UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2013-1016

BAKALÁŘSKÁ PRÁCE

Sabina Eisnerová

Sociální sítě a ochrana soukromí

Praha 2016

Vedoucí bakalářské práce: Mgr. Tatiana Iskanderová, Ph.D.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2013 – 2016

BACHELOR THESIS

Sabina Eisnerová

Social networking and privacy

Prague 2016

The Bachelor Thesis Work Supervisor:
Mgr. Tatiana Iskanderová, Ph.D.

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nich jsem při zpracování čerpala, v práci řádně cituji a uvádím v seznamu použitých zdrojů. Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne Sabina Eisnerová

Poděkování

Ráda bych poděkovala za vedení bakalářské práce a odbornou pomoc při jejím zpracování paní Mgr. Tatianě Iskanderové, Ph.D. a také své rodině za podporu a trpělivost.

Anotace

Bakalářská práce popisuje výhody a nevýhody sociálních sítí a jejich komunikaci na internetu.

Klíčová slova

Bezpečnost, komunikace, kybergrooming, kyberstalking, kyberšikana, sociální sítě, soukromé údaje a jejich ochrana.

Annotation

Bachelor thesis describes the advantages and disadvantages of social networks.

Key words

Communications, cyberbullying, cybergrooming, cyberstalking, private information and their protection, security, social networks.

OBSAH

ÚVOD ... **8**
TEORETICKÁ ČÁST ... **9**
1 SOCIÁLNÍ SÍTĚ ... **9**
1.1 Facebook ... 13
1.2 Google+ ... 16
1.3 Myspace ... 17
2 RIZIKA NA SOCIÁLNÍCH SÍTÍCH ... **18**
2.1 Krádež identity ... 20
2.2 Kyberšikana ... 22
2.3 Kybergrooming ... 23
2.4 Kyberstalking ... 25
2.5 Riziko soukromí ... 27
3 OCHRANA SOUKROMÍ ... **29**
3.1 Ochrana osobních údajů ... 30
3.2 Ochrana proti kyberšikaně ... 37
3.3 Ochrana v sociálních sítích ... 39
3.4 Ochrana hesla ... 41
3.5 Pomoc pro rodiče, jak chránit své děti na sociálních sítích ... 42
PRAKTICKÁ ČÁST ... **45**
4 VÝZKUM ... **45**
4.1 Cíl výzkumného šetření ... 45
4.2 Hypotéza ... 45
4.3 Výsledky ... 46
4.4 Diskuze ... 55
ZÁVĚR ... **59**
RESUMÉ ... **60**
SEZNAM POUŽITÝCH ZDROJŮ ... **61**
SEZNAM OBRÁZKŮ A TABULEK ... **66**
SEZNAM PŘÍLOH ... **67**

ÚVOD

Sociální sítě se staly nedílnou součástí každodenního života, a to nejen pro mladší generace. Typickým příkladem oblíbené sociální sítě je Facebook, jenž si udržuje žebříček nejčastěji navštěvované sítě nejen na světě, ale již řadu let i v České republice. Snaží se o neustálou inovaci, aby byl pro uživatele čím dál zajímavější. Především mladší generace přitom často zapomíná, že sociální sítě nepřináší pouze nové informace, bleskovou komunikaci, sdílené fotografie či videa, ale i možná rizika a hrozby. S četností komunikace po internetu počet těchto nežádoucích vlivů a útoků každoročně vzrůstá. Často je příčinou neznalost a slepá důvěra právě mladých lidí. Virtuální prostředí otevírá prostor pro nová rizika, jakými jsou zejména krádež identity, kyberšikana nebo kybergooming. Proto by otázka ochrany soukromí měla patřit mezi klíčové oblasti každého jedince, který je uživatelem jakékoliv sociální sítě. Zneužití osobních údajů s sebou nese mnohdy velmi nepříjemné dopady zejména finančního rázu. Příjemné není ani šikanování či pronásledování, které ohrožuje jedince v jeho psychické rovině, příp. i na zdraví a životě.

Cílem této práce je zjistit nejčastější rizika užívání sociálních sítí a ověřit znalost uživatelů v oblasti ochrany na sociálních sítích.

Jako metoda bude v teoretické části použita literární rešerše a v praktické části bude realizován průzkum pomocí dotazníkového šetření.

