NE bezpečie sociálnych sietí

Ľubomír Lukič
Pavol Sokol

EISI European Information Society Institute

(Ne)bezpečie sociálnych sietí

JUDr. Ľubomír Lukič
RNDr. JUDr. Pavol Sokol

EISI European Information Society Institute

JUDr. Ľubomír Lukič
RNDr. JUDr. Pavol Sokol

(Ne)bezpečie sociálnych sietí

Prvé vydanie. Vydalo European Information Society Institute, o. z. v roku 2014,
http://eisionline.org.

Realizované s finančnou podporou Ministerstva zahraničných vecí a európskych záležitostí SR v rámci dotačného programu Podpora a ochrana ľudských práv a slobôd.
Za obsah tohto dokumentu je výlučne zodpovedný European Information Society Institute, o. z.

Recenzenti:	JUDr. Peter Huba, PhD., RNDr. Róber Hajduk, PhD.
Jazyková korektúra:	Mgr. Peter Béreš
Obálka:	Diana Matláková
Tlač:	EQUILIBRIA, s.r.o.

ISBN 978-80-971307-2-5

Obsah

Úvod

Sociálne siete, pojem dnes tak často používaný, mnohokrát skloňovaný, ktorý väčšina z nás pozná. Mnohí z nás sú na nich registrovaní a aj ich aktívne používajú. Získavame pomocou nich nových kamarátov, udržiavame existujúce priateľstvá alebo šírime informácie rôzneho druhu o nás či o iných ľuďoch. Záleží len na nás, ako tento prostriedok používame. Mnoho ľudí je na sociálnych sieťach každý deň a dokonca dokážu na nich stráviť aj hodiny bez akejkoľvek väčšej prestávky, či potreby osobného, fyzického kontaktu so živou osobou. Sociálne siete sú tak čím ďalej, tým viac súčasťou nášho každodenného života, bez ktorej si niektorí už ani nevedia predstaviť cestu autobusom do školy, čakanie u lekára, kaderníčky, či obednú prestávku. Jednoducho svoj bežný deň. Asi takto vyzerá v krátkosti obraz sociálnych sietí a ich užívateľov.

Poznáme však tieto sociálne siete tak dobre, ako si myslíme? Nepoznajú nás náhodou sociálne siete lepšie, ako my ich? Či dokonca nepoznajú nás sociálne siete lepšie, ako poznáme sami seba? Aj to sú otázky, na ktoré po prečítaní tejto knihy dostaneš odpoveď alebo na ňu budeš navedený.

Život nie je len o tom, kto koho a ako dobre pozná, ale aj o tom, ako sa k tým, ktorých poznáme správame. Toto je tiež dôležité aj vo virtuálnom priestore sociálnych sietí. Dochádza tam k rôznemu druhu komunikácie medzi jej užívateľmi. Najčastejšie si užívatelia posielajú správy, zdieľajú statusy, fotografie, „lajkujú" a komentujú si zdieľaný obsah, alebo jednoducho relaxujú a zabávajú sa pri nejakej hre. Spôsob tejto komunikácie voči ostatným, teda naše správanie a prejavovanie sa, môže často vyvolať veľa otázok. Je správne označiť kamaráta na fotke bez jeho súhlasu? Ako a čo môžem zdieľať s inými? Môžem používať výtvory niekoho iného? Sú na sociálnych sieťach nejaké nebezpečenstvá a nástrahy, ktoré na mňa číhajú od iných užívateľov? Patria nadávky a urážanie na sociálne siete?

Sieťou svojich priateľov, svojim správaním, ako aj rôznymi informáciami uvedenými na sociálnej sieti, si vytvárame určitý profil a meno, resp. reputáciu. Na jej ochranu, na to aby nebola zneužitá či poškodená, si však musíš dávať pozor na to, aké informácie o sebe zverejňuješ, ako a komu odhaľuješ svoje súkromie či súkromie iných. Alebo či tvoje konanie nemôže negatívne zasiahnuť alebo obmedziť niekoho iného, či dokonca byť trestné.

Všetkým týmto vyššie uvedeným veciam sa postupne budeme venovať:

- V prvej časti sa zameriame na sociálne siete ako také. Okrem ich zadefinovania a uvedenia niekoľkých prípadov, načrtneme problémy s ich používaním.
- V druhej časti si povieme niečo o ochrane tvojho súkromia. O tom, kde sú hranice toho, čo smieš o živote iných písať alebo zobrazovať ty, a čo smú iní.
- V tretej časti si priblížime to, ako môžeš nakladať s cudzími výtvormi. O tom, kedy môžeš zdieľať fotky, videá a články, na čo si dávať pozor, a čo môže s tvojimi výtvormi robiť sociálna sieť.
- V štvrtej časti sa porozprávame o rôznych spôsoboch zneužívania sociálnych sietí. O tom, s akými nebezpečenstvami a nástrahami sa na nich môžeme stretnúť, ako ich spoznať a predchádzať im, a tak byť vo väčšom bezpečí.
- V poslednej piatej časti si povieme, ako sa vyhnúť tým najčastejším nástrahám. O tom, aké základné postupy môžeš použiť aj bez toho, aby si hneď musel žiadať niekoho o pomoc.

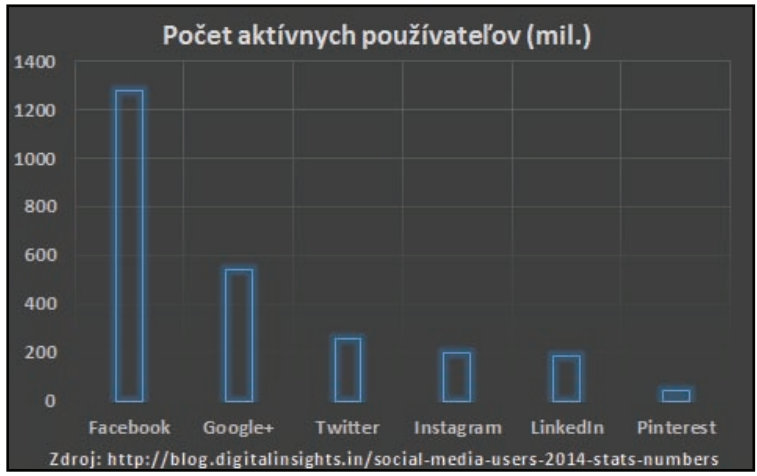
Veríme, že táto kniha bude slúžiť ako jednoduchý, prehľadný a dostatočne zrozumiteľný sprievodca svetom sociálnych sietí, ktorý ozrejmí jej zákutia a poukáže na rôzne druhy nežiaduceho konania, ktorým možno zasiahnuť či obmedziť práva iných užívateľov. Našim cieľom je poskytnúť základné informácie, odpovede na najčastejšie sa vyskytujúce otázky či situácie tak, aby si si po jej prečítaní bol vedomý svojich práv, ako aj práv iných a nebezpečenstva rôzneho druhu, ktoré sa na sociálnych sieťach môže vyskytnúť. Lebo, ako sa hovorí, nevedomosť neospravedlňuje.

1. Sociálne siete

V úvode sme spomínali sociálne siete ako fenomén dnešnej doby. S týmto fenoménom sa však spája aj množstvo otázok. Čo vlastne sú sociálne siete? Aké najznámejšie a najpoužívanejšie poznáme? Aké sú ich základne charakteristické vlastnosti? Ako nás môžu obmedzovať, či ohrozovať? Tak sa pusťme do toho a zoznámme sa s týmto fenoménom bližšie.

Sociálna sieť je webová stránka určená na nadväzovanie a udržiavanie kontaktov medzi ľuďmi. Ľudia sa tak spájajú do skupín, na základe ktorých vzniká sieť vzťahov a kontaktov, v rámci ktorej komunikujú a zdieľajú obrázky, videá a informácie. Každý používateľ si vytvorí vlastný profil, v ktorom napíše o sebe základné informácie. Tento profil by mal odrážať reálnu identitu užívateľov za použitia skutočných mien, e-mailových adries, fotografií, videí a iných identifikačných znakov. Nevýhodou sociálnych sietí je fakt, že používatelia nemusia do svojho profilu vložiť pravdivé informácie a je to takmer nemožné zistiť.

Medzi najznámejšie a najpoužívanejšie sociálne siete vo svete patrí Facebook[1], LinkedIn, Google+, Twitter, MySpace, Badoo. Na Slovensku je takouto sociálnou sieťou Pokec.sk. Môžu byť orientované všeobecne, bez zamerania na konkrétne záujmy - napr. Facebook - alebo môžu byť konkrétne orientované na určité témy a záujmy - napr. LinkedIn. Toto všetko sú tie sociálne siete, bez ktorých si mnoho ľudí už nevie predstaviť svoj každodenný život.



Obr. 1 - Počet aktívnych používateľov v sociálnych sieťach

To, že dnešná mládež využíva internet a sociálne siete každodenne je fakt. Intenzita však môže byť rôzna, a to od niekoľko minút cez niekoľko hodín až po všetok svoj voľný čas. Takéto využívanie však môže prerásť do závislosti a tu už možno hovoriť o probléme.

Rozšírenosti, resp. zvýšenému záujmu o sociálne siete, prispel aj rozvoj nových technológií a dostupnosť internetu. Najmä smartfóny a tablety s pripojením na internet sú s obľubou používané na zdieľanie rôzneho obsahu cez sociálne siete. Cez fotoaparát, ktorý má každé takéto zariadenie, možno s ľahkosťou vytvoriť fotografiu alebo video a zdieľať ich. Iným spôsobom ich využitia je napr. označovanie svojej pozície - teda zdieľanie so svetom v akom obchode sa práve nachádzaš, kde práve obeduješ, kde práve dovolenkuješ. Tieto údaje sú mnohokrát veľmi užitočné pre teba, tvojich priateľov, rodičov, ale tiež i pre zločincov, či podvodníkov, čo z nich zároveň robí citlivé a nebezpečné údaje, ktoré si treba primerane chrániť.

Sociálne siete možno v zásade považovať za verejný priestor. Znamená to, že čokoľvek na sociálnu sieť umiestniš, umiestňuješ to akoby do verejného priestoru a môže to vidieť ktokoľvek. Zdanie bezpečia a súkromia je falošné, pretože k tvojim údajom sa vždy môžu dostať aj tí, ktorým nie sú určené, a to napr. hackeri, útočníci, škodlivý softvér. Ktokoľvek, kto sa náhodou dostal k počítaču, kde užívateľ ostal prihlásený na Facebooku. Ani tvoje heslo nie je nezistiteľné, resp. neprelomiteľné, obzvlášť to platí u tých, ktorí používajú slabé heslá a navyše ich zdieľajú s ďalšími ľuďmi. História sociálnych sietí je plná príkladov zlyhania v otázke ochrany súkromia a osobných údajov užívateľov pre chyby programátorov, či bezpečnostné chyby. Postupnú premenu súkromného na verejné možno tiež vidieť aj pri každej úprave podmienok používania určitej sociálnej siete.

Neuvedomovanie si rizika a nepredchádzanie mu nevedie k bezpečnému správaniu sa na sociálnych sieťach. Deti a mládež na Facebooku bezhlavo „lajkujú“ čokoľvek, zúčastňujú sa čohokoľvek, schvaľujú akejkoľvek aplikácie, klikajú na akékoľvek odkazy. Užívatelia na svoje profily na sociálnych sieťach píšu a nahrávajú prakticky čokoľvek. Neskúsení dospelí užívatelia sa ale v tomto ohľade líšia len minimálne. Vo väčšine prípadov platí, že sa deti a mládež ochotne stavajú priateľmi na sociálnych sieťach prakticky s kýmkoľvek, kto o to požiada. Pritom v reálnom svete rodičia vedú svoje deti k tomu, že nemajú veriť cudzím ľuďom na ulici. Táto dôležitá súčasť výchovy v prípade sociálnych sietí úplne chýba.

Všetci užívatelia, ktorí sa takto nedbalo správajú, sú výrazne ohrození stratou súkromia, zneužitím osobných údajov, stratou identít, hackermi, sociálnym inžinierstvom, phishingom, spamom, vírusmi, škodlivým softvérom, vydieraním, kyberšikanou a organizovaným zločinom.

Používanie a správanie sa na sociálnych sieťach môže mať i právne dôsledky. Ako deti a mládež, tak učitelia, môžu porušovať školské poriadky, porušovať zákony, zasahovať do súkromia iných ľudí alebo inak obmedzovať ich práva. Treba stále myslieť na zásadu: „Neznalosť zákona neospravedlňuje". Teda, aj keď si myslíš, že svojim správaním nikomu neubližuješ alebo nič neporušuješ. Opak je však pravdou, a teba to nezbavuje zodpovednosti za svoje činnosti na sociálnej sieti.

Možno si si teraz položil otázku, že do akých práv už len môžem niekomu pri používaní sociálnych sietí zasiahnuť alebo aké zákony môžem porušiť. Nemusí sa to na prvý pohľad zdať, ale rozsah práv a zákonov je naozaj široký. Často si ani neuvedomuješ, že aj tento obsah či informácia môže byť nejako chránená. Príkladom je vlastnícke právo, ktoré možno vidieť v tvojich výtvoroch, virtuálnych kreditoch či peniazoch. Do tohto práva ti niekto zasiahne, ak ti ukradne tieto virtuálne peniaze alebo bez tvojho súhlasu použije tvoje dielo. Právom na ochranu osobných údajov je chránená väčšina údajov v tvojom profile. Do jeho zásahu môže dôjsť tak, že sa niekto bude vydávať za teba, použije tvoje meno, dátum narodenia, tvoju fotku. Právom na súkromie zas môžeš regulovať čo a komu chceš o sebe zverejniť. Toto právo môže byť narušené tak, že sa niekto bez tvojho súhlasu dostane na tvoj účet na sociálnej sieti a bude si čítať tvoje správy.

Uvedomelý a obozretný používateľ si musí byť vedomý svojich práv (teda čo si má chrániť, ako si to má chrániť), ako aj práv iných. Musí poznať rôznorodosť „nepríjemných" situácií, ktoré sa môžu vyskytnúť, aby sa im vedel vyhnúť a aby ich sám nevykonával. To všetko sa dozvieš v nasledujúcich kapitolách.

2. Chráň si svoje súkromie

Zaujímalo ťa niekedy, aké údaje o tebe zbiera sociálna sieť? Čo sa stane, ak zmažeš niečo na sociálnej sieti? Alebo čo máš urobiť, keď na nej nájdeš svoje fotografie a chceš, aby boli zmazané? Táto kapitola ti odpovie nielen na tieto otázky, ale aj na mnohé iné, ktoré súvisia s ochranou súkromia a osobných údajov na sociálnych sieťach.

2.1 Ľudská osobnosť, osobné údaje a sociálna sieť

2.1.1 Ako chrániť svoju osobnosť?

Zrejme sa hneď opýtaš, čo má ochrana tvojej osobnosti spoločné s ochranou súkromia? Veľmi veľa. Život, zdravie, česť, dobré meno, dôstojnosť a súkromie, fotografie, videá. Isto sú to pre teba známe pojmy. Čo ale majú spoločné? Všetky tieto stránky tvoria tvoju osobnosť a naše právo ich spoločne označuje ako *príklady tzv. ľudskej osobnosti*. Právo nevie presne zadefinovať, čo ľudská osobnosť je, alebo povedať, čo nie je. Ale vie povedať príklady. A práve tieto pojmy sú príkladmi toho, čo tvorí ľudskú osobnosť.

Naše *právo chráni* celú *ľudskú osobnosť*[2]. Nie je to len súkromie človeka, ale chráni aj jeho život, zdravie, česť a dôstojnosť. A dokonca, chráni aj tvoje podobizne, či už na fotografii alebo videu a súkromné texty, v ktorých vyjadruješ svoje myšlienky, názory, pocity a pod. Tieto súkromné texty zákon označuje ako *písomnosti osobnej povahy*. Príkladom takejto písomnosti môže byť denník, ľúbostný list, alebo aj e-mail.

Čo je vlastne súkromie? Čo znamená mať právo na súkromie? Každý z nás má *právo na súkromie*, a teda aj ty máš právo rozhodnúť, či a akým spôsobom budú zverejnené informácie z tvojho súkromného života. Máš možnosť kontrolovať, ako s odovzdanými informáciami z tvojho osobného života nakladajú druhí.

Ty sa rozhodneš, či informáciu o tom, že sa ti niekto páči, nikomu nepovieš, alebo ju povieš len svojim dobrým kamarátom. Ak im to ale povieš a upozorníš ich na to, že táto informácia nie je určená pre ďalšie osoby, musia to rešpektovať, keďže ty máš právo na ochranu svojho súkromia.

2.1.2 Čo sú osobné údaje?

Informácie o človeku, s ktorými musíš narábať opatrnejšie, ako je bežné, sa nazývajú tzv. *osobné údaje*[3]. Osobné údaje môžeš použiť len so súhlasom dotknutého človeka. Výnimočne ti môže tento súhlas dať namiesto neho priamo zákon. Základné pravidlo je, že ak pracuješ s niečím, čo obsahuje osobný údaj (napr. video zobrazujúce spolužiakov), môžeš ho použiť len na účel, na ktorý máš súhlas. Napríklad video so spolužiakmi, ktoré si bol poverený urobiť pre školský archív, nemôžeš len tak hodiť na YouTube. Potrebuješ na to osobitný súhlas všetkých spolužiakov, ktorých na ňom vidieť. V tejto časti si vysvetlíme, *kedy* je informácia osobný údaj a *ako* s ňou môžeš potom nakladať.

Podľa tohto zákona sa osobnými údajmi myslia také údaje, ktoré sa týkajú *určenej alebo určiteľnej fyzickej osoby*. Inými slovami, ide nám o to, aby sme pomocou niekoľkých znakov – údajov vedeli presne identifikovať konkrétneho človeka. Ak to možné je, musíš s týmito údajmi nakladať opatrnejšie. Ak nikoho podľa nich identifikovať nevieš, môžeš s nimi zaobchádzať ako zvyčajne.

Napríklad, ak vieme, že nejaká osoba sa volá Peter, tak takýchto osôb vieme nájsť v okolí viacero. Takže podľa mena nevieme presne určiť osobu. To znamená, že samotné meno nie je osobný údaj. Ak ale vieme, že ide o Petra zo 4.A, čo býva neďaleko školy, možno už vieme, o koho ide.

Alebo si vezmi priezvisko Horváth, ktoré patrí k najčastejšie používaným u nás. Ak sa opýtaš okoloidúceho na ulici na Petra Horvátha, tak osoba, ktorej sa pýtaš, nebude zrejme vedieť presne určiť, o akú osobu ide. Ak budeme ale postupne pridávať ďalšie údaje, v istom momente budeme vedieť určiť konkrétnu osobu. K menu a priezvisku stačí uviesť aj dátum narodenia alebo bydlisko. Hneď je nám zrejmé, o koho ide. Tieto údaje potom spoločne nazývame *osobné údaje.*

Okrem bežných osobných údajov, existuje aj ich špeciálna *skupina osobitne citlivých údajov*. Tie odhaľujú rasový alebo etnický pôvod človeka, jeho politické názory, náboženskú vieru, odhaľujú otázky jeho zdravia alebo pohlavného života. Použitie týchto osobných údajov je vo všeobecnosti zakázané. Len výnimočne umožňujú zákony ich získavanie a používanie. Príkladom môže byť napríklad vedenie zdravotnej dokumentácie u lekára. Medzi tieto osobné údaje zaraďujeme aj *rodné číslo*[4], ktoré je pre každého občana jedinečné a podľa neho nie je problém určiť, o akú osobu ide.

Každý, kto získava osobné údaje, smie tak robiť len za určitým účelom. Tento účel *nazývame účel spracovania osobných údajov*. Môže ísť napríklad o realizáciu zájazdu, poskytnutie e-mailových kont, zoznam ľudí na zber papiera a pod. Získané údaje potrebuješ ale niekde ukladať a vedieť s nimi pracovať. Predstav si situáciu, že by stredná škola mala o každom študentovi jeden papierik a tieto papieriky by boli len porozhadzované v nejakej polici. Keby si chcel zistiť, koľko má škola prvákov, bol by to problém. Z tohto dôvodu sa najskôr vytvorili tzv. kartotéky. Iste ich poznáš. Tvoja lekárka má plné skrine zdravotných kariet. Nemá ich však len porozhadzované, ale pekne usporiadané podľa priezviska alebo roku narodenia. Takéto karty musia byť patrične zabezpečené, keďže údaje v nich sú osobitne citlivé. Sociálna sieť (napr. Facebook alebo Pokec) je ako taká skriňa u lekára, ktorá je plná zdravotných kariet.

Tieto skrine u lekára môžeme nazvať *informačným systémom osobných údajov*. Informačným z toho dôvodu, že z neho vieme získať informácie a systémom preto, lebo tie zdravotné karty tam nie sú rozhádzané akokoľvek, ale podľa nejakých pravidiel. Všetky sociálne siete predstavujú z hľadiska osobných údajov práve tieto informačné systémy.

Už vieme, čo je informačný systém. Dôležitou otázkou je, čo môžeme robiť s osobnými údajmi v rámci informačného systému. Osobné údaje najprv získavame, zhromažďujeme. Napríklad, sociálna sieť prostredníctvom registračného formulára získala od teba tvoje osobné údaje (tvoje meno, priezvisko, dátum narodenia...).

Po získaní sú tieto údaje ďalej spracovávané. Napríklad, môžu byť poskytnuté zadávateľom reklamy, tvorcom aplikácií alebo len vyhodnocované v rámci sociálnej siete. Tieto činnosti spoločne nazývame spracovanie osobných údajov. Spracovať osobné údaje možno len na základe súhlasu. Ten ti môže dať zákon, alebo ten, o koho osobné údaje ide.

Osoby, ktorých osobné údaje spracúvame, nazývame dotknuté osoby. Ak napríklad ideš po chodníku, ktorý je monitorovaný kamerami, si dotknutá osoba. Kamery ťa snímajú a obrázky s tebou sa budú uchovávať. Dotknutou osobou si aj v prípade, ak používaš sociálne siete. Na druhej strane, osoba, ktorá prevádzkuje kamerový systém a sociálnu sieť, sa nazýva prevádzkovateľ informačného systému. Pamätáš si ešte na tie kartotéky? Lekár, ktorý prevádzkuje kartotéku, je prík-

ladom prevádzkovateľa. Iným príkladom je spoločnosť Google, ktorá prevádzkuje sociálnu sieť Google+.

2.2. Ľudská osobnosť a osobné údaje v sociálnych sieťach

2.2.1. Aké údaje o tebe zbiera sociálna sieť?

Sociálne siete v súčasnej dobe zbierajú *množstvo osobných údajov*. Počnúc menom, priezviskom a e-mailom, až po informácie, kde sa nachádzaš, keď nahrávaš svoje fotografie. Sociálna sieť má právo pýtať sa ťa len na také osobné údaje, ktoré sú potrebné na to, aby mohla fungovať správne. Žiadne iné údaje nemá právo od teba požadovať a následne spracovávať.

