим условима и по ком основу овлашћен да приступи рачунарском систему, те да ли могућ приступ у одређеним хитним случајевима мимо утврђених правила[14]. Осим што су надлежни органи овлашћени да претраже, односно на одговарајући начин приступе рачунарском систему, односно делу рачунарског система као и уређајима за складиштење података који се налазе на територији државе, уколико је вероватно да се подаци складиштени у другом рачунарском систему или делу система, а који се налазе на територији државе и могуће им је приступити, односно који су доступни преко рачунарског система који се предмет претраге, требало би дати овлашћење надлежним органима да у одређеним случајевима иницијалну претрагу прошире и на тај други рачунарски систем.

Дилема постоји и у погледу могућности проширења претраге на рачунарски систем који се налази на територији друге државе а ком је преко претраживаног рачунарског система могуће приступити путем Интернета или друге рачунарске мреже или тзв. прекограничну претрагу рачунарског система треба разматрати у вези са пружањем узајамне правне помоћи у кривичним стварима. Потреба регулисања приступа рачунару, рачунарским системима и рачунарским мрежама и у рачунарском систему у другој држави и претраживања података који су ускладиштени, обрађују се или преносе у њима произилази из чињенице да је у Интернет окружењу, услед природе ове глобалне рачунарске мреже и повезаности рачунарских система који се налазе у различитим државама, могућа ситуације да надлежни органи једне државе, предузимајући одређене истражне радње не буду свесни да су претрагом обухваћени подаци у оквиру рачунарских система који се налазе у другим државама, чиме може доћи до повреде територијалног суверенитета држава уколико би претраге биле предузете без претходног обавештења, односно сагласности друге државе. Из тог разлога неопходно је да постоје експлицитна међународноправна правила која уређују могућност **прекограничног приступа и претраге рачунарских система и мрежа**, односно споразуми који дефинишу услове под којима се претрага може вршити уместо праксе по принципу *laisee faire*. Из тога разлога неопходно је одговарајућим одредбама регулисати следећа питања је 1) под којим условима и у којој процедури државе једна другој могу дозволити спровођење прекограничног мрежног претраживања (претражива-

[14] S. Trepel, "Digital Searches, General Warrants, And The Case For The Courts," *Yale Journal of Law and Technology* 10/2008, 138.

ње рачунарске мреже) а уз поштовање права осумњиченог као и права и интересе трећих лица; 2) у случају да се надлежним органима стране државе прекогранично мрежно претраживање не дозволи, да ли би било могуће на одређени начин обезбедити податке који се обрађују, складиште и преносе у оквиру рачунарске мреже или система на територији те државе и у каквој процедури (уз указивање на потребу стварања експедитивних процедура за задржавање података како би се спречио њихов губитак или измена пре окончања редовне процедуре слања и поступања по замолницама); 3) да ли је оправдано инсистирати на редовним механизмима за пружање правне помоћи у кривичним стварима, а који су дуготрајни, док је природа података који могу бити електронски докази таква да се они лако и брзе мењају, односно прикривају и губе. Како би се ограничења постојећих механизама превазишле, са нарочитом пажњом би требало сагледати механизама који су неопходни за убразавање прекограничне сарадње надлежних органа у откривању, истраживању и гоњењу односно супротстављању криминалу коју почива на злоупотреби дигиталне технологије и рачунарских система.

С обзиром на то да су за кривични поступак од значаја не само подаци који су ускладиштени у једном рачунарском систему, него и подаци који се генеришу у реалном времену док сигнал кроз рачунарску мрежу пролази од извора до одредишта комуникације, корисно је предвидети могућност **пресретања телекомуникација** и за рачунарске комуникације. Међутим, како је дошло до конвергенције информационих и телекомуникационих технологија, поставља се питање да ли се постојећа овлашћења техничког надзора комуникација могу еквивалентно применити на случај пресретања различитих облика техничких комуникација као што су комуникације између рачунара[15]. У погледу прикупљања података који нису ускладишени у једном рачунарском систему него података који се генеришу у реалном времену док сигнал кроз рачунарску мрежу пролази од извора до одредишта комуникације, оправдано је разликовати прикупљање у реалном времену података о комуникационом саобраћају и пресретање у реалном времену података о садржају комуникација. Надлежним органима треба дати овлашћење да прикупљају или снимају применом техничких средстава на својој територији, односно да наређе пружаоцима телекомуникационих услуга да у оквиру својих техничких могућности прикупљају податке. Међутим, како би пресретање података о садржају комуникација предствљало радњу којом би се у највећој мери задирало у приватност, пи-

[15] W. Murdoch, "Regulation of State Surveillance of the Internet human rights infringement or e-security mechanism?", *International Journal of Electronic Security and Digital Forensics,* 1/ 2007, 44.