Teoretická část nejprve blíže definuje specifika sociálních sítí, přiblíží některé z nejčastěji užívaných sítí s nastolením možných rizik a připojí doporučení, jak jim předcházet. Druhá kapitola se již zaměří na konkrétní nejčastější rizika, se kterými se lze setkat na sociálních sítích. Třetí kapitola nastíní možnosti ochrany s doporučením pro rodiče, kteří plní svoji základní roli a jsou vzorem pro své děti. Děti totiž představují nejrizikovější věkovou skupinu na internetu.

TEORETICKÁ ČÁST

1 SOCIÁLNÍ SÍTĚ

Sociální sítě se staly v posledním desetiletí nedílnou součástí nejen mladší generace, ale všech věkových skupin populace. Jejich proměna je závislá na technologickém vývoji, stejně jako na náročnosti a zvyšujících se požadavcích uživatelů. Jak je tedy charakterizován prostor, ve kterém probíhá virtuální realita?

Jednu z definic nabízí R. Divínová, která kyberprostor označuje za *„virtuální (tedy ne skutečný) prostor, který se nám otevírá prostřednictvím počítačů a počítačových sítí. V souvislosti s počítačovou sítí - internetem hovoříme také o on-line prostředí.“*[1]

Anderson přibližuje základní fungování sítě. Internetová síť je oproti tradičním způsobům komunikace chaotická, decentralizovaná a neregulovaná. Neexistuje centrální počítač ani centrum. Veškerý obsah internetu je v serverech po celém světě. Internet v podstatě posílá informace různými cestami, aby byly obtížně zachytitelné. Díky svému vojenskému původu odolá rozsáhlé destrukci i nukleárnímu útoku. Pokud je totiž nějaká cesta vyřazena z provozu, informace se dostane ke svému koncovému uživateli cestou jinou, neporušenou. Tím se stává „virtuální“ sítí, která běhá po povrchu reálné sítě telekomunikačních společností.[2]

Sociální síť (anglicky social network) tvoří propojenou skupinu lidí. V užším slova smyslu jde o společenskou strukturu jednotlivců s určitou vazbou na další jednotlivce zapojené do stejné struktury. Jejich vazby představují grafové struktury tvaru sítě. V širším slova smyslu je síť chápána jako softwarový prostředek, a to zejména v podobě webových portálů (sociálních webů), které sociální síť formují a spravují. Na rozdíl od dřívějších portálů přidávají sociální sítě k poskytovaným službám osobní rozměr. Uživatelé komunikují v rámci portálu mezi sebou navzájem, mohou však i ostatním doporučovat informace a zdroje. Rovněž vzájemně sdílejí další doplňující informace jako např. kontakty, reference, zkušenosti apod., což v rámci sociální sítě zaujímá aspekty spolupráce. Sociální weby patří k aplikacím řady Web 2.0.[3] Postupně se

[1] DIVÍNOVÁ, R. (2005, s. 23).
[2] ANDERSON (1996) In DIVÍNOVÁ, R. (2005, s. 13).
[3] DAVIDSON, E.; VAAST, E., no 1. In MATOUŠEK, K.; DOLEŽAL, J. (2010, s. 215).

vyvinuly ze statického (ukládacího) systému na dynamický nástroj, který umožňuje informace opětovně využít (např. otevřená encyklopedie Wikipedia). Nelze však zapomínat ani na možnost kontroly využití těchto získaných informací. K tomu slouží povinnost ověřovat identitu uživatelů a jejich příslušnost k dané instituci, omezení anonymního přístupu, způsob schvalování publikovaných informací apod.[4]

Internet nabízí řadu sociálních sítí, které se liší svým účelem, charakterem svých příslušníků a jejich potřeb a cílů. Rovněž existují uvnitř sítě nebo mimo ni, otevřené pro všechny, nebo uzavřené pro určitou komunitu, v určité geografické hranici, nebo mimo ni. Takovéto nepřeberné množství možností poskytuje širokou využitelnost pro širokou populaci uživatelů. Při registraci se zpravidla ani nerozlišuje konkrétní uživatel. Sítě jsou však i oborové, profesionální, ale i zájmové nebo pro studijní účely. Profesionální sociální sítě sdružují profesionály konkrétního oboru, proto nejsou anonymní ani otevřené pro všechny. Patří sem např. sítě na podporu vědeckého bádání ResearchGate, SciSpace, Epernicus, ScienceStage.[5] „Hobby" sociální sítě zase sdružují uživatele s danou problematikou na hobby úrovni. Studentské sociální sítě nemusí sdružovat pouze studenty, ale mohou být zaměřeny i na studium (konkrétní obor nebo více oborů v rámci studentské komunity konkrétní univerzity).[6]