Zoznam vyžadovaných osobných údajov závisí od konkrétnej sociálnej siete. Zväčša však chcú tvoje *meno*, *priezvisko*, aby si mohol nejako vystupovať na sociálnej sieti a aby ťa mohli ostatní identifikovať. Takmer všetky sociálne siete vyžadujú *dátum narodenia*, keďže pri väčšine z nich (Facebook, Google+, Twitter) musíš mať určitý minimálny vek (aspoň 13 rokov). Pri niektorých sociálnych sieťach to je až 18 rokov (Badoo). Prečo práve 13 rokov? Podľa zákonov v USA (kde má sídlo väčšina sociálnych sietí) webové stránky, ktoré zbierajú informácie o používateľoch, nesmú dovoliť, aby osoba mladšia ako 13 rokov sa na túto stránku prihlásila.[5]

Kvôli bezpečnosti a identifikácii je niekedy potrebné poskytnúť aj ďalšie údaje. Môže sa napríklad stať, že zabudneš heslo, alebo sa niekto prihlási do tvojho konta. Pre tieto prípady chce mať sociálna sieť tvoj e-mail alebo telefónne číslo.

Lenže tu zoznam osobných údajov, ktoré zbierajú sociálne siete, nekončí. Ako môžeš vidieť na tabuľkách nižšie, nie sú to len tie „potrebné“ údaje. Pre predstavu, aké množstvo údajov sociálne siete zbierajú, uvádzame príklady pre sociálne siete Facebook a Pokec.

Tabuľka č. 1 – Údaje zbierané sociálnou sieťou Facebook[6]

(1) Informácie o používateľovi	(2) Príspevky na stene	(3) Príspevky na stenách ostatných
(4) Videá	(5) Stav účtu	(6) História účtu
(7) Adresa	(8) Cookie informácie, (napr. informácie o prehliadači)	(9) Alternatívne mená
(10) Vyhľadávanie v rámci Facebooku	(11) Chat	(12) Rozpoznanie tváre
(13) Pripojenie	(14) Kreditné karty	(15) Aktuálne mesto
(16) Dátum narodenia	(17) Indikácia vzťahov	(18) Vzdelanie
(19) Odobraté označenia	(20) E-maily	(21) Rodina
(22) Podrobnosti o vzťahoch medzi priateľmi	(23) Príspevky	(24) Pohlavie
(25) Pracovisko	(26) Politické názory	...

Tabuľka č. 2 – Údaje zbierané sociálnou sieťou Pokec

Meno a priezvisko	Chat	Správy na nástenke
Výška	Váha	Postava
Typ postavy	Zrak	Farba očí
Farba vlasov	Typ vlasov	Ukončené vzdelanie
Profesia	Jazyky	Obľúbená farba
Znamenie v zverokruhu	Vzťah k fajčeniu	Vzťah k alkoholu
Rodinný stav	Deti	Záľuby
Priatelia	Fotky	Videá

Ak chceš vedieť, aké osobné údaje o tebe zbiera sociálna sieť Facebook, požiadaj o ne. Máš dve možnosti, ako sa dostať k tvojim údajom[7]:

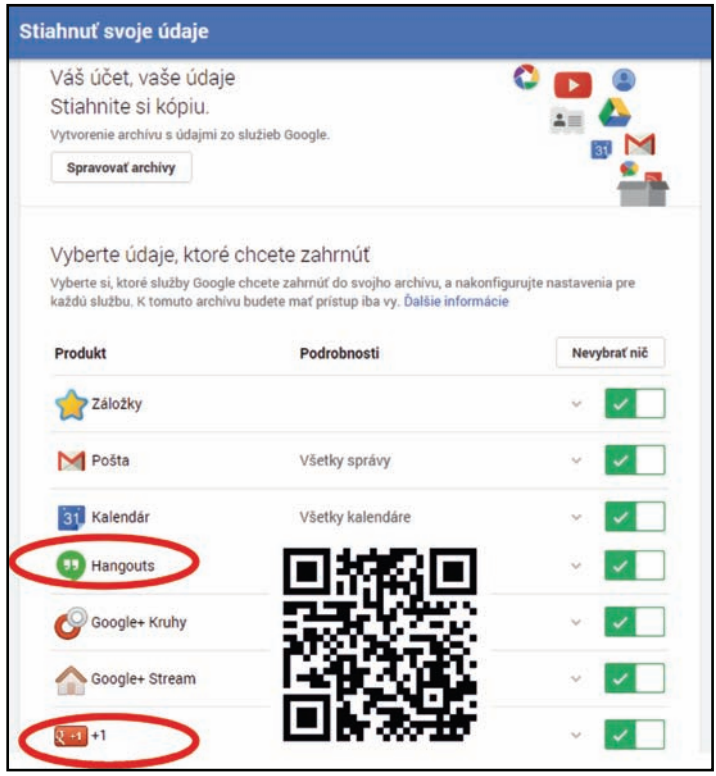
- pomocou klasickej pošty (obrázok č. 2 vľavo)
- pomocou e-mailu (obrázok č. 2 vpravo)

Obrázok č. 2 – Stiahnutie údajov v sociálnej sieti Facebook

Ak ale nechceš dlho čakať, môžeš si do pár minút urobiť kópiu niektorých svojich údajov (správy, statusy, obrázky a pod.). Choď do časti nastavenia a v rámci nich v časti „Všeobecné nastavenia účtu" máš možnosť „Stiahnite si kópiu svojich údajov z Facebooku". Po stlačení na odkaz sa ti ukáže rovnaké okno, ako vidíš na obrázku č. 3.

Obrázok č. 3 – Stiahnutie údajov v sociálnej sieti Facebook

Možnosť stiahnuť si svoje údaje máš aj na sociálnej sieti Google+. Stačí, ak pôjdeš na webovú adresu https://www.google.com/settings/takeout. Po kliknutí na odkaz sa zobrazí formulár (obrázok č. 4) na stiahnutie kópie tvojich údajov. Vo formulári si vieš nastaviť, ktoré údaje chceš zahrnúť do zálohy.



Obrázok č. 4 – Stiahnutie údajov pre služby spoločnosti Google (vrátane Google+)

2.2.2 Môže moje údaje sociálna sieť predávať?

V nedávnej dobe sa v novinách a na internete objavili správy, že sociálne siete chcú predávať naše osobné údaje a že sa proti tomu musíme brániť. Skutočnosť je však taká, že sociálne siete predávajú naše údaje už dlhšie.

Asi sa pýtaš, z čoho taká sociálna sieť zarába, keďže my za jej užívanie nič neplatíme. Odpoveďou je *reklama***.** Vďaka nej majú prevádzkovatelia sociálnych sietí peniaze na to, aby ti mohli poskytovať svoje služby. Okrem toho však sociálna sieť poskytuje tvoje údaje iným osobám, ktoré jej za to platia.

Vezmime si ako príklad sociálnu sieť *Facebook*. V pravidlách tejto sociálnej siete sa dočítaš, že súhlasíš s tým, aby tvoje meno, priezvisko, profilovú fotografiu a všetko, čo uverejňuješ, poskytuješ alebo zdieľaš na Facebooku (napr. tvoju obľúbenú značku topánok) mohol Facebook používať a poskytovať iným spoločnos-

tiam (napr. predajcom značkových topánok). Jeho zámerom je zlepšiť cieľovosť reklamy. Problém je, že nie vždy chceme, aby všetko naše správanie bolo spracúvané pre reklamu. Ak si si pozeral darčeky na Vianoce, isto nechceš, aby sa ti teraz zobrazovali podobné reklamy vždy, keď zapneš Facebook. Používanie tvojich údajov je v poriadku, ak si s ním súhlasil. Nie vždy však všetko, čo je v podmienkach sociálnej siete, musí aj platiť.

Iným príkladom je sociálna sieť *Google+*. V jej pravidlách (časť ochrana osobných údajov) je napísané, že spoločnosť Google získava od teba aj informácie o tom, aké služby tejto spoločnosti používaš (napr. Google+, vyhľadávač, YouTube a iné). Keďže Google neposkytuje len vlastné služby, ale odkazuje aj na služby iných spoločností (napr. odkazy na webové stránky), zbiera o tebe veľa osobných údajov.

Zamyslel si sa niekedy, prečo ti Google vie poskytnúť tak relevantné výsledky vyhľadávania alebo reklamy? Je to práve preto, že Google zhromažďuje rôzne informácie a používa ich na poskytovanie a zlepšovanie existujúcich, ale aj nových služieb.

Ak si to teda zhrnieme, sociálne siete zarábajú na tom, že ti ponúknu len kvalitnú a pre teba na mieru ušitú reklamu. Teraz už aspoň budeš vedieť, odkiaľ prevádzkovatelia sociálnych sietí majú peniaze na prevádzku. Sociálne siete teda nie sú bezplatné, pretože za ich užívanie platíš svojim súkromím a svojimi osobnými údajmi.

2.2.3 Smiem používať fotky a videá, na ktorých sú moji kamaráti?

Na účte tvojej sociálne siete máš istotne rôzne statusy, fotografie, videá a fotografie a videá svojich priateľov alebo iných osôb. Všetko to spolu nazývame *prejavy osobnej povahy*. Zrejme sa pýtaš, aké fotografie, videá môžeš na sociálne siete nahrávať. V zásade platí pravidlo, že fotografiu alebo video, na ktorom je zobrazená osoba, môžeš urobiť a použiť len s jej súhlasom. Samozrejme, ak na fotografii alebo videu si len ty sám, tak sám rozhodneš o zverejnení. Určité fotografie alebo videá, ktoré sa ti nepáčia, nezverejníš.

Čo ale v prípade, ak na *fotografii alebo videu nie si sám*, ale s tvojimi kamarátmi, resp. inými osobami? V tomto prípade si povinný opýtať sa osôb na fotografii alebo videu, či môžeš túto fotografiu alebo video zverejniť na sociálnej sieti. Každé zverejnenie odporúčame dobre zvážiť. Akonáhle sa fotografia alebo video ocitne

na internete a stanú sa tak verejne prístupnými, je prakticky nemožné zabrániť ich šíreniu a prípadnému zneužitiu.

Zverejnenie fotografie so sebou prináša aj ďalšie nebezpečenstvo. Môže sa stať, že si niekto prisvojí identitu osoby na fotografii, alebo ju upraví tak, aby tejto osobe uškodil. Toto úzko súvisí s krádežou identity, ktorej sa podrobnejšie budeme venovať vo 4. kapitole tejto knihy.

Fotografie alebo videá *intímneho charakteru* by sa nemali zverejňovať vôbec. Možno si kladieš otázku, čo sú fotografie alebo videá intímnej povahy. Pre každého z nás to znamená niečo iné, avšak pamätaj na to, že zverejňovanie fotografií alebo videí s erotickým obsahom môže mať trestno-právne dôsledky.

Súhlas na vytvorenie fotografie či videa s inými osobami však nie je vždy potrebný. Je tomu tak napríklad, ak sa takáto fotografia má použiť na *vedecké a umelecké účely alebo pre tlačové, filmové, rozhlasové a televízne spravodajstvo*. Ide o *tzv. zákonnú licenciu*[8], čo znamená, že priamo zákon (Občiansky zákonník) upravuje výnimky, kedy je možné prejavy osobnej povahy (napr. fotografie, videá) vyhotoviť a použiť bez súhlasu osôb na nich zobrazených. Ak sa teda objaví tvoja fotografia v skupine na sociálnej sieti (môže ísť o verejnú skupinu), kde si zachytený ako účastník nejakej akcie (napr. športovej súťaže, imatrikulácie študentov školy), prevádzkovateľ tejto skupiny týmto zverejnením nič neporušuje. Iným príkladom môže byť nafotenie rannej ulice s náhodným chodcom pre svoju umeleckú koláž.

Aj v týchto prípadoch však použitím fotografií alebo videí nesmie dochádzať k závažnému porušeniu práv osôb zobrazených na týchto fotografiách alebo videách. Príkladom takéhoto zásahu by boli fotografie z nejakého koncertu alebo párty, na ktorých by boli zobrazení návštevníci nie v príliš triezvom stave. Išlo by napríklad o reportáž pre online noviny, ktoré zverejňujú svoje články na sociálnych sieťach. V tomto prípade by bolo možné použiť zákonnú licenciu pre tlačové spravodajstvo. Avšak fotografie by mohli zosmiešniť osoby zachytené na týchto fotografiách, čo znemožňuje ich zverejnenie v týchto online novinách.

Aj deti, ktoré sa na fotografii alebo videu nachádzajú, môžu vyjadriť svoj súhlas, či nesúhlas so zverejnením. Najmä do 15. rokov veku nemusí byť vždy mladý človek tzv. právne spôsobilý udeľovať súhlas[9]. Schopnosť udeliť súhlas záleží od povahy fotografie a vyspelosti v danom veku. Je iné zhotoviť a šíriť bežné školské momentky, ako fotky zo študentskej párty alebo rôzne akty mládežníckej neroz-

vážnosti. Ak dieťa ešte samo nevie posúdiť zverejnenie fotografie alebo videa, musí to za neho urobiť zákonný zástupca (napr. rodič).

2.2.4 Čo sa stane s osobnými údajmi, keď ich zmažem?

Ak chceš zmazať svoje údaje zo sociálnej siete, môžu nastať dve situácie. V tej prvej situácii budú tvoje údaje naozaj zmazané. V druhom prípade budú pred tebou len ukryté. To sa stáva napríklad na Facebooku, pretože nie všetky príspevky a fotografie sa ukladajú len v tvojom účte. Ak napríklad zverejníš príspevok v skupine, tento ostáva na sociálnej sieti aj po zamazaní tvojho účtu. To isté platí aj v prípade poslaných správ. Tvoj kamarát bude mať vo svojej schránke tvoje správy aj naďalej. To i v prípade, keď odstrániš svoj účet.

Každý z nás predpokladá, že fotografie alebo videá sa automaticky vymažú ihneď po tom, ako klikneme na tlačidlo vymazať. Realita je väčšinou iná. Napríklad, na sociálnej sieti Facebook dochádza len k zmazaniu odkazu na fotografiu alebo video a samotnú fotografiu a video je možné si pozrieť ešte počas určitej doby. Stačí presný odkaz na ne.

Podobne je to aj na sociálnej sieti Google+. Zmazaním účtu sa neodstránia žiadne fotky. Naďalej k nim budeš mať prístup v programe Picasa. Ak ich chceš odstrániť, musíš ich vymazať vo webovom albume programu Picasa.

2.2.5 Môžem voľne označovať kamarátov na fotografiách?

Neodmysliteľnou súčasťou sociálnych sietí je tzv. *označovanie (tagovanie)*. Mnohým používateľom sociálnej siete sa stalo, že sa zrazu našli na cudzej fotografii. Výhodou je, že vieš, že nejaká fotografia s tebou bola uverejnená na sociálnej sieti.

V čom ale spočíva záporná stránka označovania? V tom, že ťa niekto označí na fotografii a súčasne ťa pridá k nejakej životnej situácii, resp. skupine alebo názoru. Informácie, ktoré má daná fotografia (určitý obsah, komentáre, súradnice a čas nahratia, používateľ) sa týmto označením prepoja s tebou. Predstav si, že by ťa niekto označil na fotografii s extrémistickým obsahom. Po tomto označení budeš spájaný s nejakou extrémistickou skupinou alebo určitými extrémistickými názormi.

Ako sa právo pozerá na označovanie (tagovanie)? V Európskej únii sa využíva v rámci spracovania osobných údajov tzv. *opt-in prístup*[10]. V praxi to znamená, že

ty musíš súhlasiť s označením (tagom) pred tým, než sa takéto označenie ukáže na sociálnej sieti. Postup je takýto: Ak ťa niekto označí na fotografii alebo videu, dostaneš o tom oznámenie, kde môžeš s označením (tagom) buď súhlasiť alebo nesúhlasiť. Ak budeš súhlasiť, dôjde k označeniu tvojej fotografie, ale ak nie, tak takéto označenie bude zmazané. Príkladom sociálnej siete, ktorá uplatňuje tento princíp, je Facebook. V minulosti to však fungovalo opačne. Označenie (tag) sa uverejnil a označenému používateľovi sa dala možnosť, aby takéto označenie mohol zmazať. Ide o tzv. *opt-out prístup*.

Ako predísť tomu, aby sa fotografie so mnou objavili na sociálnej sieti? Čo mám urobiť, keď sa mi nepáči obsah, v ktorom som označený? Nastav si to na sociálnej sieti. Ako na to, ti ukážeme v 5. kapitole tejto knihy.

2.2.6 Zodpovedám za obsah svojich príspevkov a správ?

Pridávanie príspevkov a písanie správ je asi tá najčastejšia činnosť, ktorú na sociálnej sieti robíš. Nikdy nesmieš zabudnúť, že za každý komentár a príspevok zodpovedáš. Možno si aj sám zachytil správy, kedy uverejnenie urážlivého statusu malo vážne následky pre túto osobu. Uverejnenie nejakého štipľavého komentára by si mal preto dobre zvážiť a pamätať na to, že jeho následné vymazanie nie je tak celkom jednoduché. V prípade napríklad ohovárania, sa tieto komentáre a príspevky môžu stať dôkazom proti tebe. V poslednom období sa objavilo niekoľko súdnych prípadov, kde sa príspevok na sociálnej sieti stal dôvodom pre žalobu alebo pokutu.

Prvým príkladom je prípad známeho novozélandského hráča kriketu Cairnsa, ktorý podal v roku 2010 žalobu na predsedu IPL (Indian Premier League) Modiho. Crains bol vylúčený z indického tímu Chandigarh Lions. Ako oficiálny dôvod bolo uvedené porušenie zmluvy v dôsledku zhoršenia zranenia členka, ku ktorému došlo na charitatívnej akcii. Modi (predseda IPL) vyjadril názor, že dôvodom bolo to, že Crain stál za stávkarskými podvodmi. Tento názor publikoval verejne ako príspevok na sociálnej sieti **Twitter**. Crains podal na Modiho žalobu. Súd napokon konštatoval, že Modimu sa nepodarilo zabezpečiť spoľahlivé dôkazy o tom, že Cairns bol zapojený do stávkarského podvodu a prisúdil Cairnsovi náhradu škody 90 000 libier.

Iným príkladom je prípad muža z Českej republiky, ktorý sa v roku 2014 na sociálnej sieti Facebook vo svojom príspevku vulgárne vyjadril na adresu po-

licajta, ktorý riešil jeho trestnú vec. Tento muž dostal od Českej polície pokutu 10 000 českých korún (362 eur) za to, že týmto statusom „znižoval autoritu policajného orgánu, ohrozoval dôveru v jeho činnosť a znižoval vážnosť a dôstojnosť jeho funkcie". Muž sa najprv voči pokute odvolal na súde. Tento súd sankciu potvrdil a len ju znížil na 5 000 českých korún (181 eur).

Pokutovaný používateľ sa preto obrátil na Ústavný súd Českej republiky s tým, že Polícia Českej republiky nezákonne a neoprávnene kontrolovala komunikáciu dvoch používateľov sociálnej siete a porušila tak ich právo na súkromie. Ústavný súd Českej republiky počas súdneho procesu zistil, že informácie o príspevku muža na sociálnej sieti Facebook získal v rámci výpovede iného muža, ktorý nechal sprístupniť jeho účet na Facebooku a Polícia Českej republiky si urobila screenshoty obrazovky, kde bol príspevok muža. Ústavný súd Českej republiky však považoval za potrebné, aby Polícia Českej republiky mala súhlas k sprístupneniu a vytvoreniu takýchto screenshotov od muža, ktorý vypovedal. Ústavný súd Českej republiky sa napokon pokutovaného muža zastal a pokutu zrušil ako svojvoľnú a neústavnú. Konštatoval, že aj pri zabezpečovaní údajov zo sociálnej siete Facebook musí polícia postupovať podľa trestného poriadku a musí aj zohľadňovať, či ide o súkromné alebo verejné príspevky na sociálnej sieti.

Na týchto príkladoch môžeš vidieť, že za príspevky na sociálnej sieti zodpovedáš a je dobré zvážiť, čo v nich napíšeš.

2.2.7 Aké údaje poskytujú sociálne siete externým aplikáciám?

Bez rôznych aplikácií na sociálnych sieťach si už ani nevieme predstaviť život. Niektoré nám ponúkajú možnosť stráviť čas hraním, iné naopak vzdelávaním, alebo len čítaním nejakých správ. Čo si ale pri týchto aplikáciách neuvedomujeme, je to, že ich spravuje úplné iný prevádzkovateľ, ktorého identitu nikto z nás neskúmal, resp. ju nevie zistiť. Koľkokrát sa ti stalo, že musíš dať súhlas sociálnej sieti, aby poskytla tvoje údaje tejto aplikácii? Keďže chceš túto aplikáciu vyskúšať, klikneš na áno a v tej chvíli sú tvoje osobné údaje úplne niekde inde. Pýtaš sa, aké údaje a kde? To závisí od aplikácie. Ale ak to poskytneš napríklad aplikácii z Číny, tak isto neočakávaj, že sa budeš domáhať svojich práv podobne, ako to je to napríklad v Slovenskej republike.

Čo na to ale sociálna sieť? V pravidlách sociálnych sietí máš napísané, že ak súhlasíš s poskytnutím svojich údajov pre takéto aplikácie, táto sociálna sieť ich prakticky poskytne a negarantuje, ako sa s nimi naloží.

Napríklad sociálna sieť **Facebook** poskytuje aplikáciám len **verejne dostupné informácie** (meno, priezvisko, profilová fotografia, kontakty, skupiny, pohlavie, používateľské meno). Ak aplikácia potrebuje ďalšie informácie, napr. chce mať prístup k tvojim príspevkom, fotografiám a veciam, ktoré si označil, že sa ti páčia, musí ťa požiadať o špeciálne povolenie. Kontrolu aplikácií na sociálnej sieti Facebook môžeš urobiť v nastaveniach v časti „kontrola súkromia" – Vaše aplikácie." Viac sa dozvieš v 5. kapitole.

Odporúčanie pre teba. Dobre si vždy zváž, či hra alebo iná aplikácia na sociálnej sieti stojí za odovzdanie tvojich osobných údajov úplne neznámym osobám alebo spoločnostiam. Ak si myslíš, že áno, presvedč sa aspoň, komu a aké údaje týmto spôsobom poskytuješ (napr. prečítaním ich podmienok používania).

2.2.8 Aké údaje o tebe získava like tlačidlo a podobné tlačidlá?

Kto by nepoznal tlačidlá, pomocou ktorých používatelia sociálnych sietí povedia, že sa im niečo páči a ostatným to odporúčajú pozrieť. Nie je potrebné nič písať, komentovať, jednoducho stlačením týchto tlačidiel vyjadríš to, že sa ti niečo páči (fotografia, status, určitý text). Na sociálnej sieti Facebook je tým tlačidlom *LIKE tlačidlo* na sociálnej sieti Google+ používaš *+1 tlačidlo* a na sociálnej sieti Twitter je to *tlačidlo Tweet* (obrázok č. 5).

Obrázok č. 5 – Tlačidlo Like zo sociálnej siete Facebook, tlačidlo +1 zo sociálnej siete Google+ a tlačidlo Tweet zo sociálnej siete Twitter.