тање је да ли је оправдано предвидети могућност одређивања те радње за сва кривична дела или само уз поштовање принципа пропорционалности, односно само за истраживање тежих кривичних дела. Такође, код пресретања података о садржају комуникација потребно је да државе пропишу да се мера примењује у односу на одређену комуникацију која се на територији те државе обавља путем рачунарског система, а не обавезати пружаоце електронских услуга да задржавају неселективно податке о свим комуникацијама за одређени временкси период. Што се правног уређења пресретања комуникација тиче, неопходно је у прописима на одговарајући начин превазићи неколико дилема: да ли је оправдано евентуално проширење обима техничког надзора у случајевима истраге тешких кривичних дела против поверљивости, интегритета и доступности телекомуникационих или рачунарских система и на пресретање података о садржају комуникације с обзиром на начело пропорционалности[16]; да ли је потребно одредити различите услове за предузимање ове радње у зависности од врсте комуникације (комуникација између рачунара или између појединаца и рачунара) и природе мреже (јавна или приватна) у погледу којих се пресретање одређује; које су то техничке мере које истражни органи морају да користе како би прикупљени подаци били обезбеђени на одговарајући начин; како поставити услове и одредити гаранције о којим треба водити рачуна приликом пресретања како би се постигла одговарајућа равнотежа између права појединаца на приватност и интереса кривичног поступка?

У вези са остваривањем поменутих овлашћења надлежних органа, потребно је **обавезати одређене субјекте на сарадњу**. Најпре се поставља питање, на који начин обавезати лица која имају приступ односно контролу над рачунаром или рачунарским системом у којима су ускладиштени, обрађени или се преносе подаци који могу бити искоришћени као доказ у кривичном поступку да надлежним органима омогуће приступ, односно претраживање тог рачунара, система или мреже? Како обавезу предаје одређених предмета, а која је предвиђена традиционалним правилима кривичне процедуре прилагодити виртуелном окружењу и нематеријалној природи електронских доказа (примера ради, обавезивањем да се штампају подаци или да буду представљени увидљивој и разумљивој форми у случају да су подацинекриптовани, откривањем лозинке и слично). Осим тога, са циљем стварања механизма који омогућава да се упути захтев садржан у формалном налогу полиције или суда да се одређени подаци предају надлежним органима, потребно је предвидети издавање својеврсне наредбе за предавање података, као правног основа за омогућавање при-

[16] J. Cannatacia, J. Mifsud, „The end of the purpose-specification principle in data protection?“, *International Review of Law, Computers & Technology* 1/ 2010, 108.

ступа подацима ускладиштеним у рачунарском систему или уређају за складиштење података. Поставља се питање који орган је надлежан за доношење такве наредбе и који се сви подаци могу тражити, нарочито у вези са поштовањем права појединца на неповредивост комуникација, односно интереса заштите пословне тајне. У вези са обавезом држаоца рачунара, односно рачунарског система, поставља се и питање да ли је оправдано обавезати лице које поседује знања о функционисању система који се претражује да са надлежним органима сарађује пружајући им неопходне информације нарочито ако се ради о осумњиченом лицу а имајући у виду привилегију од самооптуживања или се пак та обавеза може односити само на администраторе система и друга техничка лица. Исто тако, специфичне обавезе могу бити наметнуте операторима јавних и приватних мрежа да употребе сва неопходне техничке мере те омогуће пресретање телекомуникација од стране истражних органа, односно пружаоцима телекомуникационих услуга доступних јавности да по наредби истражних органа учине доступним податке потребне ради идентификовања корисника услуге а у погледу којих пружалац има приступ, односно контролу. С последњим у вези се поставља питање, који су то подаци? Неопходно и оправдано је направити разлику између идентификационих података, других података и осетљивих података. Стога нарочиту пажњу треба посветити правилима чија је сврха заштита података о личности, те стандардизовати процедуре и тражити од оператера да податке учине доступним на основу стандардних писаних наредби, те избегавати неформално и усмено прикупљање како би се подаци могли користити као доказ. Како се не би компромитовала истрага, исти се могу обавезати да као тајну чувају чињеницу да извршавају те радње по налогу надлежних орагана као и све информације у вези са тим. Такође, битно је предвидети право лица на које се радња односи да у одговарајућем тренутку буде обавештено у које сврхе и по ком правном основу су се подаци прикупљали.