V širokém spektru sociálních sítí patří k nejznámějším:

- Facebook (od roku 2004).
- Google+ (od roku 2011 jako obdoba Facebooku).
- Myspace (vznikl v roce 2003 a patří ke 2. nejpoužívanější světové síti).
- Twitter (od roku 2006).
- LinkedIn (od roku 2003 tvoří pracovní sociální síť).[7]

Ke známým českým sítím patří zejména Lidé.cz, Spolužáci.cz, LíbímSeTi.cz apod. Předpokládá se, že role internetu bude srovnatelná v dějinách lidstva např. s vynálezem

[4] MATOUŠEK, K.; DOLEŽAL, J. (2010, s. 215).
[5] MATOUŠEK, K., DOLEŽAL, J., KUBALÍK, J., NEČASKÝ, M. (1/2011, s. 137).
[6] MOLNÁR, Z. (1/2011, s. 136-137).
[7] BURIAN, P. (2014, s. 84).

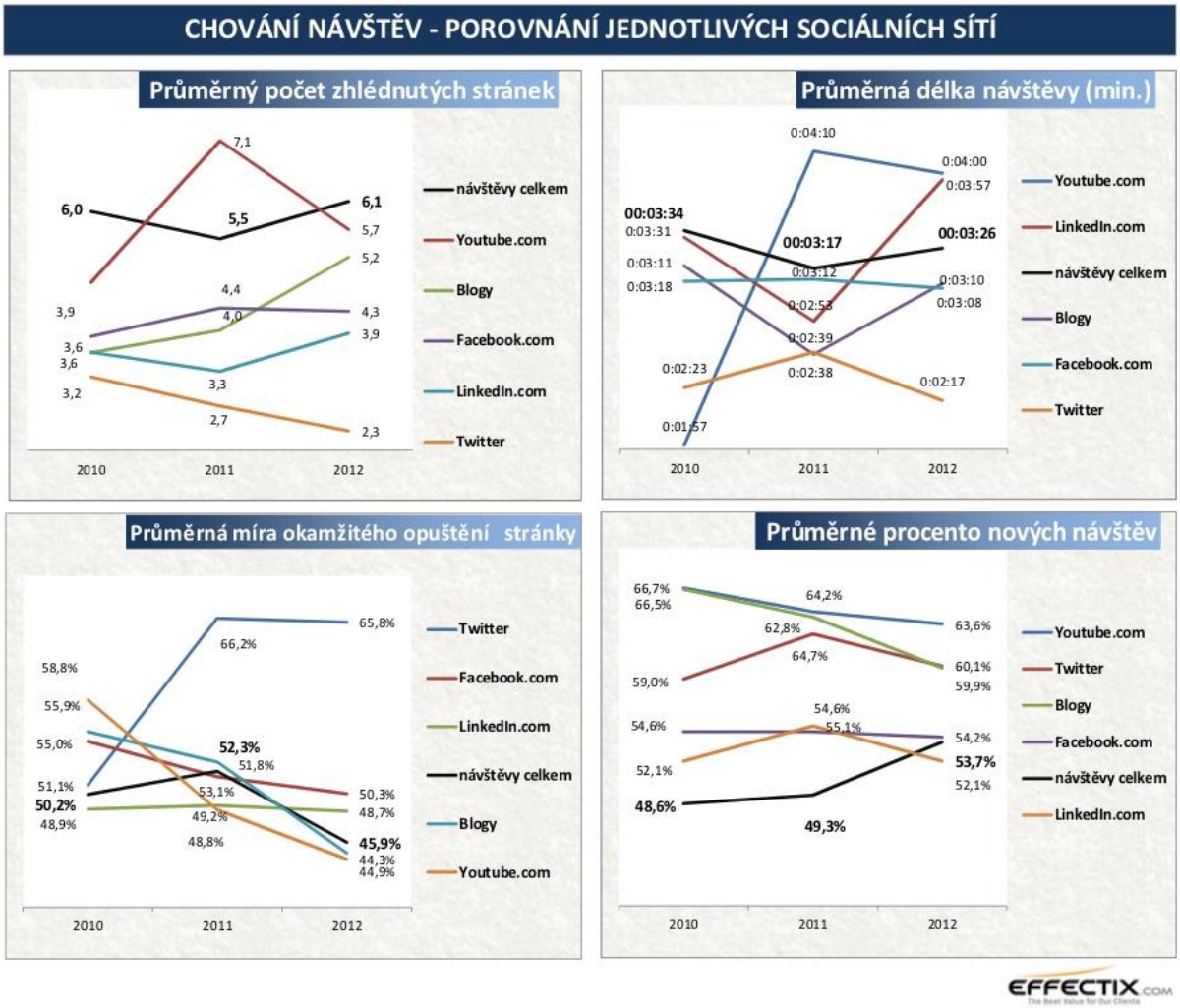
knihtisku či parního stroje. Významná odlišnost internetu však plyne z absence autora tohoto fenoménu v podobě nějaké konkrétní osoby nebo skupiny osob.[8]