Uvedomuješ si však, že súčasne s týmto kliknutím odovzdávaš sociálnej sieti ďalšie údaje o sebe? Ak použiješ jedno zo spomenutých tlačidiel, tak súčasne sociálnej sieti poskytneš svoje GPS súradnice, IP adresu tvojho zariadenia, typ tvojho zariadenia (napr. mobil). Teda sociálna sieť vie takto o tebe zistiť nielen, čo sa ti páči, ale aj kedy, kde a na akom zariadení.

Že si na to nebol upozornený? Omyl. Pri registrácii si súhlasil s podmienkami sociálnej siete, kde je aj tento súhlas uvedený.

2.2.9 Je členstvo v sociálnych skupinách neškodné?

Informácia o členstve v skupine vyzerá ako bezvýznamný údaj. Nie vždy tomu tak je aj v skutočnosti. Členstvo v skupine, ktorá má extrémistické názory, môže mať aj pre teba nepriaznivé následky. Navyše sa môže stať, že skutočné pozadie tejto skupiny sa ukáže až neskôr, dávno po tom, ako si sa do skupiny prihlásil. Napríklad, hlásiš sa do zamestnania a tvoj budúci zamestnávateľ si všimne, že obľubuješ konkurenciu (napr. pizzu od inej pizzerie). Síce to nemusí byť ihneď tvoja nevýhoda, ale môže byť. Iná situácia však bude, ak si v skupine, ktorá sa ukáže ako extrémistická a hlása napríklad rasovú neznášanlivosť. Jedného dňa ťa navštívi polícia a ty budeš uvažovať nad tým, čo si vlastne urobil, resp. neurobil. Nemusel si však nič urobiť, len sa nachádzať práve v takejto skupine. Polícii táto skutočnosť úplne postačí na to, aby si ťa preverila.

Určite sa ti už stalo, že si bol zrazu členom skupiny, o ktorej si vôbec nič nevedel. Mohlo sa stať, že administrátor skupiny zmenil názov a popis skupiny. Ak si členom vo viacerých skupinách, nemusíš si to všimnúť, ani keď máš nastavené posielanie správ z tejto skupiny. Tak sa celkom ľahko môžeš ocitnúť v skupine, s ktorej názormi vôbec nesúhlasíš. Občas je preto dobré svoje členstvá v skupinách skontrolovať.

2.2.10 Za čo sociálna sieť zodpovedá a za čo nie?

Pri registrácii asi málokedy čítaš pravidlá používania sociálnych sietí. Každý z nás automaticky súhlasí s podmienkami a neprečíta si ani časť venujúcu sa osobným údajom. A pritom ide o tak podstatné informácie.

Sociálne siete sa snažia zbaviť akejkoľvek zodpovednosti. Odvolávajú sa pritom na to, že oni ti len poskytujú prostredie, ktoré môžeš používať. Ako aj nižšie uvidíš na príkladoch, nijaký prevádzkovateľ sociálnej siete ti nezaručí, že prostredie sociálnej siete bude bezpečné. Súčasne sú všetky sociálne siete poskytované zadarmo a ty ich môžeš používať dobrovoľne. Poďme sa bližšie pozrieť na niekoľko z nich.

Facebook[11] ťa vo svojich pravidlách používania upozorňuje na to, že nie je bez chýb a používaš ho na vlastné riziko. Ďalej sa dočítaš, že využívaš Facebook bez záruk a že nikto ti nezaručí, že bude vždy bezpečný, zabezpečený, bezchybný, ale-

bo že bude fungovať bez prerušenia, oneskorenia alebo nedostatkov. Poskytovateľ sociálnej siete Facebook nezodpovedá za obsah ani informácie, ktoré sú na tejto sociálnej siete prenášané a zdieľané. Nenesie zodpovednosť za žiaden urážlivý, neprimeraný, obscénny, protizákonný alebo inak napadnuteľný obsah, ani za žiadne informácie. Dokonca Facebook nenesie zodpovednosť za správanie žiadneho používateľa tejto sociálnej siete.

Ďalšou sociálnou sieťou je *Google+*[12]. Spoločnosť Google, ako jej prevádzkovateľ, vo svojich pravidlách uvádza, že nenesie žiadne záväzky týkajúce sa obsahu služieb, konkrétnych funkcií služieb, ich spoľahlivosti alebo dostupnosti. Služby sú poskytované bez záruk „tak, ako sú". Za aktivity prebiehajúce v tvojom účte na Google+ nesieš plnú zodpovednosť. Žiadnu škodu alebo stratu ti nik nenahradí.

V pravidlách sociálnej siete *Pokec*[13] sa dočítaš, že jej prevádzkovateľ neposkytuje používateľom záruku nepretržitej funkčnosti, bezchybnej činnosti a zabezpečenia. Súčasne nezodpovedá za akúkoľvek škodu, ktorá by mohla byť používateľovi spôsobená v súvislosti s používaním tejto sociálnej siete. Rovnako nezodpovedá za obsah príspevkov, ani za diskusie a ich obsah v chate na serveroch, za porušovanie autorských práv a ani iných práv používateľmi.

Možno si už nemyslíš, že sociálne siete sú úplne bezpečné. Ich tvorcovia však robia maximum, aby tomu tak bolo. Aj napriek tomu sa však v prípade výskytu problémov zbavujú všetkej zodpovednosti. Ťažko s tým môžeš sám niečo spraviť. Hoc nie všetko, čo je uvedené v pravidlách, aj platí, je dôležité, aby si pri používaní sociálnych sietí si toho bol vedomý a správal sa uvážlivo.

2.3 Čo môžem urobiť na svoju ochranu a na ochranu iných?

Veľmi dôležitou otázkou, ktorú si každý používateľ sociálnej siete položí, je: Môžem sa chrániť, ak niekto zasahuje do mojich práv na sociálnych sieťach? Odpoveď znie: Jednoznačne áno. Existuje niekoľko možností ochrany a v nasledujúcom texte si ich priblížime.

2.3.1 Ako si chrániť svoju osobnosť?

Ak sa domnievaš, že tvoje práva sú na sociálnej sieti ohrozované alebo porušované, máš možnosť brániť sa. Náš zákon (Občiansky zákonník) na takúto obranu upravuje viacero spôsobov. Na vyriešenie situácie je niekedy potrebné obrátiť sa

na skúsenejšiu osobu (starší kamarát, učiteľ, rodič) alebo vyhľadať odbornú pomoc (advokát polícia). Vždy si pamätaj, že je lepšie konať skôr.

Naopak, ak si niekto bude myslieť, že jeho práva porušuješ ty, nemusí to hneď znamenať, že ich naozaj aj porušuješ. Ak by si ich aj náhodou porušil, skús sa s ním dohodnúť. Niekedy úplne stačí, že sa tejto osobe ospravedlníš, alebo prestaneš robiť to, čím si jeho práva ohrozil. Ak by ťa zaujímalo, aké konkrétne právne kroky môžeš pri ohrození svojich práv vykonať, pozri si túto poznámku.[14]

A čo ak ma niekto *kritizuje*? Nie každá kritika sa považuje za narušenie tvojich práv. Ak je nepravdivá a neprimeraná, tak platí to, čo sme napísali vyššie. Naopak, ak je pravdivá a primeraná, tak takáto kritika sa nepovažuje za neoprávnený zásah. Napríklad kamarát napíše na sociálnej sieti, že neovládaš matematiku, alebo že nevieš dobre rozprávať anglickým jazykom. Ak je táto správa pravdivá a napísal to primeraným spôsobom, tak nedošlo k zásahu do tvojho dobrého mena a dôstojnosti.

Určite sa pýtaš, čo je primerané a čo už nie. Pre niekoho nebude primerané, ak o ňom napíšu, že jeho mladšia 5-ročná sestra (ktorá ešte nevie ani čítať) vie lepšie rozprávať po anglicky než on. Určite by nebolo primerané, ak by niekto o tebe tvrdil, že somár alebo cvičená opica vie lepšie matematiku než ty. V daných prípadoch kritika nie je podaná primeraným spôsobom. Primeraným spôsobom by bolo uvedenie, že nepoznáš dobre matematiku a je nutné, aby si si znovu prečítal knihy súvisiace s danou témou.

2.3.2 Čo mi musí sociálna sieť povedať o používaní mojich údajov?

Predtým, než začne prevádzkovateľ sociálnej siete o tebe spracúvať osobné údaje, je povinný ti *poskytnúť dôležité informácie* a poučiť ťa, ako bude od teba tieto údaje získavať a ako ich bude používať. Bohužiaľ, ak očakávaš nejaké okienko s informáciami, nedočkáš sa ho. Vo väčšine prípadov uvidíš pri registrácii zaškrtávacie políčko, ktoré je nutné zaškrtnúť, aby tvoja registrácia bola úspešne ukončená. Pri tomto políčku sú uvedené podmienky používania alebo niečo s podobným názvom. Veľmi málo používateľov číta tieto podmienky. Ak by si na nich klikol a prečítal si ich, zistil by si, že sa v rámci nich nachádza časť venujúca sa spracovaniu osobných údajov.

Dôležité je, aby ti prevádzkovateľ sociálnej siete ešte pred dokončením registrácie oznámil nasledujúce skutočnosti:

- *svoje identifikačné údaje*, najmä svoj názov (obchodné meno) a svoje sídlo;
- v prípade, ak registrácia prebieha na serveri, ktorý spravuje niekto iný, tak potom aj *identifikačné údaje* prevádzkovateľa tohto servera;
- na aký *účel* zbiera údaje, ktoré vypĺňaš pri registrácii, alebo ich neskôr vyplníš v rámci profilu. Vo väčšine prípadov uvedie, že ich potrebuje na prevádzku tebe poskytovaných služieb. Dôležité je si pozrieť, či prevádzkovateľ sociálnej siete neuvádza, že ich chce dať niekomu inému na komerčné použitie;
- *zoznam osobných údajov*, ktoré chce od teba zberať. Bližšie sme sa zaoberali osobnými údajmi v predchádzajúcej kapitole;
- *dobu***,** na ktorú prevádzkovateľ bude potrebovať tvoje údaje;
- *poučenie o tvojich právach*, ktoré si bližšie priblížime v ďalšej kapitole;
- *ďalšie informácie*;

Medzi *ďalšie informácie*, o ktorých by si sa mal pri registrácii dozvedieť, patrí napríklad totožnosť prevádzkovateľa. Tým môže byť odkaz na nejakú stránku alebo verejný register, kde si môžeš overiť, že naozaj ide o túto konkrétnu spoločnosť. Prevádzkovateľ sociálnej siete ťa pri registrácii nesmie zabudnúť poučiť o tom, že svoje osobné údaje dávaš *dobrovoľne*, čo znamená, že mu *dávaš súhlas*, aby s nimi pracoval a používal ich. Nezabúdaj však na to, že tento súhlas máš právo kedykoľvek vziať späť. Samozrejme, v tomto prípade nebudeš môcť naďalej používať služby danej sociálnej siete.

Okrem toho, že prevádzkovateľ sociálnej siete osobné údaje sám používa, v určitých prípadoch môže tieto údaje poskytovať iným osobám. Aj na toto musíš byť však pri registrácii upozornený.

A čo je ešte dôležitejšie, buď obozretný ohľadne zverejnenia tvojich osobných údajov. Isto by si nechcel, aby si nevedel nastaviť viditeľnosť niektorých údajov ostatným a mohol si tvoje osobné údaje čítať ktokoľvek, dokonca aj ten, kto na danej sieti nie je zaregistrovaný. Pekným príkladom v tomto smere je sociálna sieť Pokec. Verejné údaje v profiloch používateľov tejto sociálnej siete a verejné albumy si môže pozrieť prakticky ktokoľvek.

Pri registrácii si tiež všímaj, kde všade budú tvoje osobné údaje putovať. Je veľký rozdiel, či ostanú len na Slovensku, alebo ich prevádzkovateľ sociálnej siete posiela, alebo ukladá v rámci Európskej únie alebo iných krajín. V prípade posielania týchto údajov mimo Európsku úniu buď veľmi opatrný. V rámci Európskej únie sa uplatňujú prísne pravidlá spracovania osobných údajov a zabezpečenia súkromia. Z tohto dôvodu je tu lepšia bezpečnosť osobných údajov a nižšia pravdepodobnosť ich zneužitia.

U väčšiny sociálnych sietí dochádza k posielaniu osobných údajov mimo Európsku úniu. Je to spôsobené najmä tým, že väčšina z nich má sídlo mimo Európskej únie. Výnimkou je napríklad Facebook, ktorý má svoju pobočku v Írsku. Napriek tomu, že prevádzkovatelia niektorých sociálnych sietí (Google, Twitter) sídlia v USA, súhlasili s tým, že údaje od európskych používateľov budú spracúvať podľa pravidiel Európskej únie.[15]

Skús sa teraz opýtať sám seba, či to nie sú dôležité informácie? Ak by si tieto informácie vedel, asi by si inak pristupoval k tomu, aké osobné údaje vložíš do sociálnej siete. Ide o veľmi podstatné informácie a napriek tomu ich pri registrácii musíš hľadať. Bohužiaľ, toto je problém nielen sociálnych sietí, ale aj iných služieb poskytovaných cez internet. Pri registrácii odklikneme a odsúhlasíme všetko, napriek tomu, že si podmienky používania neprečítame.

2.3.3 Aké mám právne možnosti ochrany svojich osobných údajov?

Okrem už spomínaných informácií, ktoré ti musí prevádzkovateľ sociálnej siete poskytnúť, máš aj ďalšie práva na ochranu svojich osobných údajov. Najmä máš právo na základe písomnej žiadosti vyžadovať od prevádzkovateľa sociálnej siete informácie, alebo aby niečo vykonal v oblasti ochrany osobných údajov.

Základným právom je právo domáhať sa informácie, či *sú alebo nie sú spracúvané* tvoje osobné údaje. Ak sa osobné údaje o tebe spracúvajú, máš právo vedieť, *aké osobné údaje* o tebe spracúva sociálna sieť a najmä spôsob ich spracúvania. Je rozdiel, či tvoje údaje ostávajú na sociálnej sieti, alebo ich môže sociálna sieť poskytnúť ďalším spoločnostiam. Jedného dňa sa nenazdáš a zrazu máš e-mailovú schránku plnú e-mailov s ponukami liečivých výrobkov z Amazónie.

Ak ťa zaujíma, ako sa dostal prevádzkovateľ sociálnej siete k tvojim osobným údajom, môžeš sa ho na to opýtať. Je povinný presne uviesť *zdroj,* z ktorého získal

tvoje osobné údaje. Príkladom takéhoto zdroja môže byť aplikácia sociálnej siete v mobile (napr. pri GPS súradnice pri statuse).

Nezabúdaj na to, že prevádzkovateľ sociálnej siete ti musí tieto informácie poskytnúť vo *všeobecne zrozumiteľnej forme*. To znamená, že z toho, čo ti napíše, by si mal pochopiť, aké osobné údaje spracúva, ako ich získal a čo s nimi robí. Myslíme si, že odpoveď, ktorá ťa odkáže na podmienky spracúvania osobných údajov, nie je adekvátnou odpoveďou.

Ak sa ti stane, že na sociálnej sieti nájdeš nepravdivé, neúplné alebo neaktuálne osobné údaje, neváhaj a kontaktuj ho s tým, že chceš, aby to *opravil, resp. vymazal*.

Tvojim najdôležitejším právom je požadovať, aby prevádzkovateľ sociálnej siete *zmazal tvoje osobné údaje*. Pôjde o dva prípady. Prvým prípadom je tvoje rozhodnutie naďalej nepoužívať danú sociálnu sieť. V tomto prípade máš právo požadovať, aby prevádzkovateľ sociálnej siete zmazal tvoje osobné údaje. Pri registrácii si dal súhlas na spracovanie tvojich osobných údajov pre to, aby si mohol používať sociálnu sieť. Keď ju už nechceš používať, prevádzkovateľ sociálnej siete nemá právo takéto údaje o tebe uchovávať a naďalej používať.

Druhým prípadom je situácia, keď prevádzkovateľ sociálnej siete spracovaním tvojich osobných údajov porušuje zákon. Príkladom na takéto porušenie môže byť to, že ťa nesprávne poučil pri registrácii, spracúva o tebe osobné údaje, o ktorých si ani nevedel, alebo poskytoval tvoje osobné údaje niekomu inému bez tvojho súhlasu a pod.

V prípade, že si myslíš, že prevádzkovateľ sociálnej siete porušuje tvoje práva a nevyhovel tvojej žiadosti o informáciu, alebo aby niečo vykonal, môžeš sa obrátiť na *Úrad na ochranu osobných údajov Slovenskej republiky*.[16] Keďže Facebook má európsku pobočku v Írsku, sťažnosti na túto sociálnu sieť môžeš podať na úrad v Írsku podobný nášmu Úradu na ochranu osobných údajov - *Data Protection Commissioner*.[17]

3. Chráň svoje a cudzie výtvory

Pri používaní sociálnych sietí bežne používaš výtvory iných. Napríklad zdieľaš cudzie články z Topky.sk, videá z YouTube, odkazy na súbory na rôznych úložiskách ako DropBox alebo pesničky na Spotify. Tieto výtvory však nemožno používať úplne neobmedzene.

Napríklad, na článok môžeš odkázať, ale nemôžeš ho len tak prekopírovať do statusu svojej fanúšikovskej stránky, ktorú si vytvoril pre svojho domáceho miláčika. Táto časť knižky ti pomôže pochopiť, ako používať výtvory iných tak, aby si z toho nemal zbytočné problémy. Tiež ti pomôže odpovedať na otázku, čo môžu robiť ostatní ľudia s tvojimi vlastnými výtvormi. Dozvieš sa napríklad aj to, kedy sa tvoj vtipný remix obrázkov môže objaviť na bilbordoch v tvojom meste.

Ak chceš používať cudzí obsah, musíš si všeobecne dávať pozor najmä na dve veci – *tzv. autorské práva iných* a *ochranu ich osobnosti*.

Autorské právo dáva autorom fotografií, videí a iných diel právo vylúčiť z ich používania koho chcú, teda aj teba. Cieľom týchto práv ale nie je brániť použitiu daných diel. Naopak, cieľom je, aby si si s autorom za použitie jeho diela dohodol odmenu. Tým mu prispeješ na jeho ďalšiu tvorbu. Nie všetky použitia diela však podliehajú autorovmu súhlasu. Ktoré presne to sú, si uvedieme nižšie.

Taktiež je potrebné mať na pamäti, že cudzie výtvory, ktoré používaš, môžu obsahovať rôzne citlivé a osobné prejavy iných - ich zahanbujúce fotky alebo osobné emaily. Nemôžeš napríklad len tak vo svojom statuse alebo tweete citovať z osobného rozhovoru tvojho spolužiaka s jeho mamou, ktorého si bol svedkom. Na použitie *tzv. prejavov osobnej povahy,* ale aj *tzv. osobných údajov* preto vždy potrebuješ tiež súhlas dotknutej osoby[18]. Tak ako chceš, aby sociálna sieť a tvoji kamaráti rešpektovali tvoje súkromie, musíš aj ty rešpektovať to ich. Inak to nemôže fungovať.

Okrem autorského práva a ochrany osobnosti ešte môžeš naraziť na problém s *tzv. chránenými označeniami,* ako sú napríklad ochranné známky, neregistrované značky a pod. Ide o rôzne slová, obrázky, tvary alebo zvučky, ktoré buď z dôvodu registrácie alebo ich intenzívneho používania nemôžeš voľne používať na označovanie *svojich vlastných výtvorov*. Samozrejme, v zásade bez problémov ich môžeš použiť, ak chceš poukázať na výrobky pôvodného podnikateľa[19]. Spojenie Coca

Cola môžeš napríklad použiť na založenie fanklubu, nie však už na pomenovanie tričiek, ktoré chceš začať predávať v susedstve cez Facebook.

Tieto práva nemajú prirodzene len druhí, ale aj ty. I ty sám môžeš byť autor. Aj tvoje súkromie musia ostatní rešpektovať. Ak si autor, máš nárok na to, aby si od teba pýtali súhlas, keď chcú použiť tvoje výtvory. Niekedy to však môžu urobiť aj bez tvojho súhlasu, či dokonca proti tvojej vôli. Tieto prípady sa volajú tzv. **zákonné licencie**. Znamenajú, že zákon povolil niečo ostatným bez ohľadu na to, či s tým súhlasíš. Bez toho by nemohol fungovať svet. A ani tebe by sa to nepáčilo. Vieš si predstaviť, že by si si musel pýtať súhlas vždy, keď chceš niekoho citovať? Alebo vždy, keď chcete v škole v rámci predstavenia alebo vyučovania zahrať nejakú postavu z filmu? Asi nie.

Poďme však k jednotlivým otázkam, ktoré ťa zaujímajú.

3.1 Kedy a ako môže sociálna sieť použiť tvoj obsah?

Môže sa stať, že sa tvoj status objaví na bilboarde v tvojom meste? Áno, možné to je. Sociálna sieť si svojimi pravidlami môže zabezpečiť, že tvoje fotografie, či iný obsah bude používať v reklame alebo aj inak. Napríklad Facebook od teba chce, aby si mu dovolil používať tvoje fotografie, meno a priezvisko pre jeho reklamné kampane[20]. Pokec naopak nežiada, aby mohol ďalej použiť tvoj obsah. V prípade Twitteru je možné takmer všetko, napríklad tvoje fotografie a tweety môžu byť bežne použité v televíznych novinách alebo v inom spravodajstve[21]. Dávaj si preto pozor, čo zdieľaš.

Čo všetko môže sociálna sieť urobiť s tvojimi výtvormi závisí od toho, s čím si súhlasil v jej obchodných podmienkach. Vždy si preto poriadne pozri, aké oprávnenia (tzv. licencie) si od teba berú. Ak vieš po anglicky, môžeš si napríklad overiť niektoré služby na stránke www.tosdr.org.

3.2 Kedy a ako môžu iní používatelia použiť tvoj obsah?

Ostatní používatelia môžu použiť tvoje chránené diela len vtedy, ak to povoľuje zákon alebo si im to dovolil ty sám.

Nie každý výtvor je však chránený autorským právom. Na to musí byť dostatočne originálny[22]. Fotka tvojej neupratanej izby môže, ale nemusí byť chránená ako autorské dielo. Dôležité je, aby mala určitý originálny umelecký prvok. Chrá-

nená preto môže byť aj obyčajná fotka jedla, ak si ju dobre naaranžoval. Aj keď fotka nie je chránená ako autorské dielo, môžeš byť obmedzený v jej použití z dôvodov ochrany súkromia iných (pozri Kapitolu 2).

Chránené je len konkrétne vyjadrenie. Zákon nechráni myšlienku, spôsob, metódu, koncept, princíp, objav alebo informáciu, ktorá je vyjadrená, opísaná, vysvetlená, znázornená alebo zahrnutá do diela. Ak si na vyučovacej hodine vypočujete výklad napríklad o zimnom spánku medveďov alebo ako sa bojovalo počas 1. svetovej vojny, takýto popis nie je chránený autorským právom. Ale naopak, tvoje poznámky v zošite z tejto hodiny sú chránené.