Неспорно је, дакле, да је постоји потреба за предвиђањем могућности да се применом одређених техничких средстава подаци у рачунарским системима прикупљају, обрађују и користе, те обавезивањем одређених субјеката који поседују релевантне податке да их учине доступним, односно да их сачувају ради откривања кривичног дела и учиниоца за потребе вођења кривичног поступка, али свеобухватан и неселективни надзор комуникација појединаца од стране пружалаца телекомуникационих услуга или полиције није оправдан, већ је неопходно предвидети одређена **процедурална ограничења и гаранције**, односно одговарајућим прописима постићи праведни баланс између потреба вођења кривичног поступка и поштовања људских права, односно овлашћења истражних органа у циљу прикупљања података и обима заштите права на

приватност појединаца. Да би се спречило арбитрерно поступање надлежних државних органа, у складу са принципом владавине права, приликом законског регулисања, односно одређивања и извршења одређених процесних радњи у циљу откривања и обезбеђивања електронских доказа о учињеном кривичном делу и учиниоцу, потребно је водити рачуна о одређеним ограничењима у виду минималних услова и гаранција које је потребно узети у обзир како би се обезбедила адекватна заштита одређених људских права и слобода. С обзиром на „захват" одређене радње, односно опасност од угрожавања права појединаца који су погођени одређивањем радње, минималне мере заштите могу се односити на судску контролу или надзор другог независног органа, законско одређивање разлога који оправдавају примену радње, те ограничења у обиму и трајању примене радње. При томе, не треба занемарити утицај процесних овлашћења, те права, одговорности и легитимне интересе трећих лица према којима радња није одређена а који су учесници у одређеном комуникационом односу. У вези са постизањем поменуте равнотеже је и питање које су то податке пружаоци Интернет и других телекомуникационих услуга дужни да чувају и у ком временском периоду а које да на захтев истражних органа чине доступним за потребе вођења кривичног поступка, с обзиром на то да, с једне стране, задржавање података о мрежном саобраћају може бити од изузетног значаја у откривању високотехнолошког криминала док, с друге стране, задржавање на неодређени или дуг временски период може донети несразмерне трошкове, а превелика истражна овлашћења могу бити у сукобу са прописима који гарантују права на приватност, односно уређују заштиту података о личности, из ког разлога приликом прописивања радњи и мера за обезбеђење доказа те при одређивању, односно примени тих мера и радњи потребно водити рачуна о одређеним принципима (законитост, неопходност, пропорционалност, транспарентност)[17].

Евидентан је недостатак правних стандарда у вези са доказним правилима о електронским записима као траговима извршења кривичног дела ради могућности њиховог коришћења у кривичном поступку, посебну пажњу је потребно посветити **електронским доказима**. При томе требало би узети у обзир законска решења у појединим државама и примере добре праке у погледу тога како да се прикупљају и сачувају електронски записи на начин којим ће се најбоље обезбедити интегритет, аутентичност и прихватљивост тих записа као доказа у кривичном поступку пред судом државе. Такође, требало би водити рачуна и о основним принципима на којима

[17] L. Costa, „Privacy and the precautionary principle", *Computer Law and security Review* 28/2012, 18.

почива дигитална форензика као део криминалистике[18], која користи научно изведене и доказане методе за идентификацију, сакупљање, документовање, чување, руковање, вредновање, анализу и интерпретацију електронских трагова[19].