Na rozšířenost sociálních sítí do životů dnešních jedinců, zejména mladších věkových kategorií, ukazuje provedený výzkum EU Kids Online II. Výsledky ukazují, že 72 % všech českých dětí ve věku 9-16 let má profil na sociálních sítích, z toho 93 % ve věku 15-16 let. Ve srovnání s 25 zeměmi EU zaujímá ČR 6. Místo, což je více, než představuje evropský průměr (59 %). Přitom skoro čtvrtina těchto dětí má na sociální síti 100 a více „přátel". [9]

Počet uživatelů Facebooku a Twitteru v ČR neustále roste. Z hlediska statistických údajů je patrné, že počet uživatelů Twitteru se rozrůstá mnohem rychleji než počet uživatelů Facebooku. V březnu 2013 měl Facebook 3,8 mil. aktivních měsíčních uživatelů (přitom „pouze" 1,8 mil. uživatelů je skutečně aktivních) a Twitter měl uživatelů ve stejném období. Nejčastějším uživatelem Faceboku je osoba mladší 36 let. U českých uživatelů je věková hranice ještě nižší, a to do 29 let. Facebook patří mezi nejsledovanější sociální sítě. Základní ukazatele z hlediska návštěvnosti vybraných sociálních sítí prezentuje obrázek 1. Nejlepších výsledků měřených parametrů dosáhl kanál YouTube.com. Návštěvník zde stráví nejvíce času, prohlédne si nejvíce stránek a opouští vstupní stránky co nejméně. Rovněž zasílá nejvíce nových návštěv vůči vracejícím se návštěvám, jejichž počet v průběhu roku klesá jen výjimečně. Pro návštěvníka Twitteru jsou naopak typické rychlé informace za zlomek stráveného času, prohlédne si nejméně stránek a zároveň nejčastěji opouští vstupní stránky. Blogy posílají návštěvníky na komerční webové stránky. Návštěvníci, kteří si prohlédnou více stránek, méně často opouštějí vstupní stránky. Nejčastěji jde o nové návštěvy. Délka zhlédnutí je ovšem kratší než u průměrného návštěvníka. Návštěvník LinkedIn je nejčastěji „věrným" návštěvníkem, který na webu stráví delší dobu, než je průměrná návštěva, na druhou stranu si prohlédne výrazně méně stránek.[10]

[8] SMEJKAL, V. (1999, s. 7).
[9] ŠMAHEL, D. (2014, s. 23-24).
[10] Statistiky sociálních sítí.*Effectix.com.* [online]. [cit. 2015-9-27]. Dostupné z: http://www.doba-webova.com/cs/statistiky-pro-socialni-sit.

Obrázek 1: Návštěvnost vybraných sociálních sítí



Zdroj: Statistiky sociálních sítí.*Effectix.com.* [online]. [cit. 2015-9-27]. Dostupné z: http://www.doba-webova.com/cs/statistiky-pro-socialni-sit.