Autorské práva vznikajú automaticky. Nie je potrebná žiadna registrácia alebo uvedenie ochranného znaku (c). Stačí, že dielo vytvoríš sám svojou vlastnou hlavou (napr. esej, myšlienka, ako bude vyzerať obraz alebo návrh počítačového programu) a nejakým spôsobom ho zhmotníš (napr. napíšeš na papier, nakreslíš na plátno, vyťukáš do klávesnice). Zo zákona tak získaš právo na udelenie súhlasu či na zakázanie používania tvojho diela. Tieto práva získavaš na celý svoj život a tvoji dedičia ešte aj na 70 rokov po tom, ak tu už nebudeš.

Ani nechránená fotka však nemôže byť použitá ledabolo inými. Ak fotka alebo video zachycuje tvoje osobné prejavy, ako napríklad spev v sprche, opaľovanie sa na záhrade, či len tvoju tvár, môže byť väčšinou použitá len s tvojim súhlasom. Je pritom jedno, že tvoj spev v sprche nie je dostatočne umelecký. Dôvod, prečo si iní musia pýtať súhlas, nie je autorské právo, ale ochrana tvojej osobnosti. Rovnako to platí aj pri osobných údajoch, ktoré sme vysvetlili v druhej časti tejto knižky.

Ak niekomu udelíš jednoduchý súhlas na použitie tvojho diela, môžeš ho aj kedykoľvek odvolať[23]. Ak ale uzavrieš s niekým zmluvu, podľa ktorej takýto súhlas udeľuješ, musíš najprv ukončiť platnosť tejto zmluvy[24]. Napríklad, ak kamarátovi len tak po telefóne dovolíš, aby si mohol dať na svoj plagát tvoju fotku, môžeš to kedykoľvek odvolať. Ak sa však dohodnete, že ti má dať niečo za to, alebo spíšete zmluvu, musíš sa riadiť dohodou.

Niekedy ľudia môžu použiť tvoj výtvor aj bez tvojho súhlasu. Je to vtedy, ak im to dovoľuje zákon. Napríklad, každý môže z tvojho diela niekedy voľne citovať, kopírovať ho pre osobnú potrebu alebo ho použiť na vyučovacie účely v škole[25]. Z verejných profilov na sociálnych sieťach môžu niekedy tvoje príspevky použiť aj v novinách[26]. A to bez ohľadu na to, či im to dovolí sociálna sieť. Dovoľuje im to zákon.

3.3 Kedy a ako môžeš ty používať obsah iných z internetu?

Nie všetko, čo je voľne dostupné na internete, môžeš aj neobmedzene zdieľať. Okrem legálnosti samotného obsahu, si dávaj predovšetkým pozor na autorské práva. Tie často obmedzujú možnosť šírenia cudzieho obsahu. Pri používaní cudzieho obsahu postupuj nasledovne. Ak používaš originálny výtvor iného, môžeš ho používať:

- **bez súhlasu autora** len obmedzene tak, ako to umožňuje zákon (tzv. **zákonné licencie**). Môžeš tak napríklad citovať, recenzovať alebo si z neho urobiť osobnú kópiu na svojom hardisku;
- takmer neobmedzene pri tzv. **voľných dielach**, čo sú originálne diela, ktoré boli kedysi chránené, no dnes ich ochrana už vypršala (uplynulo 70 rokov od smrti autora). Napríklad si môžeš stiahnuť a pustiť hudbu od Beethovena, Mozarta alebo akúkoľvek ľudovú hudbu. Aj pri týchto dielach však musíš dávať pozor na to, aby si neurážal zosnulého autora;
- len so **súhlasom autora** v prípadoch, ktoré nepatria k vyššie uvedeným zákonným licenciám alebo voľným dielam. V takých prípadoch však môže autor používanie jeho diela zakázať. Autor má právo najmä zakázať kopírovanie diela, jeho komunikovanie verejnosti distribúciu diela. Autora môže zastupovať aj niekto iný. Určite poznáš organizáciu SOZA. Tá zastupuje niektorých autorov hudobných diel. Nie však všetkých. Podobných organizácií je viacero;

Základné pravidlo je, že ak niečo robíš *verejne*, potrebuješ súhlas autora, ibaže by si chcel citovať, recenzovať alebo komentovať. Ak niečo robíš len v okruhu svojich blízkych priateľov, je to komplikovanejšie. Skúsme si teda najprv povedať nejaké príklady:

- *Zdieľanie hudby alebo filmov cez služby ako BitTorent* je vo väčšine prípadov protiprávne. Pri každom zdieľaní ponúkaš sám tieto diela verejnosti. Na to ale potrebuješ súhlas autora. Ak ho nemáš, porušuješ jeho práva. Ak hudba alebo film je voľné dielo, tak ho môžeš zdieľať cez BitTorent.
- *Sťahovanie hudby alebo filmov zo služieb ako Ulož.to* je vo väčšine prípadov protiprávne. Či to bude protiprávne alebo nie, závisí od legálnosti zdroja. Ak na Ulož.to nájdeš voľné dielo (napr. klasickú hudbu), alebo máš od autora súhlas (napr. video tvojho kamaráta), môžeš si ho stiahnuť. V opačnom

prípade (napr. najnovšie filmy idúce v kinách) síce pri každom stiahnutí neponúkaš nič verejnosti, no kopíruješ z tzv. nelegálneho zdroja. Kopírovať pre osobnú potrebu môžeš len z legálneho zdroja.

- *Kopírovanie knihy v školskej knižnici* je v poriadku. Nič neponúkaš verejnosti a kópiu vykonávaš z legálne dostupného zdroja, t. j. z knihy zakúpenej knižnicou. Skopírovať si však nesmieš celú knižku alebo jej podstatnú časť z hľadiska rozsahu[27]. 90 strán zo 100 stranovej knihy bude tvoriť podstatnú časť. Ak by si však vzal 30 strán, tak to nepovažujeme za podstatnú časť. Pri 40-50 stranách je ťažko povedať, či to je podstatná alebo nepodstatná časť knihy. Bude to veľmi závisieť od knihy, jej obsahu, o aké kapitoly ide a pod.
- *Kopírovanie obrázkov z internetu do tvojho počítača* je v zásade v poriadku. Vždy však hľadaj oficiálny zdroj. Stiahnuté obrázky môžeš použiť ako svoju plochu na počítači, vytlačiť si ich alebo zavesiť ich vo svojej izbe. Nemôžeš ich však zvyčajne verejne použiť napr. na tvojej webstránke.
- *Napáliť kamarátovi počítačový program* je protiprávne. Svoju kópiu môžeš používať len na svojom počítači. Nemôžeš z nej robiť ďalšie kópie pre iných, hoci aj kamarátov.

V nasledujúcej časti si uveďme niekoľko príkladov použitia obsahu na sociálnej sieti.

3.3.1 Môžem zdieľať videá z YouTube?

Áno. Použitie voľne dostupných videí z YouTube na tvojej nástenke, resp. časovej osi alebo účte nepodlieha súhlasu autora. Je pritom jedno, či máš verejný alebo súkromný profil. V takom prípade nezáleží ani na tom, či je video na YouTube legálne alebo nie[28].

Zdieľanie videí však môže porušovať aj iné zákony, než autorské. Protiprávny môže byť už samotný ich obsah. V zásade platí, že to, čo zákon zakazuje vytvoriť (napr. videá burcujúce k nenávisti medzi rasami, národmi a pod.), by si nemal ani zdieľať. Tvoje zdieľanie by mohlo byť chápané ako podporovanie týchto nepekných vyjadrení netolerancie. Ak zdieľaš videá preto, aby si ich verejne alebo medzi kamarátmi odsúdil, je dobré dať to najavo svojim komentárom, aby nevznikli pochybnosti, či s obsahom videa súhlasíš alebo jeho obsah odmietaš. Tvoje právo odsúdiť protiprávny obsah je kryté právom na slobodu prejavu.

3.3.2 Môžem použiť obrázky z webu?

Záleží to od toho, čo chceš s nimi presne robiť a či tvoj profil je verejný alebo súkromný. Súhlas autora je zvyčajne potrebný vždy, keď kopíruješ jeho výtvor alebo ho sprístupňuješ verejnosti.

Ak je tvoj profil uzatvorený len pre kamarátov, fotografie môžeš v zásade voľne používať bez súhlasu autora. Keďže ide o neverejný priestor, nesprístupňuješ dané dielo žiadnej verejnosti[29]. Tvoje kopírovanie musí byť ale obmedzené na osobné účely. Teda nesmieš na ňom zarábať.

Ak na tvoj profil majú prístup aj iné osoby, ako len kamaráti, uploadnutie obrázku na sociálnu sieť si bude vyžadovať súhlas autora. Tvoje kopírovanie už nie je osobné a výtvory sprístupňuješ aj verejnosti. Autor má preto nárok na odmenu. Z tohto dôvodu, keď chceš cudziu fotku použiť pre verejnú stránku na Facebooku, potrebuješ v zásade vždy súhlas autora. Výnimkou je, ak sa môžeš oprieť o jednu zo zákonných licencií.

Samozrejme, fotku môžeš použiť vždy, ak ti to dovolí autor, resp. ten, kto od neho prebral spravovanie jeho práv. Takou osobou môže byť organizácia kolektívnej správy ako napr. SOZA[30] alebo LITA[31]. Ak nájdeš článok s ilustračnou fotkou, ktorá sa automaticky kopíruje do náhľadu tvojho príspevku, nemusíš sa obávať. Prevádzkovateľ stránky súhlasil aj s takýmto použitím, keď zaviedol tlačidlo „páči sa mi“ pod svoje články. Vždy keď preto uvidíš toto tlačidlo pre svoju sociálnu sieť, nemusíš sa pri zdieľaní báť. Tento súhlas však nepokrýva prekopírovanie celého článku do tvojho verejného statusu.

3.3.3 Môžem odkazovať na akékoľvek stránky?

Ak je tvoj profil súkromný, tak v zásade áno. Ak je ale verejný, musíš si dať väčší pozor. Odkazovaním na nelegálny obsah zavesený na stránkach ako Ulož.to by si mohol porušiť práva autorov. Podobné platí i pre iný nelegálny obsah (napr. nenávistné videá). Ak vieš, že odkazovaný obsah je nelegálny, radšej naň neodkazuj. Predídeš tak problémom.

3.3.4 Môžem použiť cudziu hudbu vo svojom videu a to následne zverejniť?

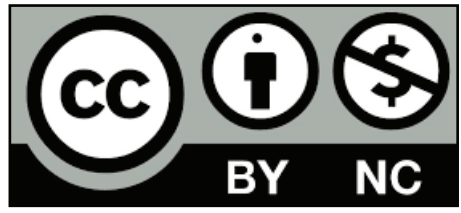
Hudba (bez ohľadu na to, či ide o klasickú skladbu alebo modernú pesničku) je tiež chránená ako dielo. Aj pri hudbe však platia tzv. zákonné licencie a možnosť použitia tzv. voľných diel, ktoré sme už v tejto knižke spomínali. V ostatných prí-

padoch potrebuješ na použitie hudby súhlas autora. Ak ho nemáš, môžeš použiť len jej drobnú časť. A to len vtedy, ak hudbu vo svojom videu komentuješ alebo recenzuješ. Bežný remix, bohužiaľ, dnes nie je v súlade s právom. Aj prípustnosť paródie je otázna. Existujú však riešenia, ako na to.

Použiť môžeš hudbu, ktorá je zverejnená pod *tzv. licenciami Creative Commons*. Ak pri tejto hudbe uvidíš symbol, pozri si pozorne, aké použitia sú dovolené:

- skratka [BY] znamená, že dielo môžeš ľubovoľne používať, ale musíš uviesť meno autora;
- skratka [NC] znamená, že dielo môžeš ľubovoľne používať, no len na nekomerčné účely;
- skratka [ND] znamená, že dielo môžeš ľubovoľne šíriť, ale nie upravovať;
- skratka [SA] znamená, že dielo môžeš ľubovoľne upravovať, ale tvoj vlastný odvodený výtvor bude musieť byť dostupný za rovnakých podmienok, ako pôvodné dielo;

Ak teda uvidíš hudbu pod licenciou „Creative Commons BY NC" (obrázok č. 6) znamená to, že ju môžeš ľubovoľne používať a upravovať, ale nesmieš tak robiť za účelom zárobku a musíš uviesť pôvodného autora. Napríklad na stránke http://www.google.sk/advanced_search v časti „práva na používanie" si môžeš vyhľadávať hudbu pod takou licenciou, ktorá zodpovedá tvojim potrebám.



Obr. č. 6 – Licencia Creative Commons BY NC

Ak pridáš na YouTube video, ktoré obsahuje hudbu, jej autori ťa namiesto odstránenia tohto videa môžu nechať tak. Ako protihodnotu za tolerovanie tvojho používania ich diel ale získajú časť odmeny z reklamy, ktorú by YouTube prípadne vyplatil tebe.

Môže sa však stať, že tvoje video bude nahlásené ako porušujúce autorské práva niekoho iného a YouTube ho stiahne. Ak sa tak stane, poraď sa so skúsenejším (rodič, učiteľ) alebo s odborníkom v danej oblasti. Môže sa stať, že si v skutočnosti

nikoho práva neporušil. V tom prípade máš možnosť nesúhlasiť s týmto nahlásením. Toto rozhodnutie so sebou ale môže niesť rôzne následky, ako napríklad odhalenie tvojej identity. Tým riskuješ súdny spor alebo zneužitie tvojich osobných údajov. Poraď sa preto vždy skôr, ako sa rozhodneš brániť svoje videá.

3.4 Kedy môžeš použiť na svojom účte cudzie chránené názvy?

Chceš založiť fanklub svojmu obľúbenému mestu alebo firme? Ich súhlas nepotrebuješ. Musíš však dbať na to, aby bolo jasné, že:

- ide len o neoficiálny fanklub;
- tvoje vyjadrenia nie sú vyjadrením mesta alebo firmy;

Pozor na to, ak si chceš zaregistrovať meno iného človeka, a teda nie firmy, ako názov svojho účtu. Možné to je, ak je človek verejne známy. Verejne známymi sú napríklad speváci, športovci alebo politici. Na druhej strane nemôžeš len tak vytvoriť účet pre svojho spolužiaka alebo učiteľa, ktorý si to neželá.

Aj v prípade verejných osôb musí byť tiež jasné, že účet nie je ich. Ak si účet nezriadil za účelom kritiky, recenzovania alebo parodovania, môžeš navyše prísť o účet. Osoby, ktorých meno si použil, môžu mať väčší záujem na tom, aby používali účet s daným menom ako ty.

3.5 Môžeš zodpovedať za obsah svojich spolužiakov?

Môžeš byť zodpovedný za to, čo robia iní na tvojej stránke na Facebooku? Áno, možné to je. Ak si napríklad zriadiš fanklub svojej školy alebo niektorého učiteľa s jeho súhlasom, musíš dávať pozor aj na to, čo tam budú písať druhí. Nemusíš sledovať každý príspevok, ale ak sa o nejakom nevhodnom dozvieš, či už oznámením od niekoho alebo pri čítaní komentárov, musíš konať. Odstráň komentáre alebo príspevky, ktoré môžu porušovať práva iných. Ak máš pochybnosť, konzultuj to so skúsenejším (rodič, učiteľ) alebo s odborníkom v danej oblasti. Priestor na vyjadrenie môžeš dať aj tomu, kto napísal príspevok. Urobíš tak lepšie rozhodnutie, keďže bude založené na viacerých informáciách.

Ak by si nelegálny príspevok neodstránil alebo ho nebodaj ešte propagoval ďalej, mohol by si byť spoluzodpovedný. Napríklad, ak by si propagoval príspevok s rasovou neznášanlivosťou. Vždy je dobré konzultovať so skúsenejším (rodič, učiteľ) alebo s odborníkom v danej oblasti, ak by si si nevedel poradiť. Najmä, ak ti šírenie obsahu môže privodiť trestnú zodpovednosť.

Ešte jedno upozornenie. Ak sa rozhodneš založiť si profil, aby si cez neho niečo predával alebo poskytoval, musíš na ňom uviesť základné informácie o tebe, kontaktné údaje a dozorný orgán[32]. Pri tom buď radšej opatrný, sociálne siete majú pre podnikateľov osobitné pravidlá, ktoré sú iné než pre obyčajných používateľov.

4. Chráň sa pred zneužívaním

Sociálne siete sú miesto, kde si ľudia vytvárajú svoje online profily a napĺňajú ich rôznymi osobnými informáciami, obrázkami a myšlienkami. Používajú ich najmä na komunikáciu, nadväzovanie nových priateľstiev, či udržiavanie tých existujúcich. Sociálne siete prinášajú ľudom mnoho pozitívneho. Zároveň však prinášajú aj veľa rizík. Nebezpečenstvo môže mať rôznu podobu. Jednak môže prichádzať vo forme škodlivého softvéru (napr. počítačový vírus) alebo vo forme škodlivého správania sa iných ľudí.

Jedným z najznámejších škodlivých konaní sú tzv. hackerské útoky. Pri hackerskom útoku dochádza k nedovolenému prieniku, resp. pokusu o prienik do tvojho počítača alebo profilu na sociálnej sieti. Hacker tak obchádza bezpečnostné opatrenia tvojho počítača alebo profilu a napríklad bez toho, aby mal tvoje heslo, sa snaží dostať do tvojho konta na sociálnej sieti.

Podvodné webové stránky, aplikácie či správy, ktoré sa šíria cez sociálne siete, sa snažia získať tvoje osobné údaje. Tie sú potrebné na to, aby ťa mohli následne zaplaviť nevyžiadanou reklamou, spamom, alebo z teba urobiť obeť podvodu. Mnohokrát sa snažia od teba vylákať prihlasovacie údaje do tvojho internetového bankovníctva alebo číslo tvojej platobnej karty, aby ťa mohli okradnúť.

Veľké nebezpečenstvo predstavuje aj komunikácia na sociálnych sieťach. Možno si ani neuvedomuješ riziká vyplývajúce z dôvery k cudzím ľuďom alebo aj zdieľania citlivých informácií s kamarátmi.

Mnoho ľudí využíva sociálne siete aj na zdieľanie intímnych fotografií. Nezdieľajú ich pritom len so svojimi priateľmi, ale aj s neznámymi ľuďmi. Neraz sa stáva, že po skončení kamarátstva sa fotografie ocitnú na verejných stránkach alebo profiloch. Tieto intímne fotky sú potom ľahko zneužité na zosmiešňovanie alebo vydieranie.

Ďalším súvisiacim rizikom je tzv. kyberšikana. Tá spočíva v urážaní, zosmiešňovaní alebo obťažovaní druhých. Šírenie kyberšikany je značne uľahčené modernými technológiami, akými sú napríklad sociálne siete, blogy, fóra alebo mobilné telefóny.

Materiály obsahujúce sex, násilie a extrémizmus sú na internete veľmi ľahko dostupné, a to aj v tých najdrsnejších podobách. Tento nebezpečný a nezákonný obsah je ďalšou nástrahou, s ktorou sa môžeš stretnúť na sociálnych sieťach.

Sociálne siete ponúkajú mnoho zaujímavých funkcií. Dokážu zjednodušiť život. Je však potrebné, aby si si uvedomoval nebezpečenstvá, ktoré súvisia s používaním sociálnych sietí. Ak sa v kľúčovej chvíli dokážeš správne zachovať, často dokážeš predísť početným problémom a nepríjemným situáciám. Účelom tejto kapitoly je pripraviť ťa na najčastejšie situácie, ktoré súvisia s používaním sociálnych sietí. Keďže konania ľudí v príkladoch uvedených v tejto kapitole sú protiprávne a často dokonca aj trestné[35], najlepšie urobíš, ak sa im úplne vyhneš.

4.1 S akým škodlivým softvérom a ako sa môžem stretnúť na sociálnych sieťach?

Škodlivý softvér (tzv. malware[34]) je počítačový program, ktorého úlohou je poškodiť, obmedziť, alebo získať kontrolu nad tvojim počítačom. Malware zahŕňa rôzne typy počítačových vírusov, ransomware, spyware, adware, keylogger a pod (viac ďalej). K tebe sa môže dostať cez email, SMS, WhatsApp alebo sociálne siete.

Cez sociálne siete sa škodlivý softvér šíri tak, že je „ponúkaný" najčastejšie cez nejaké lákadlo, napr. vtipné video, obrázok, zaujímavý nadpis článku alebo link na stiahnutie práve uniknutých intímnych fotiek celebrít. Po kliknutí na daný odkaz alebo súbor sa spustí škodlivý softvér a prenikne do tvojho počítača či profilu. Škodlivý softvér tak už môže v tvojom mene posielať správy tvojim priateľom, ktoré budú obsahovať link na jeho stiahnutie. Takto sa bude nekontrolovane šíriť ďalej.

Nepozornosťou, neznalosťou a nepremysleným klikaním na všetko, čo sa objaví na sociálnych sieťach, môžeš udeliť škodlivému softvéru povolenie na prístup k tvojmu účtu. Ten následne z neho získa tvoje údaje a použije ich ďalej. Keďže má prístupové práva k tvojmu účtu môže napr. uverejňovať „lákavé" príspevky na tvoju nástenku a tak sa šíriť medzi tvojimi priateľmi.

Škodlivý softvér je často maskovaný inými rozličnými programami. Na stiahnutie ti ponúknu napríklad nejaký antivírusový program (napr. antivírus 2014), či program na zrýchlenie tvojho počítača. Ak si ho stiahneš a nainštaluješ, do tvojho počítača sa dostane aj škodlivý kód. Preto musíš byť pri sťahovaní neznámych softvérov veľmi opatrný.

Tvorca škodlivého softvéru potom môže na tvojom počítači, či profile na sociálnej sieti, robiť čo bude chcieť. Môže napríklad zmeniť alebo vymazať údaje a tvoje heslá, zhromaždiť ich a následne preposlať ďalej. Môže deaktivovať bezpečnostné prvky tvojho počítača, vytvoriť si vzdialený prístup na tvoj počítač, odpočúvať ťa a sledovať tvoju izbu cez počítačovú kameru, alebo len jednoducho sledovať, čo robíš na počítači.

Čo konkrétny škodlivý softvér robí a čo je jeho cieľom, závisí aj od jeho druhu, ktorý zaútočí na tvoj profil alebo tvoj počítač.

Adware je akýkoľvek softvér, ktorý automaticky sťahuje, prehráva alebo zobrazuje reklamu v tvojom počítači alebo na tvojom profile na sociálnej sieti. Adware môže byť legálny, ale aj nelegálny. Legálny je vtedy, ak je napr. súčasťou určitého softvéru, ktorý je zdarma (freeware), kde cenou za to, že môžeš nejaký softvér používať zadarmo, je práve zobrazovanie reklamy. Obdobne to môže byť aj na sociálnej sieti, keď na to, aby si mohol hrať hru zadarmo, jej musíš napríklad povoliť zdieľanie statusov o tvojom postupe v hre na tvojej nástenke, čím si robí reklamu. To sa však deje s tvojim súhlasom. Naopak, nelegálny adware zobrazuje reklamy bez tvojho súhlasu. Do tvojho počítača alebo profilu sa zväčša dostal prostredníctvom počítačového vírusu, červa alebo iného škodlivého softvéru.