## 5. Закључак

Како у великом броју држава нису предвиђене адекватне радње и мере ради откривања и обезбеђења доказа за потребе вођења кривичног поступка за дела високотехнолошког криминала, постоји потреба да се одговарајућим прописима у националним законодавствима надлежним органима дају овлашћења која су неопходна за истрагу и гоњење кривичних дела учињених у вези са рачунарским системима као и других кривичних дела за гоњење којих је неопходно прикупити податке у електронском облику. Ова овлашћења би требало да одговарају различитим циљевима, као што су прикупљање доказа, лоцирање извора и идентификовање починиоца кривичног дела. У том смислу, поставља се питање, да ли правном регулисању тих овлашћења приступити реактивно или проактивно. Такође, неопходно је одредити у односу на која кривична дела се специфична овлашћења предузимају: да ли у односу на кривична дела која су у кривичним законима одређена као дела против рачунарских система, дела чије радње су предузете злоупотребом рачунара или у случају да је потребно обезбедити доказ у елекетронском облику без обзира о ком кривичном делу се ради. Незанемарљивом броју држава као узор у стварању правног оквира за супротстављање високотехнолошком криминалу послужила су решења садржана у Конвенцији Савета Европе. Међутим, не умањујући битан допринос Конвенције а имајући у виду да је тренутно технолошко окружење далеко од тога да је идентично стању од пре више од десет година, процесноправне одредбе која се заснивају на решењима из поменуте Конвенције су неприхватљива и застарела и не могу дати одговарајуће резултате у откривању и обезбеђењу доказа за потребе вођења кривичног поступка за дела високотехнолошког криминала. Данас је у далеко већој мери комликовано ући у траг извршиоцу, открити криминалне активности на Итернету и обезбедити електронске доказе него 2001.године, јер процес својеврсне "дигиталне глобализације" наставља да се убрзава, а постављени оквир је више реактиван него проактиван, а није ни технички неутралан. Примера

[18] Leigland R., Krings A., "A formalization of digital forensic", *International Journal of Digital Evidence* 2/2004, 28.

[19] Више видети: Т.Лукић, „Дигитални докази", *Зборник радова Правног факултета у Новом Саду* 2/2012, 177-192; М.Писарић, „Електронски записи као доказ у кривичном потупку", *Зборник радова Правног факултета у Новом Саду* 2/2009, 519-536.

ради, постоји обиље комуникационих мрежа и средстава: подаци се размењују уз помоћ привремених *online*датотека и сервера, а у све широј употреби су паметни мобилни телефони којима се приступа Интернету, *VOIP* технологија, апликацијеса систематском енкрипцијом (*Skype*) те софтвери који прикривају комуникациони канал и онемогућавају утврђивање адресе извора и одредишта комуникације (какав је *TOR -The Onion Roter*), па је потребно експедитивно деловати да би се открио траг или извор комуникације. Проналажење извршиоца преко *IP*адреса није више толико једноставно као пре неколико година, из више разлога: тачно је да се уз помоћ *IP* адресе може открити веза са одређеним пружаоцем Интернет услуга и територијом одређене државе, али то не значи да ће се та адреса довести у везу са крајњим корисником јер су све више у употреби динамичке *IP*адресе, а осим тога могуће је коришћењем одређених програма прикривати, односно исте мењати. Стога је неопходно преиспитати основне постулате на којима почива Конвенција Савета Европе а тиме и решења у националним системима држава потписница, међу којима је и Република Србија, односно размотрити потребу унапређења постојећих и предложити увођење нових решења у кривичном процесном праву.

*Milana Pisarić, Assistant*
*University of Novi Sad*
*Faculty of Law Novi Sad*

# The Normative Response to Problems of Detection and Investigation of Cyber Crime

***Abstract:*** *Certain aspects of cyber crime represent the essence of the problems that authorities prosecuting crimes committed by abuse of information technology face everyday. All these specific feauters of cyber crime crime must be taken into consideration in order to understand and overcome difficulties in investigation and prosecution of crimes and trial of perpetrators. Given all the above and in order to respond to the specific nature of criminal activities committed using computer networks and systems, it is understandable that countries strive to adapt or complement the existing criminal law provisions. To create an appropriate legal framework for fighting this type of crime by means of criminal law, rules of substantive criminal law should incriminate certain behaviors and predict offenses against the confidentiality, integrity and availability of computer data and computer systemsand rules of criminal procedure law should determine the appropriate powers of the authorities in order to identify sources of illicit actions and collect information on the committed offense and the offender which could be used as evidence in criminal proceedings.*

***Key words:*** *cyber crime, the normative response, detection, investigation.*