Internet tedy představuje řadu příležitostí, např. umožňuje být kreativní. Příležitostmi, které internet nabízí, se zabýval výzkum EU Kids Online II. Z jeho výsledků vyplynulo, že nejméně se internet používá pro hraní her cestou do školy nebo do práce, více se využívá ke sledování online videí (např. YouTube), poté již figuruje komunikace prostřednictvím sociálních sítí včetně používání online messengerů, online čtení nebo sledování zpráv (75 % evropských dětí). Na ještě vyšším stupni, tedy ještě častěji děti využívají internet na společné online hraní her, stahování filmů a hudby a sdílení obsahů v rámci sítí (peer to peer).[11] Tady výzkum uvádí 56 % uživatelů, z toho třetinu

[11] Peer-to-peer - *rovný s rovným*. V případě počítačových sítí mezi sebou uživatelé přímo komunikují.

zaujímají děti ve věku 9-10 let. Nejvyšší úroveň zahrnují již návštěvy chatovacích místností, blogování a trávení času ve virtuálním světě (např. Second Life). Tohoto stupně dosahuje pouze 23 % evropských dětí.[12]

Nelze však zapomínat, že s šíří online aktivit lineárně vzrůstá i počet rizik. Čím více je dítě (nebo jiná osoba) aktivní, tím více času na internetu stráví a tím vzrůstá pravděpodobnost výskytu rizik.

1.1 Facebook

Jak již bylo řečeno, nejčastěji užívanou sociální sítí je Facebook. Ten byl spuštěn 4. února 2004. Původním záměrem jeho zakladatele Marka Zuckerberga bylo vytvoření komunitní sítě pro studenty Harvardské univerzity. Od 11. 8. 2006 se tato síť otevřela pro celý svět s omezením dolní hranice uživatelů pro registraci na 13 let. Posláním Facebooku je poskytnout lidem možnost sdílet, čímž se stane svět otevřenějším a propojenějším. Jde tedy v podstatě o službu, která umožňuje kontakt mezi lidmi a prostřednictvím fotografií, videí, tvorby zájmových skupin a plánování akcí usnadňuje komunikaci. Pro samotnou registraci je potřeba pouze e-mailová adresa nebo číslo mobilního telefonu.[13]

Roku 2012 se Facebook výrazně změnil nastavením nové koncepce osobních profilů. Timeline profil mění účel Facebooku. Jeho podstatou už není pouze kontakt s přáteli či rodinou, ale snaha o tvorbu „kroniky svého života", která je volně přístupná komukoliv. Timeline od zaregistrování shromažďuje veškerá data, která řadí chronologicky. Kdokoliv si tedy může přečíst již dávno neaktuální informace psané v afektu, euforii či jiném stavu pozměněného vědomí. Informace lze nahrávat i zpětně. Novinkou je rovněž sdílení obsahu navštívených webových stránek, a to i bez připojení k Facebooku. Tím Facebook zprostředkovaně informuje i ostatní uživatele o všech krocích daného uživatele na zdi, což podle mnoha odborníků na problematiku sociálních sítí nahrává stalkerům. Proto je zásadní otázkou nastavení soukromí svého účtu. To přináší otázku znalosti či lhostejnosti některých uživatelů v tomto nastavení. Vzhledem k tomu, že na Facebooku chatují nejčastěji osoby mladší 29 let, které jsou méně podezíravé a více

[12] ŠMAHEL, D. (2014, s. 32-33).
[13] KRÁL, M. (2015, s. 172).

otevřené ve virtuálním prostředí, hrozí zde více nebezpečí stalkingu, kyberšikany nebo dalších útoků. Nová koncepce také přináší nově „Like“ tlačítka nebo „legalizaci“ poskytování osobních údajů uživatelů a dat správcům a vývojářům facebookových aplikací, a to navíc i v případě, že konkrétní uživatel danou aplikaci vůbec nepoužívá, ale např. uživatelův přítel ano. Poněkud neefektivním právem Facebooku je možnost uživatele „přejmenovat“ nebo smazat při obdobě uživatelského jména s obchodní značkou nebo registrovanou ochrannou známkou. Navíc automaticky s používáním Facebooku uživatel souhlasí s těmito podmínkami nejen aktuálně, ale i do budoucnosti.[14]

Problematiku ochrany osobních údajů na Facebooku přibližuje v publikovaném rozhovoru nejmenovaný zaměstnanec Facebooku, který sdělil, že na serverech Facebooku jsou uchovávány veškeré informace, všechny provedené akce, kliknutí na něčí profil, změny v profilových informacích ať již smazané, či nikoliv. Z historie poté lze zjistit nejlepší přátele. Veškeré informace o více než dvě stě dvaceti milionech lidí jsou uchovávány na několika tisících serverech ve čtyřech datových centrech po světě. Všichni zaměstnanci Facebooku se tak mohou prostřednictvím speciálního přístupu (dříve hesla tzv. master password) nebo tlačítka „switch login“ po jeho zdůvodnění nalogovat do různých profilů, což ukazuje na vysoké riziko zneužití osobních dat uživatelů. Z rozhovoru dokonce vyplynulo, že za zneužití univerzálního přístupu byli již dva lidé vyhozeni.[15]