Obrázok č. 7 - Adware

Spyware je počítačový program, ktorý bez tvojho súhlasu a vedomia zhromažďuje a odosiela tvoje údaje (osobné údaje, fotografie, videa, návyky na internete, heslá). Bežnými funkciami spywaru je zbieranie snímok z tvojej obrazovky, fotenie okolia pomocou webkamery, nahrávanie zvuku cez mikrofón alebo iné sledovania tvojho konania. Napríklad tzv. keylogger[35], ktorý slúži najmä na odchytávanie tebou stlačených kláves na klávesnici (napr. na zistenie tvojho hesla). Údaje získané spywarom môžu byť použité na rôznu nelegálnu činnosť, ako napríklad na krádež tvojej identity alebo podvod.

Existujú prípady, kedy ty sám dáš súhlas na to, aby sociálna sieť mohla zhromažďovať rôzne údaje o tebe. Takýto súhlas udeľuješ najčastejšie pri registrácií nového konta. Pritom často súhlasíš aj s použitím tvojich údajov sociálnou sieťou, ako aj a ich poskytnutím ďalším podnikateľom.

Počítačový vírus a červ je škodlivý program, ktorý napadá súbory v tvojom počítači, ktoré potom maže alebo mení. Červy sa na rozdiel od vírusov dokážu počítačovou sieťou šíriť sami.

Ransomware je škodlivý program, ktorý obmedzí prístup do tvojho počítača alebo k tvojim súborom a žiada zaplatenie určitej sumy peňazí ako „výkupného" pre odblokovanie prístupu. Niektoré druhy ransomwaru zašifrujú údaje na celom disku, zatiaľ čo iné prístup iba blokujú.

Príkladom ransomwaru, je **CryptoLocker**, ktorý zašifroval dôležité súbory na počítači a za ich odšifrovanie žiadal „výkupné" vo výške 300 EUR/USD. Ak by si mu „výkupné" nezaplatil do nejakého času, zničil by kľúč potrebný k odšifrovaniu súborov. Na obrázku vidíš ako takáto správa môže vyzerať.

Obrázok č. 8 - Správa zobrazovaná CryptoLockerom

Tvorcovia škodlivého softvéru[36] veľmi radi využívajú sociálne siete na jeho šírenie, pretože sa na nich nachádza veľké množstvo ľudí, ktorí klikajú na kadečo, čo je pre nich zaujímavé bez toho, aby si uvedomovali riziká s tým spojené.

Škodlivý softvér je väčšinou nástrojom páchania trestnej činnosti a je často využívaný útočníkmi pri protiprávnych konaniach[37]. Škodlivým softvérom dochádza najčastejšie k porušeniu práva na súkromie, listového tajomstva, tajomstva prepravovaných správ, práva na ochranu osobných údajov a ochrany osobnosti (napr. ak ťa niekto sleduje spywarom a prípadne ďalej zverejňuje údaje o tebe alebo ich nejako zneužije), do vlastníckeho práva (napr. ak počítačový vírus vymaže tvoje údaje alebo ich ransomware zašifruje).

Tipy na ochranu pred škodlivým softvérom:

- Skontroluj si zoznam svojich „priateľov“ na Facebooku a na iných sociálnych sieťach. Koľko z tých ľudí sú ľudia, ktorých poznáš osobne a ktorým dôveruješ? Dôkladne si vyberaj, koho si pridáš za priateľa na sociálnej sieti, aby si tak minimalizoval vystaveniu sa týmto hrozbám.
- Dávaj si pozor na čo klikáš a čítaj poriadne, keď dávaš svoj súhlas rôznym aplikáciám na prístup k tvojim údajom v profile. Čomu nerozumieš, s tým nesúhlas, čo nepoznáš, to nesťahuj!

- Ak zistíš, že tvoj účet bolo napadnuté škodlivým softvérom, kontaktuj kamarátov, aby neklikali na podozrivé linky, ktoré im mohol program poslať cez tvoj účet. Tým zabrániš nákaze ďalších používateľov.
- Nainštaluj si program, ktorý dokáže rozoznať a blokovať škodlivý softvér. Zapni si firewall, prípadne iný program, ktorý monitoruje, aké údaje sú odosielané z tvojho počítača. Pravidelne aktualizuj svoj prehliadač a operačný systém.
- Pravidelne si zálohuj všetky tvoje údaje na samostatné pamäťové zariadenie, ktoré nie je pripojené k sieti alebo k počítaču (USB, externý disk a pod.).

4.2 Prečo by niekto hackoval môj účet na sociálnej sieti?

Hacking v kontexte sociálnych sietí možno charakterizovať ako neoprávnené preniknutie do tvojho konta, profilu. To sa môže uskutočniť napr. za použitia malwaru, teda určitého škodlivého softvéru, ako aj za použitia tzv. sociálneho inžinierstva, kedy ide skôr o psychologickú hru využívajúcu informácie v profile na získanie tvojej dôvery.

Pri sociálnom inžinierstve ťa chcú zmanipulovať tak, aby si niečo urobil (napr. spustil nejaký škodlivý softvér) alebo aby od teba získali určité informácie (napr. prístupové údaje do profilu na sociálnej sieti). **Sociálne inžinierstvo** môže prebiehať osobne (v reálnom svete) alebo prostredníctvom komunikačného prostriedku (napr. telefón, email, rýchle správy).

Príkladom sociálneho inžinierstva v kontexte sociálnych sietí môže byť, ak sa niekto predstaví ako zamestnanec Facebooku a na overenie tvojej totožnosti ťa požiada o prihlasovacie meno alebo heslo. Prípadne opačná situácia, ak by niekto kontaktoval Facebook, pretože zabudol heslo do svojho účtu (v skutočnosti by to bol však tvoj účet) a žiadal, aby mu bolo zaslané alebo povedané nové heslo. Takéto situácie sa nestávajú a takmer s určitosťou ide o podvodníkov.

Sociálne inžinierstvo sa môže robiť aj tzv. **phishingom** (čítaj fišingom, „rybárčenie"). Phishing je spôsob podvodného získania osobných a citlivých údajov. Útočník sa snaží získať tvoje údaje (napr. prihlasovacie meno, heslo, číslo platobnej karty) vydávaním sa za dôveryhodnú osobu cez email či správu. Typickým príkladom je, ak by ti napr. došla správa na Facebook, ktorá vyzerá, ako by bola priamo od Facebooku, v ktorej budeš požiadaný o aktualizáciu údajov k účtu prostredníctvom webovej stránky, na ktorú odkazuje pôvodná spáva. Zvyčajne sa

v správe tiež nachádza varovanie typu, že ak si neaktualizuješ údaje, tvoj účet bude zmazaný. Webové stránky, kde máš vykonať aktualizáciu údajov, často vyzerajú (takmer) identicky so skutočnou stránkou. Ak na tejto stránke uvedieš svoje údaje, tak tie potom môžu byť zneužité na prístup do tvojho účtu, alebo na páchanie ďalšej trestnej činnosti (napr. neoprávnené použitie finančných prostriedkov z tvojej platobnej karty, rozosielanie škodlivého softvéru).

Aj keď si myslíš, že údaje a fotografie, ktoré zdieľaš, nie sú ničím výnimočné, hacker ich dokáže zneužiť a použiť proti tebe. Preto buď pri zdieľaní vždy opatrný. Aj jedna informácia v zlých rukách môže spôsobiť veľa nepríjemností.

Informácie ako dátum a miesto narodenia, rodné meno matky, prvý domáci miláčik, ktoré sa často bez väčších problémov dajú zistiť z tvojho profilu, bývajú zvyčajne použité ako bezpečnostné otázky na overenie identity, napr. pri strate hesla alebo pre zablokovanie platobnej karty. Mnoho ľudí si práve kombináciou podobných základných informácií vytvára heslá. Ak máš takéto údaje verejne dostupné alebo sa niekto k nim dostane, môžu byť ľahko zneužité.

Sociálne siete ponúkajú možnosť v profile nastaviť, aby (všetky, prípadne len niektoré) údaje o tebe mohli vidieť všetci, priatelia tvojich priateľov, len tvoji priatelia, alebo iba ty. Ak si zvolíš, aby tvoje údaje videli len tvoji priatelia, musíš dbať na to, koho si pridáš za priateľa. Ak si pridávaš aj ľudí, ktorých nepoznáš vôbec alebo len veľmi málo, tak opäť ohrozuješ svoje údaje a vystavuješ sa tak riziku, že si do svojej „siete" pustíš hackera, ktorý vaše priateľstvo zneužije. Veľa ľudí, ak dostane správu od priateľa obsahujúcu link, tak naň bez rozmyslenia kliká. Zrejme si myslia, že ich priateľ im nemôže poslať nič zlé. Prekvapením potom je, ak link neposlal v skutočnosti ich priateľ a po kliknutí na odkaz budú presmerovaní na stránku, ktorá obsahuje škodlivý softvér.

Ak hacker chce len získať tvoje osobné údaje a všetky pre neho užitočné informácie sú dostupné tvojim priateľom, tak sa nemusí prácne dostávať do tvojho konta, ale stačí mu, ak sa stane tvojim priateľom. Niekedy môžu hackerovi stačiť aj informácie dostupné len tvojim priateľom. Preto pozor aj na žiadosti o priateľstvá od osôb, ktorých nepoznáš a s ktorými nemáš žiadnych spoločných známych.

Hacking je zvyčajne trestný[38] a dochádza pri ňom k zásahu do viacerých práv. To však záleží od toho, čo vlastne hacker s tvojim počítačom a tvojimi údajmi spraví. Právo na súkromie je narušené, už keď dôjde k preniknutiu do tvojho účtu. Právo na ochranu osobných údajov je narušené, ak dôjde k šíreniu alebo zverej-

ňovaniu údajov o tebe. Týmto zároveň dôjde aj k narušeniu listového tajomstva a tajomstva prepravovaných správ. Ak niekto používa tvoj hacknutý profil na urážanie iných, písanie neslušných komentárov a statusov v tvojom mene, môže tak dochádzať k zásahom do tvojho práva na ochranu osobnosti (napr. k zásahom do tvojho mena, tvojej dobre povesti, cti a dôstojnosti).

Tipy na ochranu pred hackingom:

- Dobre zváž, aké údaje o sebe uverejníš. Ak toho zverejníš príliš veľa, môžeš poskytnúť útočníkovi dostatok informácií na to, aby sa dostal do tvojho konta, či zistil tvoje heslo.
- Dôsledne si nastav vo svojom profile bezpečnostné prvky a urči, ktoré údaje môžu byť viditeľné verejnosti, ktoré len priateľom tvojich priateľov, ktoré len priateľom a ktoré len tebe.
- Nepoužívaj rovnaké heslo na všetky sociálne siete, lebo ak útočník zistí heslo na jednu sociálnu sieť, bude mať ihneď prístup aj k ostatným tvojim profilom.
- Neprihlasuj sa na rôzne stránky cez kontá na sociálnej sieti, ale stále si vytvor nový účet na danej stránke. Je to síce zdĺhavejšie, ale bezpečnejšie, pretože ak niekto získa prístup ku tvojmu kontu na sociálnej sieti, bude mať automaticky prístup aj na tieto stránky.
- Ak sa niekto neoprávnene dostal do tvojho konta alebo ho používal, okamžite si zmeň heslo. Pamätaj, že heslo by malo byť dostatočne dlhé a malo by sa skladať z písmen, číslic a znakov. Ideálne je, ak máš do každého konta iné heslo.
- Ak bol tvoj účet hacknutý, informuj všetkých svojich priateľov, že môžu dostávať „spamové" správy, ktoré sa budú tváriť, že prichádzajú z tvojho účtu. Upozorni ich, aby neotvárali tieto správy a neklikali na žiadne odkazy, pretože môže ísť o škodlivý softvér.
- Ak sa nemôžeš prihlásiť do svojho účtu, pretože hacker na ňom zmenil heslo, obráť sa okamžite na prevádzkovateľa sociálnej siete a postupuj podľa jeho pokynov.

4.3 Moje meno, priezvisko, fotografie, ale nie môj profil. Čo to má znamenať?

Na sociálnych sieťach používaš na komunikáciu a zdieľanie informácií s inými tzv. profil. Tam sa nachádzajú základné údaje o tebe a ide vlastne o tvoju vlastnú identitu. Môže sa však stať, že osoba, s ktorou komunikuješ, si vytvorila účet na sociálnej sieti a použila cudziu identitu alebo sa nejakým spôsobom dostala do účtu inej osoby (napr. hacknutím). V takýchto prípadoch možno hovoriť o tzv. krádeži identity (identity theft).

Krádež identity sa teda dá jednoducho definovať, ako vydávanie sa za niekoho iného pomocou jeho súkromných, osobných informácií za účelom finančného zisku, alebo ako neoprávnené používanie osobných údajov za akýmkoľvek iným účelom.

Informácie, ktoré možno zneužiť, sú všetky informácie a doklady, na základe ktorých je možné niekoho identifikovať a následne získať neoprávnené výhody. Údajom, ktorý možno zneužiť, môže byť napr. meno, rodné číslo, dátum narodenia i číslo občianskeho preukazu alebo platobnej karty. Zneužiť sa rovnako dajú aj tzv. biometrické údaje, ako odtlačky prstov alebo záznam tvojho hlasu. Rovnako opatrne je potrebné zaobchádzať aj s PIN-kódmi a inými identifikačnými číslami.

Overiť si identitu osoby v reálnom svete je pomerne ľahké pomocou rôznych dokladov, ako je rodný list alebo občiansky preukaz. Vo virtuálnom svete však nie je nikde garantované, že osoba s určitou virtuálnou identitou, je aj reálne touto osobou. Niektoré digitálne informácie, akými sú heslá, čísla účtov, prihlasovacie mená a pod. sa nemusia považovať za prvky reálnej identity, avšak môže ísť o dôležité identifikačné prvky virtuálnej identity, prostredníctvom ktorých sa možno dostať k osobným údajom. Preto je potrebné byť pri narábaní s nimi veľmi opatrný, aby nedošlo k ich vyzradeniu neoprávnenej osobe.

A čo sa stane, ak ukradnem identitu na sociálnej sieti? Ak si myslíš, že sa budeš vydávať za niekoho iného a nič sa nestane, mýliš sa. Predstav si prípad, že niekto vytvorí profil, ktorý bude popisovať teba. Aby tento profil pôsobil realisticky, páchateľ použije tvoje fotografie, videá, statusy, komentáre a samozrejme informácie, ktoré máš zverejnené na sociálnych sieťach, prípadne inde na internete. Ak si svoje údaje nechrániš, takáto nepravá identita sa dá vytvoriť celkom jednoducho: vy-

tvoríš účet s informáciami, ktoré nájdeš voľne dostupné na viacerých sociálnych sieťach. Tak sa dá ľahko vytvoriť profil, ktorý vyzerá, ako keby bol tvoj.

Možno si už počul aj o tzv. nigérijskom liste. Ide o podvodný email alebo správu, v ktorej sa páchateľ pokúša získať tvoje osobné údaje pod rôznou zámienkou, ako napr. vyplatenie výhry v lotérii, vyplatenie dedičstva po tvojom ujovi, ktorý žil v Afrike a nikdy si o ňom nepočul a iné podobné vymyslené situácie, ktoré zvyčajne lákajú na získanie nejakých peňazí.

Ďalším spôsobom vykonania krádeže identity je získanie elektronických údajov, cez ktoré sa prihlasuješ do sociálnych sietí (napr. heslá, loginy, odpovede na kontrolné otázky, atď.). Tento spôsob je pre páchateľa jednoduchší, keďže všetky informácie o tebe, tvoje fotografie, videá, statusy, správy a históriu má k dispozícii a nemusí presviedčať tvoje okolie o tom, že si to ty.

Elektronické údaje môže páchateľ získať aj neoprávneným kopírovaním údajov. Ak používaš školské počítače, počítače v práci alebo v kaviarňach na prihlasovanie sa do sociálnych sietí, buď v tomto smere obozretný. Na tomto počítači môže byť nainštalovaný spyware. Útočník môže získať tvoje údaje aj phishingom alebo pomocou sociálneho inžinierstva. Ak sa ti napríklad stalo, že administrátor sociálnej siete chcel od teba tvoj login a heslo, tak ver tomu, že niekto sa pokúsil cez „psychologickú hru" od teba získať prihlasovacie údaje. Administrátor nikdy od teba nepotrebuje tvoje prihlasovacie údaje. Nemá dôvod ich od teba pýtať. Ak ti príde správa alebo email, v ktorom ich od teba žiada, nereaguj. Pre páchateľa najľahší spôsob získania tvojho účtu je neoprávnené preniknutie do tvojho účtu (tzv. hacking). Sociálne siete obsahujú niekoľko bezpečnostných opatrení voči hackingu – napr. obmedzený počet pokusov o prihlásenie, zaslanie e-mailu o prihlásení do tvojho konta a pod.

Účelom krádeže identity môže byť napr.:

- získanie finančných prostriedkov a tovaru, služieb alebo iných výhod alebo vyhýbanie sa dlhom;
- poškodenie dobrého mena alebo povesti;
- vylákanie a sexuálne zneužitie obete;

Príkladom krádeže za účelom podvodu je prípad ženy, ktorá na sociálnej sieti Pokec vystupovala pod vymyslenou identitou slobodnej matky s dcérou, ktorej zomrel manžel i rodičia pri autonehode. Žena sa skontaktovala s jedným mužom a postupne mu uviedla, že má nedostatok finančných prostriedkov a potrebuje

peniaze na základné životné potreby. Tiež napísala, že potrebuje peniaze na lieky, mlieko, škôlku pre jej dcéru (tá bola tiež vymyslená) a na vyplatenie pôžičky po jej zomrelých rodičoch. Takýmto spôsobom postupne od tohto muža vylákala finančné prostriedky v celkovej výške približne 33 430 €. Keďže sa obohatila takým spôsobom, že uviedla iného do omylu, bola právoplatne odsúdená za trestný čin podvodu na podmienečné 2 roky trestu odňatia slobody.[39]

Ako príklad krádeže identity, kedy dochádza k znevažovaniu osoby, môžeme uviesť prípad ženy, ktorej intímne fotografie boli zverejnené na sociálnej sieti Facebook. Páchateľ vytvoril fiktívny účet a fotoalbum, do ktorého dal päť intímnych fotografií tejto ženy (bola vyfotená nahá v kúpeľni). Tento páchateľ bol právoplatne odsúdený na trest povinnej práce v trvaní 100 hodín a súčasne dostal povinnosť sa tejto žene osobne ospravedlniť.[40] V tomto prípade sa dopustil trestného činu poškodzovania cudzích práv (§ 376, § 377 trestného zákona).

Ak je účelom vytvorenej kradnutej identity vylákanie a sexuálne zneužitie obete, tak možno hovoriť o tzv. kybergroomingu. Kybergrooming je psychická manipulácia prostredníctvom internetu, vrátane sociálnych sietí s cieľom získať dôveru obete, vylákať ju na osobné stretnutie a spravidla sexuálne zneužiť. Páchateľ si na sociálnej sieti vytipuje zraniteľnú a ľahko dostupnú obeť. Signálom pre neho je práve veľké množstvo zverejnených osobných údajov, fotografie, ochota ku komunikácii s neznámymi, vysoká miera dôverčivosti, rýchle otváranie citlivých tém. Páchateľ väčšinou oslovuje súčasne väčšie množstvo detí a hľadá také, ktoré prejavia záujem a vyhovujú jeho potrebám (blízkosť bydliska, malá kontrola zo strany rodičov, ale aj chýbajúce kamarátske vzťahy alebo problémy doma, ako napríklad prebiehajúci rozvod rodičov). S tými potom rozvíja komunikáciu ďalej. Chce si dieťa získať tak, aby za ním prišlo dobrovoľne. Väčšinou postupne prizná, že je od neho starší, aj keď si môže vek prispôsobiť. Svoju stratégiu stavia na tom, že sa pre dieťa stane starším kamarátom, ochrancom, ponúka mu bezpečie a uznanie. Obeťami kybergroomingu sa najčastejšie stávajú deti, ktoré začínajú viac chodiť na internet, používať chat a sociálne siete, pričom nepoznajú ich nástrahy a nebezpečenstvá.

Ak by sa ti stalo, že ti niekto posiela nevhodné správy, ktorých cieľom je vylákať ťa na neznáme miesto, nikdy na takéto stretnutie nechoď. Zo zdanlivo peknej zámienky na stretnutie sa môžu vyvinúť rôzne nebezpečné situácie.

Známym príkladom kybergoomingu v ČR je kauza Pavla Hovorku (PH). Ten sa zoznamoval s maloletými chlapcami na rôznych internetových zoznamkách (sociálnych sieťach) a vystupoval aj ako sponzor detských domovov. Svoje obete lákal k sebe na vrátnicu (pracoval ako strážnik), kde ich pohlavne zneužíval. Pri odmietaní osobného stretnutia PH svoje obete vydieral hrozbou zverejnenia fotografií, ktoré mu predtým chlapci sami dobrovoľne poslali, či šírením správ o ich údajnej homosexualite, atď. PH bol obvinený z trestných činov[41], nakoniec odsúdený na 6,5 roka vo väzení a bola mu nariadená sexuologická liečba.[42]

Krádež identity sa nestáva len vo filmoch. Aj v našich končinách je žiaľ známych viacero prípadov, kedy k takejto krádeži identity došlo a pre obeť to malo vážne následky. Obeťou sa môžeš stať aj ty, pričom o tom nemusíš ani vedieť, alebo to zistíš až neskôr. Riziká môžeš znížiť len tým, že budeš pri nadväzovaní nových priateľstiev opatrný a pred tým, ako sa novému virtuálnemu priateľovi s čímkoľvek zdôveríš, ho najprv dobre spoznáš.

Pri krádeži identity dochádza najmä k zneužitiu osobných údajov, teda k zásahu do práva na ochranu osobných údajov, s čím zvyčajne súvisí aj zásah do práva na súkromie. Páchateľ sa tak dopustí trestného činu neoprávneného nakladania s osobnými údajmi (§ 374 trestného zákona). Ak popri tom napríklad aj šíri nepravdivé údaje, ktoré môžu ohroziť vážnosť obete, prípadne jej spôsobiť ujmu, môže sa dopustiť trestného činu ohovárania (§ 373 trestného zákona). Príkladom je prípad 19-ročnej dievčiny z Bánoviec nad Bebravou, ktorá ohovárala inú ženu na Pokeci[43]. Založila si nick sexuologicka2, pridala si k nemu fotky tejto ženy a jej rodiny a následne ponúkala sexuálne služby. Tým, že si toto dievča ukradlo cudziu identitu, všetko, čo napísala na sociálnej sieti, sa spájalo s inou ženou, u ktorej to spôsobilo problémy v rodine a u spoluobčanov. Bola odsúdená na 12 mesiacov s podmienečným odkladom na jeden rok. Toto dievča najprv ukradlo identitu inej ženy a potom prostredníctvom tejto kradnutej identity sa dopustila trestného činu ohovárania.

Tipy ako si chrániť svoju identitu:

- neposkytuj žiadne informácie o sebe a iných osobách telefonicky alebo internetom cudzej osobe, ktorá ich žiada, ak ju vopred nepoznáš;
- nevyplňuj žiadne podozrivé formuláre a ani neodpovedaj na podozrivé emaily a správy, ktoré ti sľubujú nejakú výhru, či veľký obnos peňazí;

- ak si na stránke, kde udávaš svoje osobné údaje, skontroluj si, či stránka používa zabezpečené pripojenie (https);
- nastav si zasielanie upozornení cez Google Alerts (návod nájdeš v 5. kapitole) alebo inú podobnú službu, keď sa na internete objaví nejaký nový obsah, v ktorom sa spomína tvoje meno;
- dodržuj rovnaké zásady, ktoré platia pri hackingu, pretože aj hacknutím sa možno dostať k tvojim osobným údajom;

4.4 Je v poriadku, ak ma niekto neustále uráža a zosmiešňuje?

Takéto správanie nie je v žiadnom prípade v poriadku. Ak ťa niekto dlhodobo úmyselne uráža, vyhráža sa ti, zosmiešňuje ťa, alebo ťa obťažuje prostredníctvom elektronických prostriedkov (napr. sociálnych sietí, e-mailov), dopúšťa sa tzv. kyberšikany (niekedy sa používajú aj cudzie výrazy cyberbulling, kyber-mobbing, e-mobbing). Sociálne siete sú pre kyberšikanu takmer ideálne prostredie, a to najmä pre to, že páchateľ má k nim kedykoľvek a kdekoľvek prístup, je v anonymite a môže ľahko a rýchlo šíriť rôzny obsah veľkému počtu osôb.

Tieto príklady ti pomôžu lepšie rozpoznať tzv. kyberšikanu:

- štipľavé a vulgárne komentovanie profilu obete, jej fotografií a statusov;
- zverejňovanie nevhodných zosmiešňujúcich alebo ponižujúcich videí a fotografií na nástenke obete;
- uverejnenie súkromných fotiek a videí (väčšinou s erotickým obsahom) bývalých partnerov po rozchode, aby došlo k zahanbeniu obete na verejnosti;
- zakladanie nenávistných skupín zameraných proti konkrétnej osobe;

Ku kyberšikane môže dôjsť aj neoprávneným preniknutím do cudzieho profilu (hacking) alebo vytvorením falošného profilu obete niekým iným (krádež identity). Páchateľ potom môže v mene obete šikanovať iného alebo šikanovať samotnú obeť (napr. rozosiela nepravdivé urážajúce správy, vkladá nevhodné fotografie a videá a pod.)

Páchateľom kyberšikany sa môžeš stať aj neúmyselne. Takáto situácia môže nastať vtedy, ak neodhadneš dôsledky svojho konania a napríklad unáhlene zverejníš nevhodné fotky, urazíš niekoho, alebo si neuvedomíš, čo môže pre druhého znamenať nemiestny vtip.

Hoci reakciu obete nevidíš hneď, často ani nezistíš, čo si svojimi zraňujúcimi slovami alebo fotkami spôsobil[44]. Kyberšikana je veľmi nebezpečná a môže mať dlhodobé škodlivé dôsledky na osobnosť obete.

Ak ťa niekto dlhodobo prenasleduje, obťažuje, vyhráža sa ti alebo tvojim blízkym osobám tak, že máš pri tom strach, ide o stalking, čiže nebezpečné prenasledovanie. Zneužívanie internetu, resp. sociálnych sietí na prenasledovanie sa označuje ako cyberstalking. Cyberstalking sa považuje za jednu z foriem kyberšikany. Je natoľko závažná, že je trestným činom.[45]

Kyberšikana nie je sama o sebe trestným činom ani priestupkom. Avšak jej prejavmi (nátlak, vydieranie, vyhrážanie) dochádza k výrazným zásahom do viacerých základných práv a slobôd. Preto jej prejavy môžu byť viacerými trestnými činmi:

- **Účasť na samovražde** (§ 154 trestného zákona) – napr. úmyselné podporovanie obete v tom, aby vykonala samovraždu.
- **Porušenie dôvernosti ústneho prejavu a iného prejavu osobnej povahy** (§ 377 trestného zákona) – napr. zverejnenie e-mailovej komunikácie z počítača obete.
- **Ohováranie** (§ 373 trestného zákona) – napr. vytvorenie skupiny na Facebooku s cieľom zosmiešňovať obeť, kde sa budú uvádzať nepravdivé informácie, ktoré môžu obeť vážne poškodiť.
- **Poškodzovanie cudzích práv** (§ 376, § 377 trestného zákona) – napr. páchateľ oklame obeť tak, že pri chatovaní predstiera, že je niekto iný a spôsobí jej tým vážny problém (napr. v rodinných vzťahoch).
- **Nebezpečné vyhrážanie** (§ 360 trestného zákona) – napr. zasielanie takých výhražných správ, ktoré spôsobia, že obeť sa bude báť o svoj život alebo zdravie.
- **Vydieranie** (§ 189 trestného zákona) – napr. páchateľ núti obeť k šikanovaniu ďalšej osoby alebo vykonaniu iného činu. V opačnom prípade zverejnení jej intímne fotografie.
- **Šírenie toxikománie** (§ 174 trestného zákona) – napr. výsmešné poznámky na sociálnych sieťach o drogovej abstinencii obete za tým účelom, aby obeť opäť užila drogy.

Je vhodné, ak sa kyberšikana najprv rieši neformálne s rodičmi alebo v škole. Ešte predtým, ako sa problémom začne zaoberať polícia. Ak máš pocit, že sa k tebe niekto správa tak, ako bolo vyššie popísané, neváhaj a vyhľadaj odbornú pomoc (napr. rodičia, učiteľ). Byť obeťou kyberšikany nie je nič, pre čo by si sa mal hanbiť a trápiť sa. Práve naopak, čím skôr sa tento problém začne riešiť, tým je to lepšie aj pre teba.

Tipy na ochranu pred kyberšikanou sú obdobné, ako sme ich uvádzali v časti venujúcej sa hackingu a krádeži identity.

4.5 Môžem zasielať alebo zdieľať fotografie intímneho charakteru?

Zasielanie elektronických správ (sms, mms, e-mailov, správ na sociálnych sieťach atď.) či zdieľanie materiálu s erotickým a sexuálnym podtextom sa označuje ako **sexting**. Ide o sexuálne orientované komentáre, odhalené fotografie a videá. Sexting sa vyskytuje hlavne u dospievajúcej mládeže. Mladí ľudia často odosielajú svoje fotografie a videá s očakávaním obdivu. Neuvedomujú si, že sa týmto vystavujú vysokému riziku vydierania, nátlaku, verejného posmechu, sexuálneho obťažovania či sexuálneho útoku. Tento materiál môže na internete kolovať niekoľko rokov a môže byť použitý aj oveľa neskôr, čím môže teba alebo inú blízku osobu vážne ohroziť v súkromnom i pracovnom živote.

Sexting podporuje šírenie pornografie mladistvých a detí, ktoré je celosvetovo zakázané. Aj v Slovenskej republike už bol zaznamenaný rad prípadov sextingu. Viacero z nich možno posudzovať práve ako šírenie detskej pornografie.

Materiály zhotovené v rámci sextingu sa často radia práve do tzv. detskej pornografie[46]. Je dôležité upozorniť, že dieťa je podľa Trestného zákona osoba mladšia ako 18 rokov (nie 15!). Paradoxom je, že osoby staršie ako 15 rokov môžu mať „legálne" sex[47], avšak nesmú sa pri tom fotografovať či natáčať (do 18 rokov). Potom by sa mohlo jednať o výrobu a držanie detskej pornografie. Akékoľvek zneužívanie detí na výrobu pornografických materiálov je trestné, rovnako ako aj šírenie alebo vlastnenie takýchto materiálov.

Príkladom zneužitia materiálu zo sextingu je zverejnenie obrovskej databázy súkromných fotografií a videí zachytených zo Snapchatu hackermi, ktoré boli zbierané po celé roky. Princíp Snapchatu spočíva v tom, že odoslaná fotografia či video sa po prečítaní príjemcom hneď odstráni. Táto služba je preto často využívaná práve na zasielanie si intímnych fotografií. Keďže až 50 % používateľov Snapchatu tvo-

rí mládež vo veku 13 - 17 rokov, uniknuté fotografie a videá môžu byť potenciálne klasifikované ako detská pornografia. Toto je tiež dobrým príkladom na to, aby sa rozplynula tvoja predstava o nenarušiteľnosti súkromia na sociálnych sieťach.

Iným príkladom je prípad Veroniky, ktorá sa v roku 2007 cez sociálnu sieť dohodla na stretnutí s Petrom. Po stretnutí si s ním ešte pravidelne dopisovala a vymenila aj niekoľko intímnych fotiek. Keď Veronika po pár mesiacoch ukončila kontakt s Petrom, začali jej hromadne vyvolávať ďalší neznámi muži. Peter z pomsty zavesil jej fotky na erotickú zoznamku.

Tipy na ochranu pre zneužitím tvojej intímnej fotografie, či videa:

- Nevyhotovuj a nezasielaj svoje intímne fotografie a videa nikomu, lebo nevieš kto, kedy a ako ich môže zneužiť proti tebe.
- Ak máš vyhotovený takýto materiál a chceš si ho ponechať, tak ho maj dobre zašifrovaný, aby sa k nemu nemohol len tak hocikto dostať.

4.6 Čo je poplašná správa? Môžem ju šíriť po sociálnych sieťach?

Poplašnou správou je taká nepravdivá správa, ktorá môže vyvolať obavy a znepokojenie z nejakých budúcich udalostí. Správa musí byť nepravdivá, teda musí byť v rozpore so skutočnosťou, alebo musí túto skutočnosť aspoň značne skresľovať. Poplašná správa zároveň musí nepriaznivo zasiahnuť do života iných. Šírenie poplašnej správy je však potrebné odlišovať od tvojho vlastného hodnotenia situácie, alebo od kritiky určitého zariadenia.[48]

Určite si si už na internete niekedy prečítal správu s nepresnými, skresľujúcimi informáciami, účelovo upravenými polopravdami. Takéto správy označujeme ako „Hoax“[49]. Hoax varuje pred neexistujúcim nebezpečenstvom a napriek svojej nezmyselnosti vyzýva na to, aby bol preposielaný ďalším užívateľom sociálnych sietí. Oklamaný, resp. zavedený užívateľ sociálnej siete ho s vierou, že ide o pravdivú informáciu, šíri ďalej. Tak sa potom táto nepravdivá správa šíri medzi ľuďmi neuveriteľnou rýchlosťou. Jednoduchosť a prakticky nulová cena a námaha pri preposielaní spôsobila jeho veľký rozmach.

To, či je Hoax trestný alebo nie, závisí od obsahu správy. Ak obsahuje poplašnú správu, je trestným. Naopak, preposielanie hoaxu nie je trestným, ak dopad informácií nie je natoľko závažný, aby vyvolal obavy, znepokojenie, či nepriaznivo zasiahol do života ľudí.

Príkladom hoaxu, ktorý je len neškodnou fámou a nie je trestným, je nasledujúci „oznam", ktorý sa začal šíriť sociálnou sieťou Facebook tesne pred tým, ako malo dôjsť k zmene pravidiel tejto sociálnej siete:

OZNAM ... pre istotu dávam všetkým na vedomie... V reakcii na novú politiku FB vás informujem, že všetky moje osobné údaje, ilustrácie, kresby, články, karikatúry, obrázky, fotografie, videá, atď., sú predmetom mojich autorských práv (v súlade s Bernským dohovorom).

Pre komerčné využitie všetkých vyššie uvedených predmetov autorského práva je v danom prípade vyžadovaný môj písomný súhlas!

FB je teraz verejná spoločnosť. Preto sa všetkým používateľom sociálnej siete odporúča umiestniť na svojich stránkach podobné „oznámenie o súkromí", inak (ak toto oznámenie nebolo na internetových stránkach aspoň raz zverejnené), je automaticky umožnené využívať vaše osobné údaje, vaše fotografie a informácie uverejnené v správach na stránkach vášho profilu.

...

Každý, kto číta tento text, ho môže skopírovať na svoj profil na FB. Vďaka tomu budete chránení autorským zákonom.

Touto správou informujem Facebook o tom, že šírenie, kopírovanie, využívanie mojich osobných údajov, alebo akejkoľvek inej akcie vo vzťahu k môjmu profilu na sociálnej sieti, je bez môjho povolenia zakázané. Tento zákaz sa vzťahuje aj na zamestnancov, študentov, agentov alebo akýkoľvek iný personál, ktorý je týmto alebo iným spôsobom zmluvne spojený s Facebookom.

Hoax však môže vyzerať natoľko vierohodne, že vážne znepokojí aspoň časť obyvateľstva, pričom postačuje, že páchateľ spôsobí len nebezpečenstvo vážneho znepokojenia. Tak šírením tohto hoaxu dôjde k spáchaniu trestného činu šírenia poplašnej správy (§ 361 trestného zákona).

Ďalším príkladom hoaxu je napr. zaslanie poplašnej správy agentúrou AP cez Twitter: „*Blesková správa: Dva výbuchy v Bielom dome a Barack Obama je zranený.*" Táto poplašná správa však nebola dielom agentúry AP, ale výsledkom hackerského útoku na účte agentúry na sociálnej sieti Twitter. Dôsledkom tohto hoaxu bola okamžitá panika na burze, čo spôsobilo prepad akcií v súhrnnej hodnote 136,5 miliardy dolárov.[1]

Ak prídeš do kontaktu s takouto správou, nešír ju radšej ďalej. Vytvorenie a šírenie vierohodne vyzerajúcej nepravdivej informácie môže mať nemalé dôsledky na práva určitej (zvyčajne väčšej) skupiny ľudí, ktorá s nim príde do styku. Ak by si šíril poplašnú správu a súd by ťa za to uznal vinným, môžeš dostať trest odňatia slobody až na 2 roky.

4.7 Aký obsah sa na internete považuje za nebezpečný a nezákonný? Ako mi môže škodiť?

Za nebezpečný a nezákonný obsah možno považovať taký obsah, pred ktorým sa treba chrániť a ktorý je často aj v rozpore s našimi zákonmi. Za taký považujeme najmä obsah, ktorý propaguje drogy a obchodovanie s nimi, nenávistné komentáre voči ľuďom z odlišných skupín, propaguje rasistické a xenofóbne názory, popiera holokaust, propaguje anorexiu a bulímiu, pornografiu, či obsah, ktorý podnecuje a podporuje sebapoškodzovanie a samovraždy. Do nebezpečného a nezákonného obsahu patrí aj násilný obsah zobrazujúci napr. brutálne videá hraných scénok, ale aj reálne napadnutia, alebo skutočné udalosti s tragickým koncom, týranie zvierat, mučenie, popravy. Existujú dokonca špecializované portály, ktoré zhromažďujú takýto násilný obsah.

Tento obsah sa šíri na sociálnych sieťach prostredníctvom zasielania správ, vytvárania skupín alebo siete užívateľov vytvárajúcich a/alebo propagujúcich určitý druh tohto materiálu, zdieľania statusov, obrázkov, videí. Je to veľmi jednoduché a zvyčajne na to stačí pár kliknutí. Užívatelia sa cítia byť anonymní (v závislosti od sociálnej siete a reálnosti profilu), čo povzbudzuje ich odvahu. Táto anonymita je však iba relatívna, lebo v prípade začatia trestného stíhania sa polícia ku konkrétnym páchateľom dopátra.

Takýto nelegálny obsah môže byť škodlivý najmä pre deti, ktoré si nie sú vedomé nelegálnosti a škodlivosti takéhoto obsahu. Často práve ich nevedomosť môže byť zneužitá na to, aby sa stali súčasťou nejakej skupiny zaoberajúcej sa týmto nelegálnym obsahom. Príkladom sú extrémistické skupiny, ktoré sa pokúšajú zviditeľniť a propagovať svoje názory, ideológiu či samotné extrémistické hnutie (skupinu) a naverbovať tak nových členov. Sociálne siete predstavujú ideálny prostriedok na vykonávanie tejto ich nelegálnej činnosti. Nelegálny obsah typu detská pornografia, videá zobrazujúce rôzne sexuálne úchylky, týranie zvierat,

či extrémne násilie páchané na nevinných obetiach, je veľmi škodlivý. Môže mať vplyv aj na tvoj ďalší psychický alebo morálny vývoj.

Príkladom zo Slovenska je 20-ročná Lucia, ktorá dlhodobo trpela depresiami. Z tohto dôvodu sa v roku 2010 neúspešne pokúsila o samovraždu. Zistila, že ona sama sa zabiť nedokáže. Príliš sa bála toho, že by sa jej to nepodarilo. Rada preto prijala návrh Mateja Č., s ktorým sa zoznámila na internete. Ten jej ponúkol, že ju zabije tak, aby nič necítila. Cez chat sa dohodli na všetkých podrobnostiach a presnom dátume stretnutia. Ich posledný rozhovor je z 1. septembra 2010. O deň neskôr, po stretnutí s Matejom Č., Lucia zmizla. Jej telo našla polícia 15. mája 2011.

Ako sme už spomínali, tento obsah je často protizákonný až trestný. Príkladom je, ak niekto utýra zviera na smrť, dopustí sa tak trestného činu týrania zvierat a následne uverejní na sociálnej sieti video, na ktorom to bude zachytené. Zasielaním násilných videí deťom sa možno dopustiť trestného činu ohrozovania mravnej výchovy mládeže (§ 211 trestného zákona), pretože tým môže byť narušený mravný vývoj dieťaťa.

4.8 Čo robiť, ak zistíš, že tvoj profil alebo údaje o tebe boli zneužité?

V predchádzajúcom texte sme si povedali, s akými nástrahami a nebezpečenstvom sa môžeš stretnúť na sociálnych sieťach. Čo však robiť, ak zistíš, že niekto zneužíva tvoj profil, tvoje osobné údaje či dokonca teba samého. Postup môžeme vo všeobecnosti zhrnúť do týchto krokov:

1. **Okamžitá reakcia.** Akékoľvek protiprávne konanie treba riešiť okamžite. Sama sa daná situácia nevyrieši. Čím dlhšie situáciu nechávaš neriešenú, tým sa môže zhoršovať a jej následky môžu byť závažnejšie.
2. **Nekomunikuj s páchateľom.** S páchateľom nekomunikuj, nič mu nevysvetľuj, nepresviedčaj ho, pretože to nemá žiaden zmysel. Páchateľ by akurát mohol po sebe zahladiť stopy. Navyše, môže ísť o naprogramovaný softvér alebo o osobu z opačnej strany planéty, ktorá ti nebude rozumieť, resp. ti nebude chcieť rozumieť.
3. **Zabezpeč dôkazy.** Môžeš napríklad spraviť screenshoty[51], uložiť obrázky a správy. Všetko to pomôže pri vyšetrovaní tohto činu a odhaľovaní páchateľa.
4. **Bráň sa.** Ak si myslíš, že určitým protiprávnym konaním bol spáchaný trestný čin, využi svoje zákonné právo a podaj trestné oznámenie.

5. **Vyhľadaj odbornú pomoc.** Ak sám nevieš posúdiť, aké právne dôsledky má určité konanie, resp. čoho všetkého sa môžeš domáhať a ako sa máš brániť, tak vyhľadaj odbornú pomoc advokáta, prípadne mimovládnej organizácie[52], ktorá sa takýmito problémami zaoberá. Tieto subjekty ti pomôžu pri bránení a vymáhaní tvojich práv. Ak ešte nie si plnoletý, požiadaj o pomoc rodiča alebo učiteľa. Isto nie je dôvod hanbiť sa.
6. **Nahlás a žiadaj zablokovanie údajov, resp. profilu, ktorými dochádza k zásahom do tvojich práv.** Využi dostupné možnosti a požiadaj prevádzkovateľa danej sociálnej siete o zablokovanie falošného profilu, či odstránenie nevhodného príspevku. Mnoho sociálnych sietí má dnes veľmi jednoduché postupy na „nahlásenie" takýchto incidentov.

5. Ako sa môžem chrániť priamo na sociálnej sieti?

Právne prostriedky ochrany sú veľmi dôležité, ale v niektorých prípadoch chvíľu potrvá, kým sa dočkáš výsledkov. Z tohto dôvodu je dobré poznať aj niektoré možnosti v rámci sociálnych sietí, ako sa dá chrániť voči zásahom do ľudskej osobnosti a osobných údajov. Nižšie si podľa sociálnych sietí ukážeme niektoré z nich.

Táto kapitola je doplnená obrázkami jednotlivých nástrojov, odkazov alebo iných častí sociálnych sietí. Odkazy na návody alebo nástroje sú vytvárané pomocou nástroja *Google url shorter*[53]. Väčšina obrázkov priamo obsahuje *QR kód*[54] s odkazom na adresu daného nástroja alebo návodu.

5.1 Facebook

5.1.1 Ako si nastavím súkromie na Facebooku?

Najprepracovanejšie nastavenie súkromia má sociálna sieť Facebook. Základné nastavenia súkromia nájdeš v hornej lište (obrázok č. 9). Ak klikneš na ikonku súkromia, tak sa ti zobrazí „Rýchle nastavenie súkromia".

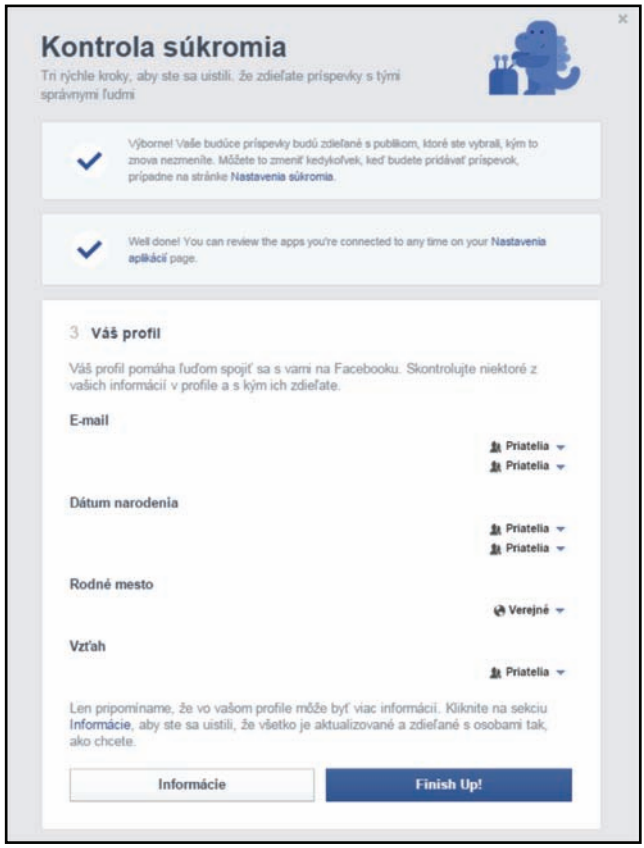
Obrázok č. 9 – Ikonka nastavenia súkromia na Facebooku

Základné nastavenie súkromia si upravíš, ak klikneš na 1. ponuku – „Kontrola súkromia". Tu si nastavíš súkromie v troch krokoch:

- **1. krok – „Vaše príspevky"** (obrázok č. 10) – v tomto kroku si môžeš nastaviť, kto uvidí tvoje príspevky. Ide o príspevky, ktoré pridávaš v hornej časti Noviniek alebo cez svoj profil.
- **2. krok – „Vaše aplikácie"** (obrázok č. 10) – v tomto kroku si vieš nastaviť aplikácie, v ktorých si prihlásený pomocou Facebooku. Môžeš zmeniť, kto vidí tieto aplikácie a tiež všetky budúce príspevky, ktoré táto aplikácia vytvorí za teba. Dokonca môžeš odstrániť aplikácie, ktoré už nepoužívaš.