Wolf poukazuje na tenkou hranici mezi nevinnou konverzací a odhalováním svých citlivých dat na veřejném místě, jakým Facebook bezesporu je. Přestože sám Facebook nepředstavuje žádnou přímou hrozbu, díky své jednoduché aplikaci poskytuje svým prostřednictvím komukoliv informace, které mohou být ve své zákeřnosti až kritické.[16]

Vždy je proto nutné chránit si soukromí, což lze zajistit vhodným nastavením sdílení s konkrétním okruhem osob. Rovněž je velmi důležité dodržovat určité zásady, které

[14] Jak se mění facebook. *Úřad pro ochranu osobních údajů.* [online] 2013. [cit. 2015-9-27]. Dostupné z: https://www.uoou.cz/jak-se-meni-facebook/ds-2457/archiv=0&p1=2589.
[15] Ochrana soukromí na Facebooku? *Úřad pro ochranu osobních údajů.* [online] 2010. [cit. 2015-9-27]. Dostupné z: https://www.uoou.cz/ochrana-soukromi-na-facebooku/ds-2463/archiv=0&p1=2589.
[16] WOLF, K. Soukromí a bezpečnost v sociálních sítích prakticky – Facebook díl 1. *LUPA.cz* [online]. 2009 [cit. 2015-09-27]. Dostupný z WWW: http://www.lupa.cz/clanky/soukromi-v-socialnich-sitich-prakticky-facebook/.

Král shrnuje následovně:

- Vždy pečlivě vybírat přátele (existuje kategorie známí).
- U každé aktivity je vhodné nastavit kategorii uživatelů, kteří ji uvidí.
- Vždy je potřeba nezapomínat na možné důsledky svých aktivit (např. neoznamovat dlouhodobě volný byt apod.).
- Nastavit si pravidla pro soukromí (oprávnění uživatelů).
- Pro přístup je vhodné unikátní heslo, které není využíváno i pro jiné služby.
- Vhodné je nastavení upozornění na přihlášení k jeho sledování pro možnost zneužití profilu.[17]

Wolf publikoval několik praktických rad, jak se co nejvíce chránit na Facebooku. Např. pro změnu viditelnosti přátel je potřeba navštívit stránku „Soukromí profilu“ v menu Nastavení soukromí. Rovněž lze jednoduše vypnout veřejnou viditelnost včetně zákazu veřejného umístění do vyhledávačů (záložka „search privacy settings“).[18]

Největší problém sociálních sítí spočívá v absenci sociálních bariér. Např. tagování[19] na choulostivých fotografiích a videu, informace ze statusů nebo o stavu vztahu představuje největší rizika ztráty soukromí. Proto je přímo nutností nastavení viditelnosti nápisů na zdi, nastavení, kteří přátelé smějí vzkazy na zeď posílat, a nastavit soukromí. Přestože lze vypnout viditelnost mnoha sekcí daného profilu, nelze zapomínat na skutečnost, že nelze zabránit dostupnosti informací přes přátele.[20]

[17] KRÁL, M. (2015, s. 175).
[18] WOLF, K. Soukromí a bezpečnost v sociálních sítích prakticky – Facebook díl 1. *LUPA.cz* [online]. 2009 [cit. 2015-09-27]. Dostupný z WWW: http://www.lupa.cz/clanky/soukromi-v-socialnich-sitich-prakticky-facebook/.
[19] Otagovat fotografii znamená přiřadit jméno dosud „neidentifikované“ postavě.
[20] WOLF, K. Jak překonat nástrahy Facebooku a vytěžit z něj co nejvíce - díl 2. *LUPA.cz* [online]. 2009 [cit. 2015-09- 27]. Dostupný z WWW: http://www.lupa.cz/clanky/jak-prekonat-nastrahy-facebooku-dil-2/.