Obrázok č. 10 – 1. a 2. krok nastavenia súkromia na Facebooku

- **3. krok – „Váš profil“** (obrázok č. 11) – v tomto kroku si nastavuješ, kto a aké informácie o tebe môže vidieť. Vo svojom profile môžeš mať aj viac informácií. Klikni na sekciu Informácie, aby si sa uistil, že všetko je aktualizované a zdieľané s osobami tak, ako chceš.



Obrázok č. 11 – 3. krok nastavenia súkromia na Facebooku

5.1.2 Čo mám urobiť, keď sa mi nepáči obsah, v ktorom som označený?

Isto sa ti už stalo, že tvoji priatelia na sociálnej sieti Facebook v dobrej viere označili na nelichotivých fotkách (napr. z párty) alebo sa o tebe zmienili v príspevkoch, ktoré by si si radšej nechal pre seba (napríklad príspevky o kolegoch, učiteľoch). Ak ti teda prekáža príspevok, v ktorom si označený, môžeš označenie odstrániť, alebo požiadať osobu, ktorá ťa označila, aby fo-

tografiu alebo príspevok odobrala. Nahlásenie na sociálnej sieti Facebook urobíš nasledovne:

- na svojej časovej osi presuň kurzor myši nad daný príspevok a klikni na ⌄;
- z rozbaľovacej ponuky vyber možnosť Nahlásiť / Odobrať označenia;
- vyber možnosť „Chcem odobrať toto označenie u príspevku" alebo „Chcem odobrať označenie svojou osoby z fotky";
- vyber možnosť odobrať označenie, alebo požiadaj o odňatie značky osobu, ktorá fotografiu zdieľa;

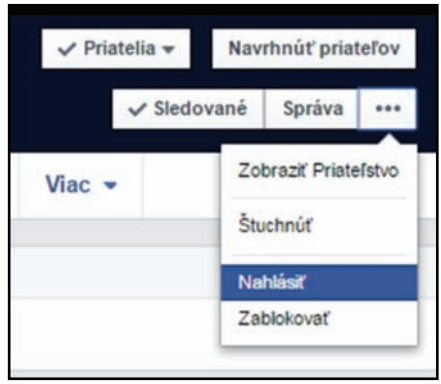
5.1.3 Ako môžem nahlásiť nevhodný alebo urážlivý obsah na Facebooku?

Obsah, ktorý porušuje pravidlá používania sociálnej siete Facebook, poskytovateľ tejto sociálnej siete odstráni. Ide napríklad o nahotu, šikanovanie, realistické vyobrazenie násilia alebo spam. Ak na Facebooku narazíš na niečo, čo tieto pravidlá porušuje, použi **odkaz pre nahlásenie** vedľa daného príspevku alebo fotky a odošli hlásenie. Je možné, že na sociálnej sieti Facebook uvidíš niečo, čo sa ti síce nepáči, ale pravidlá tejto siete to v skutočnosti neporušuje. Ak narazíš na niečo, čo by si radšej nevidel, máš tieto možnosti:

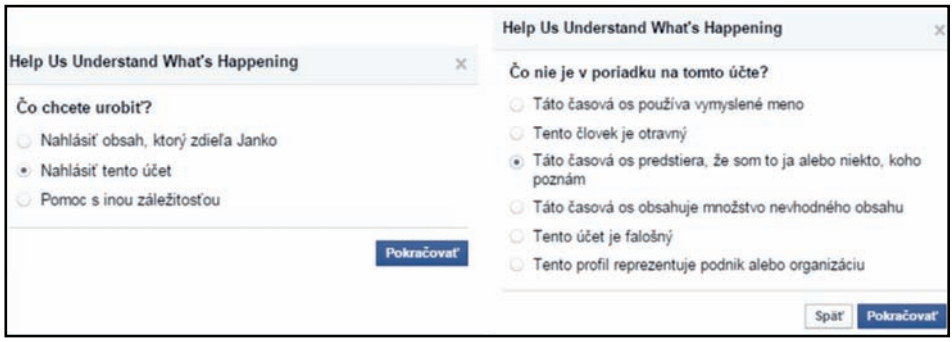
- skryť daný obsah z vybraných príspevkov;
- odoslať správu príslušnej osobe, ktorá posiela obsah, ktorý ťa obťažuje a požiadať o jeho odstránenie;
- odobrať z priateľov alebo zablokovať príslušnú osobu;

5.1.4 Ako sa chrániť v prípade krádeže identity na Facebooku?

Ak sa na tejto sociálnej sieti niekto vydáva za teba, alebo ak sa stretneš s falošným používateľom, máš možnosť to nahlásiť priamo prevádzkovateľovi Facebooku. Urobíš to tak, že v profile používateľa klikneš na nahlásiť (obrázok č. 12). Následne vyberieš možnosť „Nahlásiť tento účet". Potom máš k dispozícii dve možnosti, a to buď „táto časová os predstiera, že som to ja alebo niekto, koho poznám" alebo „tento účet je falošný".



Obrázok č. 12 – Možnosť nahlásenia krádeže identity v sociálnej sieti Facebook

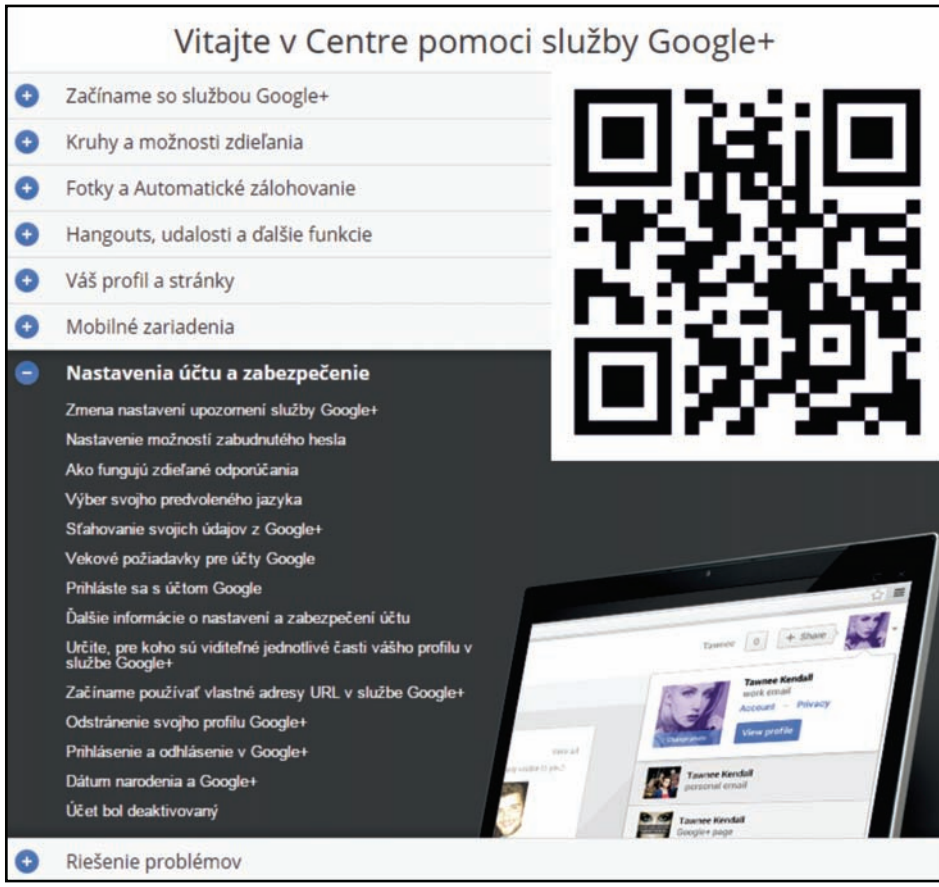


Obrázok č. 13 – Nahlásenie krádeže identity v sociálnej sieti Facebook

5.2 Google+

5.2.1 Ako si nastavím súkromie na Google+?

Informácie k nastaveniu súkromia a bezpečnosti účtu na Google+ nájdeš v „Centre pomoci služby Google+" (obrázok č. 14). Toto centrum nájdeš na webovej adrese: https://support.google.com/plus alebo http://goo.gl/3pFUTi.

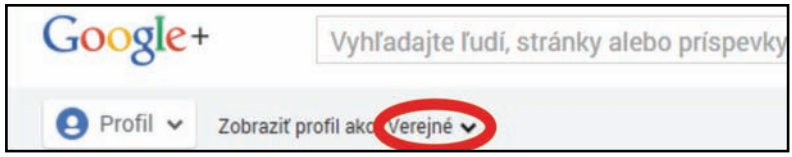


Obrázok č. 14 – Centrum pomoci služby Google+

Najdôležitejšou časťou Centra pomoci služby Google+ je „Nastavenie účtu a zabezpečenie". V rámci týchto nastavení nájdeš aj tieto odkazy:

- *Zmena nastavení upozornení služby Google+* - na tomto odkaze vieš nájsť návody na nastavenie upozornení týkajúcich sa tvojho profilu a obsahu, ktorý zverejníš (http://goo.gl/sxWJDT).

- *Ďalšie informácie o nastavení a zabezpečení účtu* – informácie týkajúce sa sťahovania svojich údajov z Google+, nastavenie možnosti zabudnutia hesla, zapnutie alebo vypnutie nahlasovania polohy pre iOS zariadenia, zdieľanie polohy a iné (http://goo.gl/h93h7l).
- *Určite, pre koho sú viditeľné jednotlivé časti vášho profilu v službe Google+* - tvoje meno a tvoja profilová fotografia sú vždy verejné. Ale veľa častí profilu však môžeš nastaviť tak, aby sa zdieľali iba s niektorými ľuďmi (http://goo.gl/YYCUl6). Stačí, ak si zobrazíš svoj profil a potom v ľavom hornom rohu klikneš na rozbaľovacie menu a zvolíš si „Zobraziť profil ako: verejné" (obrázok č. 15). Takto uvidíš to, ako verejnosť vidí tvoj profil.



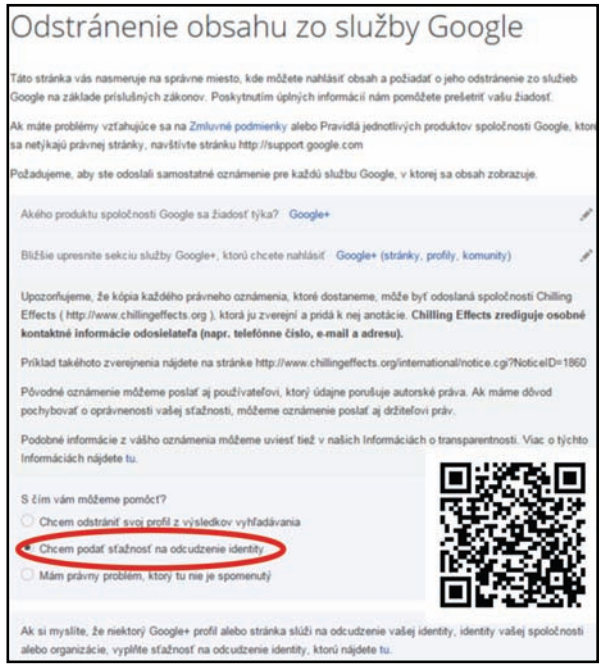
Obrázok č. 15 – Nastavenie zobrazenia profilu na sociálnej sieti Google+

- *Odstránenie svojho profilu Google+* je možné urobiť na tomto odkaze https://plus.google.com/downgrade. Dobre si prečítaj, čo sa maže a čo ostáva na sociálnej sieti Google+.

5.2.2 Ako sa chrániť na Google+?

Google na stránke podpory používateľom uvádza, že ak si na sociálnej sieti **Google+** narazil na obsah, ktorý môže porušovať zákon, máš informovať spoločnosť Google, ktorá daný materiál dôkladne prešetrí a zváži jeho zablokovanie, odstránenie alebo k nemu zamedzí prístup.

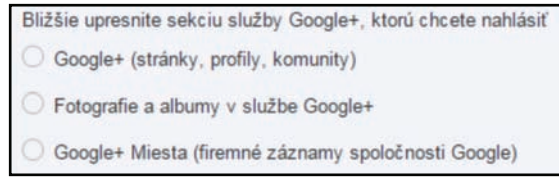
Google v rámci svojich služieb vrátane sociálnej siete Google+ využíva **nástroj na odstránenie obsahu zo služby Google**[55]. Úvodnú obrazovku nástroja môžeš vidieť na obrázku č. 16.



Obrázok č. 16 – Nástroj na odstránenie obsahu v sociálnej sieti Google+

Keď sa už nachádzaš na tejto úvodnej obrazovke, klikni na Google+. Zobrazí sa ti ponuka, ako môžeš vidieť na obrázku č. 17. Už si len zvolíš, ktorej oblasti sa tvoje nahlásenie týka:

- **Google+** zvolíš v prípadoch, ak máš podozrenie z krádeže identity, alebo máš právny problém;
- **fotografie a albumy v službe Google+** zaškrtneš, ak pôjde o porušovanie tvojich autorských práv, alebo ak obrázky porušujú nejaké súdne rozhodnutie alebo znázorňujú sexuálne zneužívanie detí;
- **Google+ Miesta** môžu využiť firmy, ktorých problémy súvisia s využívaním tejto služby;



Obrázok č. 17 – Sekcie na odstránenie obsahu v sociálnej sieti Google+

5.2.3 Ako sa chrániť v prípade krádeže identity na Google+?

Sociálna sieť **Google+** v rámci už spomínaného nástroja na odstránenie obsahu zo služby Google umožňuje podanie sťažnosti na odcudzenie identity (obrázok č. 18).

Obrázok č. 18 – Nástroj na odstránenie obsahu v sociálnej sieti Google+

5.2.4 Ako môžem nahlásiť nevhodný alebo protizákonný obsah na Google+?

Obsah, ktorý porušuje pravidlá používania sociálnej siete Google+, spoločnosť Google odstráni. Ide napríklad o protizákonný obsah, nevhodné príspevky, profily, fotografie alebo videá. Nahlásiť môžeme aj problém s autorskými právami. Konkrétne návody a odkazy nájdeš na webovej stránke http://goo.gl/2cLyA7 (obrázok č. 19).

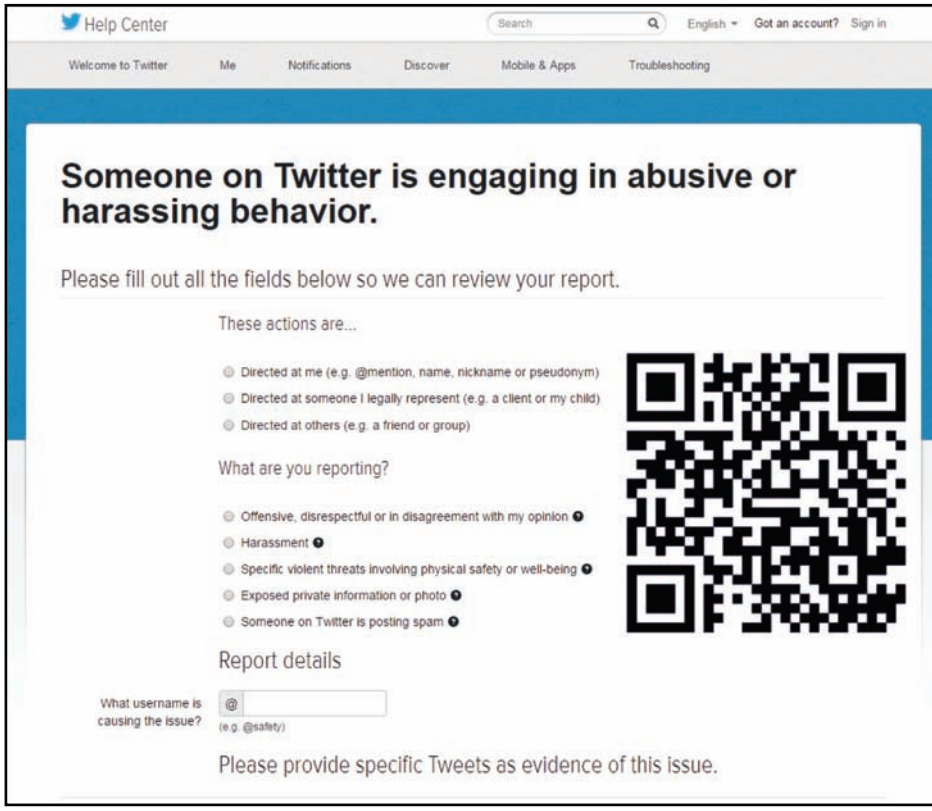
Obrázok č. 19 – Nahlásenie spamu, zneužitia alebo nevhodného obsahu v sociálnej sieti Google+

5.3 Iné spôsoby ochrany

5.3.1 Môžem sa brániť na Twitteri?

Odpoveď je áno. Môžeš využiť formulár na nahlásenie problému v rámci systému podpory (help center), ktorý sa nachádza na adrese https://support.twitter.com/forms/abusiveuser alebo http://goo.gl/nnkdv0 (obrázok č. 20). Samozrejme, prevádzkovateľ sociálnej siete Twitter automaticky nezmaže príspevok, ani neurobí nejaké kroky bez predošlého preskúmania. Tento formulár môžeš použiť v situácii, keď:

- nájdeš príspevok, ktorý ťa uráža;
- niekto ťa obťažuje;
- niekto sa ti vyhráža fyzickým násilím;
- nájdeš zverejnené svoje osobných údaje alebo fotografie bez tvojho súhlasu;
- niekto rozposiela spam;

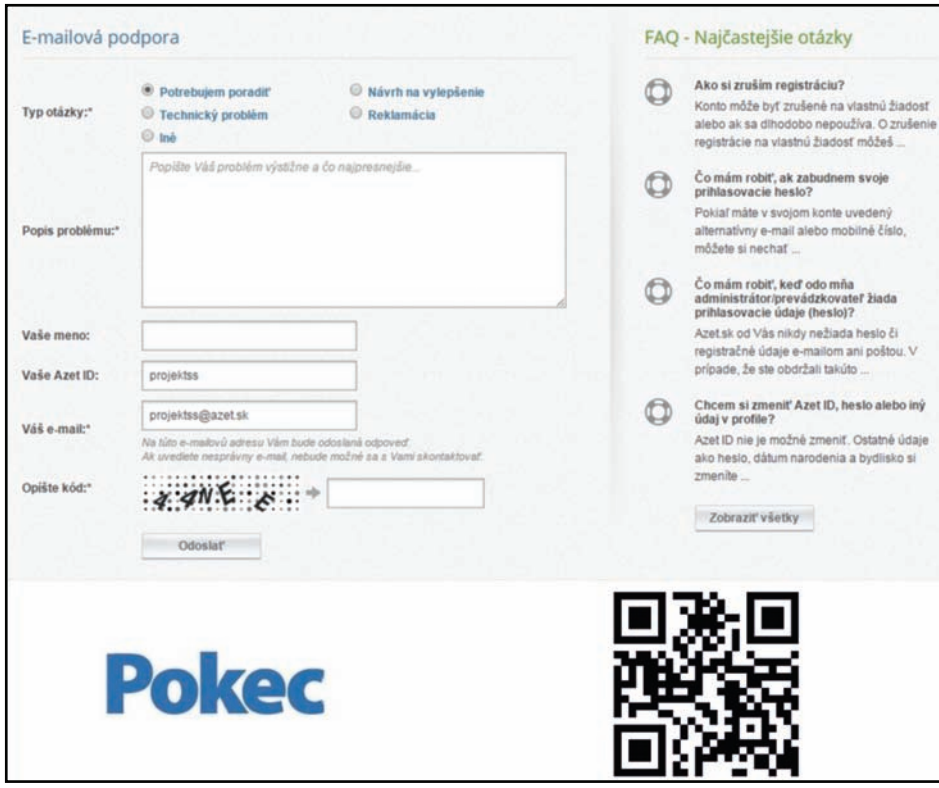


Obrázok č. 20 – Formulár na hlásenie zneužívania alebo obťažovania v sociálnej sieti Twitter

Prevádzkovateľ sociálnej siete Twitter chce od teba, aby si do tohto formulára napísal, ktorý používateľ tejto sociálnej siete porušuje pravidlá, koho sa to porušenie dotýka (teba, tvojho známeho alebo niekoho iného). Okrem toho musíš napísať odkazy na nejaké tweety. Tieto odkazy poslúžia ako dôkaz, že to, čo tvrdíš, je pravda.

5.3.2 Môžem sa brániť na Pokeci?

V rámci sociálnej siete **Pokec** nehľadaj prepracovaný systém riešenia problémov, ako tomu bolo pri predchádzajúcich sociálnych sieťach. Jediná možnosť, ako sa spojiť s prevádzkovateľom tejto sociálnej siete, je použiť kontaktný formulár – **E-mailová podpora**[56]. Ako vyzerá tento formulár môžeš vidieť na obrázku č. 21.

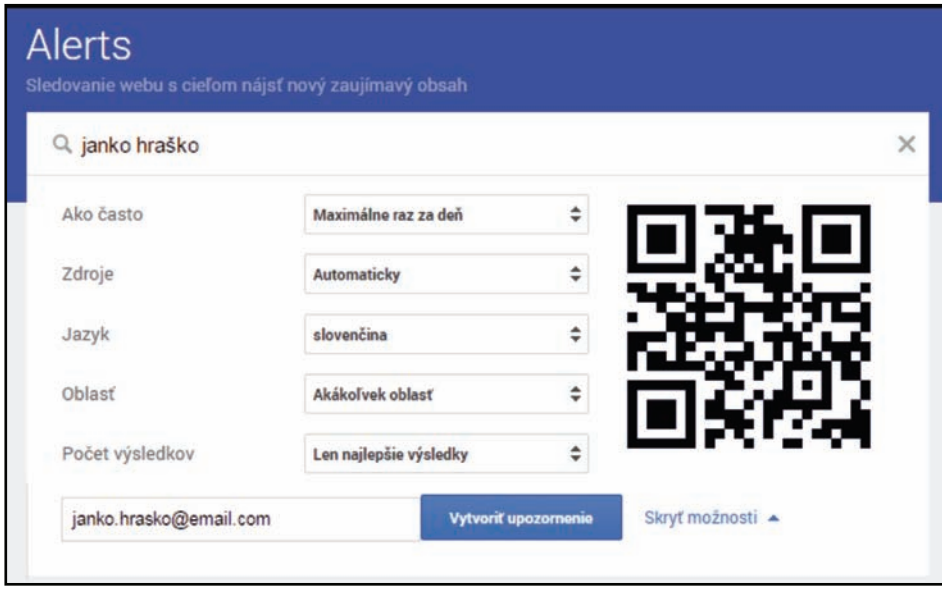


Obrázok č. 21 – Formulár na hlásenie problémov v sociálnej sieti Pokec

5.3.3 Ako si nastaviť zasielanie informácií o sebe na internete?

Isto sa ti viackrát stalo, že si pri použití vyhľadávania natrafil na seba. Buď išlo o nejakú správu, alebo len fotografiu zo školskej alebo spoločenskej akcie. Ak máš záujem dostávať informácie o tom, keď sa vyskytneš niekde na internete a vyhľadávač Google k tomu bude mať prístup, použi nasledujúci návod.