1.2 Google+

Google Google+ neoznačuje jako sociální síť. Jde o sociální vrstvu napříč všemi jeho produkty, která je sjednocuje. Před spuštěním Google+ byly služby Googlu totiž roztříštěné.[21]

Google+ je obdobou Facebooku. Zahrnuje stream příspěvků, umožňuje nahrávat fotografie. Místo přístupu formou přátelství zde existují tzv. kruhy. Uživatelé mohou své příspěvky sdílet veřejně nebo s vybranými kruhy. Firmy si zde mohou zakládat firemní stránky. Komunikace zde je více zdrojem informací než místem velké interakce jako na Facebooku. Uživatelské příspěvky se neplusují ani nekomentují. Koncem roku 2012 se aplikace rozšířila o funkci Komunity, která sdružuje uživatele do skupin s různými zájmy. Zajímavostí je Hangouts nebo možnost skupinových videohovorů až pro 10 lidí současně. Skoro již nepostradatelnou funkcí jsou místa vhodná k propagaci podniků (např. restaurací, ZOO apod.). Díky aplikaci v chytrém telefonu se při hledání vhodného místa na mapě zobrazí přesná adresa, otevírací doba, recenze ostatních uživatelů Google+ a příp. i aktuální nabídka nebo speciální akce v tomto podniku.

Jelikož je potřeba reagovat na nové potřeby uživatelů, původní verze, která přinášela lidem možnost sdílet a připojit se přes Google, již nestačí. Nově má být aplikace rozšířena o další možnosti:

- Cílenější zážitek Google+ - Google+ je místem lidí se společnými zájmy. Proto budou přidány nové funkce (např. Google+ sbírky, kde půjdou sdílet tematické příspěvky) a naopak přemístěny některé funkce (např. fotky Google+ budou přesunuty do nové aplikace Fotky Google) pro poutavější Google+.
- Použití Googlu bez profilu Google+ - pro snazší přístup a vše na jednom místě bude účet Google nabízet vše, tedy možnost sdílet obsah, komunikovat, tvořit na kanálu YouTube a další. Základní účet Google nebude možné vyhledat ani následovat na rozdíl od veřejných profilů Google+. Pro ty, kteří již mají

[21] OLANOFF. D. For the last time, let's all say it together: "Google+ is NOT a Social Network". In The Next Web [online]. 2012 [cit. 2015-09-29]. Dostupné z: http://thenextweb.com/socialmedia/2012/03/08/for-the-last-time-lets-all-say-it-togethergoogle-is-not-a-social-network.

vytvořené profily na Google+ a neplánují využití Google+ samotného, budou vytvořeny lepší možnosti pro řízení a odstranění veřejných profilů.[22]

1.3 Myspace

MySpace jako první sociální síť začala podporovat internetový marketing. Tato síť je rovněž podobná Facebooku včetně možnosti chatování, ale umožňuje více úprav vzhledu profilů.

Jako úspěšnou sociální síť ji v roce 2011 koupil Justin Timberlake. Začátkem roku 2013 došlo ke kompletnímu redesignu, který se vyznačoval nevšedním ovládáním. Zaměřuje se na hudebníky a spojení s uživateli. Měsíčně aplikaci navštíví více než 50 milionů uživatelů. V listopadu 2014 si 300 milionů uživatelů přehrálo během jednoho měsíce nabízené videoklipy. Ze statistik vyplývá, že nejčastějšími uživateli aplikace MySpace jsou mladí ve věku 17 - 25 let. MySpace rovněž navštěvují původní uživatelé, kteří zde mají uložené fotky a vystavují je na jiných sociálních sítích. MySpace má přes miliardu založených účtů uživatelů z celého světa a v databázi přes 465 milionů e-mailových adres uživatelů ze Spojených států. Hlavním příjmem je však reklama.[23]

[22] HOROWITZ, B. Everything in its right place. *Google. Official Blog.* [online]. 2015 [cit. 2015-09-27]. Dostupné z: http://googleblog.blogspot.cz/2015/07/everything-in-its-right-place.html.
[23] JAVŮREK, K. MySpace žije! Měsíčně ho navštíví 50 milionů uživatelů. *Zive.cz* [online]. 2015 [cit. 2015-09-27]. Dostupné z: http://www.zive.cz/bleskovky/myspace-zije-mesicne-ho-navstivi-50-milionu-uzivatelu/sc-4-a-176906/default.aspx#utm_medium=selfpromo&utm_source=zive&utm_campaign=copylink.