Choď na webovú stránku https://www.google.sk/alerts. Tam máš políčko „Vytvoriť upozornenie na." Klikni do tohto políčka a napíš svoje meno a priezvisko. Keď to dopíšeš, zobrazia sa ti ďalšie možnosti. Klikni na „Zobraziť možnosti." Mal by si vidieť formulár, ako na obrázku č. 22. Na vytvorenie upozornenia zadáš svoj email, na ktorý chceš, aby chodili upozornenia. Môžeš tiež určiť, ako často majú chodiť, z akých zdrojov, jazykov a krajín. Tiež si vieš nastaviť, či chceš všetky výsledky vyhľadávania alebo len tie najlepšie.



Obrázok č. 22 – Formulár na nastavenie služby Google Alerts

Použité zdroje

[1] Vyhlásenie o právach a povinnostiach lokality Facebook zo dňa 15. novembra 2013, dostupné na: https://www.facebook.com/legal/terms

[2] Zásady využívania údajov lokality Facebook zo dňa 15. novembra 2013, dostupné na: https://www.facebook.com/about/privacy/

[3] Pravidlá ochrany osobných údajov Google zo dňa 31. marca 2014, dostupné na: http://www.google.sk/intl/sk/policies/privacy

[4] Zmluvné podmienky Google zo dňa 30. apríla 2014, dostupné na: http://www.google.sk/intl/ sk/policies/terms/regional.html

[5] Všeobecné pravidlá pre servery prevádzkované spoločnosťou Azet.sk, a.s., dostupné na: http://pomoc.azet.sk/vseobecne-podmienky/

[6] Zmluvné podmienky sociálnej siete Twitter (Terms of Service) zo dňa 8. septembra 2014, dostupné na: https://twitter.com/tos

[7] Zásady ochrany osobných údajov sociálnej siete Twitter (Twitter Privacy Policy) zo dňa 8. septembra 2014, dostupné na: https://twitter.com/privacy

[8] Žaloby a dokumenty organizácie Európa vs. facebook, dostupné na: europe-v-facebook.org

[9] ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C.H. Beck, 2013. ISBN 978-80-89603-09-1.

[10] CHMELÍK, J. a kol.: Mravnost, pornografie a mravnostní kriminalita. Praha: Portál, 2003. ISBN 978-80-7178-739-6.

[11] DUNOVSKÝ, J. - MITLÖHNER, M. - HEJČ, K.: Problematika dětských práv a komerčního sexuálního zneužívání dětí u nás a ve světě. Praha: Grada Publishing, 2005. 978-80-247-6316-3.

[12] HOLLÁ, K.: Kyberšikana. Bratislava: IRIS, 2013. ISBN 978-80-8153-011-1.

[13] IVOR, J. a kol.: Trestne právo hmotné. Osobitná časť. Bratislava: IURA Edition, 2010. ISBN 978-80-8078-308-2.

[14] JIROVSKÝ, V.: Kybernetická kriminalita. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2.

[15] KMEC, Jiří a kol.: Evropská úmluva o lidských právech. Komentář. C.H.Beck, 2012. ISBN 978-80-74003-65-3

[16] MADLIAK, J. a kol.: Trestné právo hmotné II. Osobitná časť. Košice: UPJŠ v Košiciach, 2010. ISBN 978-80-7097-695-1.

[17] MAISNER, M. a kol.: Základy práva informačných technológií. Bratislava: IURA EDITION, 2013. ISBN 978-80-8078-549-9.

[18] PETROWSKI, T.: Bezpečí na internetu pro všechny. Liberec: DIALOG, 2014. ISBN 978-80-7424-066-9.

[19] POLČÁK, R.: Právo na internetu. Spam a odpovědnost ISP. Brno: Computer Press, 2007. ISBN 978-80-251-1777-4.

[20] SMEJKAL, V. - SOKOL, T. - VLČEK, M.: Počítačové právo. Praha: C.H.Beck, 1995. ISBN 978-80-704-9101-9.

[21] STRÁŽNICKÁ,V. a kol.: Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex, 2013. ISBN 978-80-894-4795-4.

Poznámky

[1] Facebook založil študent Harvardu Mark Zuckerberg v roku 2004. Od toho času sa služby poskytované Facebookom rozrastajú, ako i počet jeho používateľov. Facebook je v súčasnosti najpoužívanejšou sociálnou sieťou, ktorá má približne 1,3 miliardy aktívnych používateľov.

[2] §11 zákona č. 40/1964 Zb. Občiansky zákonník: Fyzická osoba má právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy.

[3] §4 ods. 1 zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov: (1) Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

[4] Rodné číslo pridelené osobe narodenej pred 1. januárom 1953 je deväťmiestne s trojmiestnou koncovkou. Po 1. januári 1954 je desaťmiestne so štvormiestnou koncovkou. Celé desaťmiestne rodné číslo musí byť bezo zvyšku deliteľné číslom 11.

[5] Bližšie pozri Children's Online Privacy Protection Act (COPPA). Plný text nájdeš na webovej stránke: http://www.coppa.org/coppa.htm

[6] Bližšie pozri na tejto webovej adrese: http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html

[7] Bližšie k tomu pozri http://www.europe-v-facebook.org/EN/ Get_your_ Data_/get_ your_ data_.html

[8] §12 ods. 2-3 zákona č. 40/1964 Zb. Občiansky zákonník: (2) Privolenie nie je potrebné, ak sa vyhotovia alebo použijú písomnosti osobnej povahy, podobizne, obrazové snímky, zvukové alebo obrazové a zvukové záznamy na úradné účely na základe zákona.

(3) Podobizne, obrazové snímky a obrazové a zvukové záznamy, sa môžu bez privolenia fyzickej osoby vyhotoviť alebo použiť primeraným spôsobom tiež na vedecké a umelecké účely a pre tlačové, filmové, rozhlasové a televízne spravodajstvo. Ani také použitie však nesmie byť v rozpore s oprávnenými záujmami fyzickej osoby.

[9] Bližšie pozri na: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

[10] Bližšie pozri na: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

[11] Bližšie pozri Vyhlásenie o právach a povinnostiach zo dňa 15. novembra 2013.

[12] Bližšie pozri Zmluvné podmienky Google zo dňa 30. apríla 2014.

[13] Bližšie pozri Všeobecné pravidlá pre servery prevádzkované spoločnosťou Azet.sk, a.s.

[14] Občiansky zákonník upravuje tri špecifické prostriedky na ochranu osobnosti. Ktokoľvek si môže vybrať a využiť ktorýkoľvek z týchto prostriedkov. Ak sa domnievaš, že práva tvojej osobnosti na sociálnej sieti sú ohrozované alebo porušované, máš možnosť brániť sa a domáhať sa:

- aby sa upustilo od neoprávnených zásahov do práva na ochranu tvojej osobnosti, teda od takého konania na sociálnej sieti, ktoré zasahuje do tvojej ľudskej osobnosti. Napríklad, jeden z tvojich kamarátov má na sociálnej sieti umiestnené fotografie, na ktorých si zobrazený aj ty. Ty si na takéto vyhotovenie nedal súhlas a nesúhlasíš ani s uverejnením fotografie na sociálnej sieti. Upozorníš kamaráta, aby fotografiu stiahol, no on fotografiu nestiahne. Keďže neoprávnený zásah (zverejnenie fotografie bez tvojho súhlasu) pretrváva, môžeš na súde podať žalobu;
- aby sa odstránili následky týchto zásahov. Napríklad sa môžeš domáhať toho, aby sa fotografia z predchádzajúceho príkladu nielenže ďalej neuverejňovala, ale sa aj vymazala. Alebo budeš požadovať, aby sa vymazali nepravdivé príspevky o tebe na sociálnej sieti;
- aby ti bolo dané primerané zadosťučinenie. Príkladom by bol prípad, keď niekto o tebe na sociálnej sieti napíše nepravdivý údaj. Satisfakciou bude, ak na tej istej sociálnej sieti napíše, že to, čo o tebe napísal, nie je pravda a ospravedlní sa;

[15] Ide o tzv. bezpečný prístav (safe harbor). V rámci neho sa spoločnosti mimo EÚ zaručia, že budú spracovávať osobné údaje občanov z krajín Európskej únie v súlade s legislatívou Európskej únie (najmä Smernicou Európskeho parlamentu a Rady 95/46/EC o ochrane jednotlivcov pri spracovaní osobných údajov a voľnom pohybe týchto údajov). Zoznam spoločností, ktoré k nemu pristúpili, je možné nájsť na tejto adrese: https://safeharbor.export.gov/list.aspx

[16] Podanie sa nazýva návrh na začatie konania o ochrane osobných údajov. Úrad na ochranu osobných údajov má na rozhodnutie 60 dní. V odôvodnených prípadoch však túto lehotu môže predĺžiť. V prípade, ak ešte nemáš 18 rokov, návrh na začatie konania podáva tvoj zákonný zástupca (napríklad rodič).

[17] Webová stránka Data Protection Commissioner je: https://www.dataprotection.ie

[18] Ochrana osobnosti (§ 11 ObčZ) je širšia, ako len ochrana osobných prejavov (§ 12 ObčZ) alebo ochrana súkromia (§ 11 ObčZ, § 5 ZoOOU). Zahŕňa okrem iného aj ochranu života a zdravia, občianskej cti a ľudskej dôstojnosti.

[19] Aj toto používanie samozrejme podlieha obmedzeniam, ale bežné použitie mládežou sa v zásade bude kvalifikovať pod zákonné obmedzenia práv držiteľa označenia. A to či už v rozsahu zákona o ochranných známkach, tak aj v právach nekalej súťaže.

[20] *Pozri* https://www.facebook.com/legal/terms

[21] *Pozri* https://twitter.com/tos; https://support.twitter.com/articles/114233-guidelines-for-using-tweets-in-broadcast; http://arstechnica.com/tech-policy/2013/01/news-flash-for-the-media-you-cant-sell-photos-grabbed-from-twitter/

[22] *Pozri viac* Husovec, Martin: Judikatórna harmonizácia pojmu autorského diela v únijnom práve. In Bulletin slovenskej advokácie č. 12/2012.

[23] *Pozri viac* Husovec, Martin: Súhlas alebo licenčná zmluva? Reakcia na článok prof. Telca In Revue pro právo a technologie Vol. 8/2013.

[24] Môže ísť o výpoveď alebo odstúpenie od zmluvy – zákonné alebo dohodnuté.

[25] *Pozri* § 24-38 AutZ.

[26] *Pozri* § 33 AutZ – tzv. použitie na informačné účely.

[27] Ustanovenie § 24 ods. 3 AutZ ("Ustanovenia odsekov 1 a 2 sa nevzťahujú na b) celé literárne dielo ani na jeho podstatnú časť").

[28] Rozhodnutie Súdneho dvora EÚ vo veci BestWater C-348/13, bod. 18.

[29] Používanie diel na sociálnych sieťach je v niektorých prípadoch v tzv. šedej nejasnej zóne. Odpoveď na otázku v prvom rade záleží od toho, ako používaš sociálnu sieť. A teda či na nej máš len skutočne úzky okruh priateľov a tvoj profil je uzatvorený verejnosti, alebo naopak tvoj rozsah priateľov tvoria osoby aj mimo úzkeho kruhu rodiny a priateľov, či prípadne tvoj profil a tam zdieľané dáta zdieľaš aj so širšou verejnosťou. Ak ide o prvý prípad (úzky uzatvorený okruh osôb), zrejme použitie kópie diela bude v rámci zákonnej licencie pre osobnú potrebu, a ďalšie podávanie materiálov tvojim priateľom nebude predstavovať verejný prenos diela, pretože bude absentovať prvok verejnosti. Na druhej strane, ak používaš sociálnu sieť ako viac otvorené miesto (širší, resp. neuzatvorený okruh osôb), nemôžeš sa dovolať ani zákonnej licencie pre osobnú rozmnoženinu a tvoje ďalšie šírenie bude predstavovať tzv. verejný prenos diela. Inými slovami, musíš získať nielen samotnú kópiu diela na základe licencie, ale aj získať licenciu pre ďalšie šírenie diela na sociálnej sieti.

[30] SOZA je neziskové občianske združenie autorov a vydavateľov hudobných diel. V súlade s oprávnením MK SR spravuje na území Slovenskej republiky majetkové autorské práva k hudbe z celého sveta a vykonáva kolektívnu správu práv podľa Autorského zákona. Jej webová stránke je: http://www.soza.sk.

[31] LITA je občianske združenie autorov. LITA pomáha autorom starať sa o ich práva a používateľom uľahčuje získať súhlas na použitie diel. Webová stránka: http://www.lita.sk.

[32] Ustanovenie § 4 ods. 1 zákona č. 22/2004 Z. z. o elektronickom obchode.

[33] Trestné právo je jedno z právnych odvetví, ktoré chráni významné, dôležité spoločenské vzťahy pred protiprávnym konaním tým, že určuje v Trestnom zákone čo je trestným činom, určuje podmienky trestnej zodpovednosti (i beztrestnosti), druhy sankcií, spôsob ich ukladania a výkonu. Osobitná časť Trestného zákona, kde sú uvedené jednotlivé trestné činy sa delí na hlavy, pričom názov hlavy reprezentuje určitú oblasť spoločenských vzťahov či práv a slobôd, ktorým sa poskytuje ochrana a to tak, že tam ustanovené konania sa považujú za trestné. Príkladom je napr. I. Hlava s názvom „Trestné činy proti životu a zdraviu" kde sa poskytuje ochrana právu na život; II. Hlava s názvom „Trestné činy proti slobode a ľudskej dôstojnosti" poskytuje ochranu viacerým právam a slobodám, napr. právu na súkromie, listovému tajomstvu, tajomstvu prepravovaných správ, osobnej slobode; IV. Hlava s názvom „Trestné činy proti majetku", tým, že považuje vykonanie tam uvedených konaní (trestných činov) za trestné, poskytuje ochranu právu vlastniť. Možno teda uzavrieť, že trestné právo okrem iného poskytuje ochranu základným právam a slobodám, preto v tejto kapitole sa budeme zaoberať najmä konaniami, ktoré možno považovať z pohľadu trestného práva za protiprávne.

[34] Výraz malware vznikol ako skratka dvoch anglických slov, a to malicious (zákerný) a software (softvér).

[35] Viac na: http://sk.wikipedia.org/wiki/Keylogger

[36] Tvorca škodlivého softvéru nemusí tento softvér aj sám šíriť. Preto použité označenie nemusí byť stále pravdou. Máme na mysli skôr tých, ktorých chcú využiť škodlivý softvér na určitú nelegálnu činnosť. Tvorca škodlivého softvéru mohol napísať určitý program za úplne iným účelom ako zločineckým, avšak v dôsledku vynaliezavosti páchateľa vie byť tento program aj na tento účel použitý, prípadne k zmene určitého programu na škodlivý softvér došlo iba malým zásahom do programu, resp. jeho úpravou.

[37] Protiprávne konanie páchateľa môže byť často trestné, teda takéto konanie môže napĺňať znaky rôznych skutkových podstát trestných činov. Najčastejšie môže ísť o trestný čin porušovania tajomstva prepravovaných správ (§ 196 trestného zákona), poškodzovania cudzej veci (§ 245 trestného zákona), neoprávneného prístupu do počítačového systému, k inému nosiču informácií alebo jeho časti (§ 247 trestného zákona).

[38] Hlavným trestným činom, ktorého sa hacker bude dopúšťať pri hackingu je trestný čin neoprávneného prístupu do počítačového systému, k inému nosiču informácií alebo jeho časti (§ 247 trestného zákona). Na subsumovanie konania pod skutkovú podstatu tohto trestného činu je nevyhnutné získanie neoprávneného prístupu do počítačového systému, k inému nosiču informácií alebo jeho časti a páchateľ musí zároveň alternatívne:

a) takto získané informácie neoprávnene použiť;

b) takto získané informácie neoprávnene zničiť, poškodiť, vymazať, pozmeniť alebo znížiť ich kvalitu;

c) urobiť zásah do technického alebo programového vybavenia počítača;

d) alebo vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát mariť funkčnosť počítačového systému alebo vytvárať neautentické dáta s úmyslom, aby sa považovali za autentické, alebo aby sa s nimi takto na právne účely nakladalo;

Hacker musí toto konanie vykonať v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech.

[39] Bližšie pozri rozhodnutie okresného súdu Piešťany vo veci 2T/41/2014

[40] Bližšie pozri rozhodnutie okresného súdu Galanta vo veci 29T/184/2013

[41] Bol obvinený z trestného činu sexuálneho zneužívania (§ 201 trestného zákona), vydierania (§ 189 trestného zákona), ohrozovania mravnej výchovy mládeže (§ 211 trestného zákona), zvádzania k pohlavnému styku a znásilnenia (§ 199 trestného zákona)

[42] Viac na: http://zpravy.idnes.cz/deviant-hovorka-se-dockal-za-zneuziti-dvaceti-chlapcu-mirnejsiho-trestu-14o-/krimi.aspx?c=A090526_073207_krimi_cena na: http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba

[43] Viac na: http://trencin.sme.sk/c/5307089/dievcina-dostala-za-ohovaranie-na-pokeci-podmienku.html#ixzz3KAtvvTvd

[44] Porov. Jak zvládnout kyberšika? Online Safety Institute, z.s.p.o., 2012. Preložené a upravené z nemeckého originálu organizácie Klicksafe.de (www.klicksafe.de). Dostupné online: http://www.bezpecne-online.cz/finish/3-materialy-pro-ucitele/8-jak-zvladnout-kybersikanu Kyberšika. Národní centrum bezpečnějšího internetu, 2012. Dostupné online: http://www.bezpecne-online.cz/finish/3-materialy-pro-ucitele/65-kybersikana

[45] V Slovenskej republike možno kyberstalking postihovať už od 1. septembra 2011 ako trestný čin nebezpečného prenasledovania. Podľa § 360a trestného zákona sa páchateľ dopustí trestného činu nebezpečného prenasledovania, ak iného dlhodobo prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života tým, že:

a) sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe;

b) vyhľadáva jeho osobnú blízkosť alebo ho sleduje;

c) ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli;

d) zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu;

e) alebo ho inak obmedzuje v jeho obvyklom spôsobe života;

Za tento trestný čin hrozí trest odňatia slobody až na jeden rok.

V prípade, ak sa takéhoto konania dopustí na chránenej osobe (dieťa, tehotná žena, osoba staršia ako 60 rokov, chorá osoba, a pod.), závažnejším spôsobom konania (napr. po dlhší čas, organizovanou skupinou, na viacerých osobách, atď.), z osobitného motívu (typicky z pomsty alebo so sexuálnym motívom) alebo verejne, sa trest zvyšuje na 6 mesiacov až 3 roky odňatia slobody.

Treba zdôrazniť, že trestný čin je spáchaný verejne aj vtedy, ak sa tak stane obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom, alebo pred viac ako dvoma súčasne prítomnými osobami.

[46] Pojem detská pornografia možno vymedziť ako zobrazenie sexuálneho styku s dieťaťom alebo zobrazenie obnažených častí tela dieťaťa smerujúce k vyvolaniu sexuálneho uspokojenia inej osoby.

[47] Podľa § 201 trestného zákona sa trestného činu sexuálneho zneužívania dopustí ten, kto vykoná súlož s osobou mladšou ako pätnásť rokov alebo kto takú osobu iným spôsobom sexuálne zneužije.

[48] Porov. IVOR, J. a kol.: Trestne právo hmotné. Osobitná časť. Bratislava: IURA Edition, 2010, ISBN 978-80-8078-308-2. s. 411-412.

[49] Anglické slovo hoax označuje podvod, žart.

[50] Viac na: http://spravy.pravda.sk/svet/clanok/278655-virtualny-utok-na-biely-dom-zrazil-trhy-na-kolena/

[51] Screenshot (snímku obrazovky) vytvoríš nasledovne: Na klávesnici stlač tlačidlo Print Sreen, väčšinou má skratku Prt Sc. Tak „vyfotíš" presne to, čo máš v tú chvíľu na obrazovke a obrázok sa automaticky uloží do vyrovnávacej pamäte. Potom môžeš otvoriť niektorý textový editor, napr. Word alebo program Skicár (Štart> Programy> Príslušenstvo> Maľovanie), a zadáš príkaz „vložiť" (buď pravým tlačidlom myši alebo klávesovou skratkou „Ctrl + v"). Snímka obrazovky sa ti zobrazí v textovom súbore. Ulož ho tak, aby si našiel súbor, až ho budeš chcieť niekomu ukázať.

[52] Napr. občianske združenie European Information Society Institute (EISi), ktoré sa zaoberá prienikom technológií, práva a informačnej spoločnosti. EISi slúži ako neuniverzitné centrum pre výskum internetového práva a práva duševného vlastníctva a popri tom aktívne bojuje za ochranu práv a slobôd internetových užívateľov, spotrebiteľov a poskytovateľov služieb. Viac na: http://eisionline.org/. Pozri tiež webstránky: http://www.zodpovedne.sk/, http://pomoc.sk/ a http://stopline.sk/.

[53] Bližšie pozri na: https://goo.gl/

[54] QR kód (QR Code) je dvojrozmerný čiarový kód, ktorého účelom je rýchle rozpoznanie textov zakódovaných do tohto čiarového kódu. QR kód vyvinula v roku 2004 japonská spoločnosť Denso-Wave.

[55] Tento nástroj môžeš nájsť na tejto webovej adrese: https://support.google.com/legal/troubleshooter/1114905?rd=1/troubleshooter/1114905?rd=1

[56] Tento formulár nájdeš na tejto webovej adrese: http://onas.azet.sk/kontakty

JUDr. Ľubomír Lukič
RNDr. JUDr. Pavol Sokol

(Ne)bezpečie sociálnych sietí

Prvé vydanie.
Vydalo European Information Society Institute, o. z. v roku 2014, http://eisionline.org.

MINISTERSTVO ZAHRANIČNÝCH VECÍ
A EURÓPSKYCH ZÁLEŽITOSTÍ
SLOVENSKEJ REPUBLIKY

Realizované s finančnou podporou Ministerstva zahraničných vecí a európskych záležitostí SR v rámci dotačného programu Podpora a ochrana ľudských práv a slobôd.
Za obsah tohto dokumentu je výlučne zodpovedný European Information Society Institute, o. z.

Recenzenti:	JUDr. Peter Huba, PhD., RNDr. Róber Hajduk, PhD.
Jazyková korektúra:	Mgr. Peter Béreš
Obálka:	Diana Matláková
Tlač:	EQUILIBRIA, s.r.o.

ISBN 978-80-971307-2-5

ISBN 978-80-971307-2-5