2 RIZIKA NA SOCIÁLNÍCH SÍTÍCH

Široká využitelnost sociálních sítí s sebou přináší i rizika a řadu nebezpečí. K poměrně rozšířeným negativním vlivům patří zejména falešné profily, kyberšikana, hoax[24] nebo otázka bezpečnosti. Poměrně hojně diskutovanou otázkou je přenositelnost dat a možnost migrace mezi sociálními sítěmi. Řada uživatelů si neuvědomuje, že účet uživatele je technicky majetkem správce sítě. A právě právní odpovědnost může vyvolat do budoucna problémy. U českých provozovatelů jako např. Lidé či LíbímSeTi by problém tohoto typu být neměl, což neplatí u globálních sítí, jako je např. Facebook. Přestože se musí řídit americkou legislativou, nesmí zároveň odporovat českému právnímu řádu.[25] Kdo však řeší příp. spory nebo porušení zákona? Americké, nebo české právo?

Obecně se pojmem počítačová kriminalita zabýval např. Doc. Ing. Vladimír Smejkal, CSc. Počítačovou kriminalitu charakterizuje jako trestnou činnost, ve které figuruje počítač jako souhrn hardwarového a softwarového vybavení s údaji, příp. některý z komponentů počítačů, příp. většího počtu počítačů samostatných nebo připojených do počítačových sítí, a to buď jako předmět trestné činnosti (tj. cíl „oběť“ zločineckého útoku), samozřejmě s výjimkou takové trestné činnosti, jejímž předmětem jsou opsaná zařízení jako věci hmotné, anebo jako nástroj trestné činnosti (nástroj zločince).[26]

Z hlediska právního systému ČR jsou internetem totiž poskytovány služby na základě dvou základních principů. Prioritní je princip teritoriality, podle něhož je rozhodné právo vždy právem země, kde je služba poskytována. Doplňujícím principem je právo upravující realizovanou službu (činnost) prostřednictvím obecně platných právních norem obsažených zejména v občanském a obchodním zákoníku, autorském zákoně

[24] Hoax obecně označuje podvod, mystifikaci či žertovnou klamnou zprávu. V elektronické komunikaci je hoax speciálně nevyžádaná e-mailová nebo IM zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako řetězový e-mail. Typickými hoaxy jsou falešný poplach, zábavné dopisy nebo prosící zprávy.
[25] ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP*. [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/.
[26] SMEJKAL, V. (1999, s. 65).

nebo ve speciálních předpisech např. o telekomunikacích, o hromadných sdělovacích prostředcích, o bankách, o loteriích a jiných hrách apod.[27]

Díky své specifičnosti má internet i vlastní specifické trestné činy, které lze rozdělit do dvou základních kategorií:

- Informační trestná činnost - zpřístupnění informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu, anebo naopak shromažďování informací o osobách za účelem jejich pozdějšího nelegálního využití.
- Internetová trestná činnost - páchání trestné činnosti v internetovém prostředí.[28]

K nejvíce rozšířeným rizikům, která jsou již v povědomí uživatelů, patří bezpečnostní rizika spojená s možností zneužití účtu. Existuje řada možností, jak překonat bezpečnostní heslo k účtu, a to od uhodnutí hesla, přes nedostatečné zabezpečení např. e-shopu, po únik hesla přes nešifrované spojení, vir na počítači nebo díky phishingu.[29] Následky bývají vždy nepříjemné, ať už jsou osobního nebo finančního rázu. Uživatel má následně velice omezené možnosti k zablokování a zabránění dalšímu páchání škody. Velkým rizikem je zneužití těchto údajů při přihlášení do dalších služeb (e-mail, SMS brána apod.).[30]

Další nebezpečí představují socialboti neboli počítačem řízení avataři. Tváří se jako běžní uživatelé, živě sdílí a diskutují s cílem získat přátelství. S přáteli totiž sdílí i osobní údaje pro komerční využití. Bezpečnostní hrozbou je i přihlašování do dalších služeb prostřednictvím účtu ze sociální sítě zpravidla na základě pozměněného konceptu OpenID. Rovněž aplikace třetích stran, které vyžadují určitý přístup k účtu

[27] SMEJKAL, V. (1999, s. 16).
[28] (Tamtéž, s 87-96).
[29] PHISHING označuje podvodné e-mailové útoky na uživatele internetu, jejichž cílem je vylákat důvěrné informace. Nejčastěji jde o údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí jít přitom o účty bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězi nebo kde je možné jakýmkoliv způsobem zneužít jejich služby. Příkladem může být PayPal, eBay, Skype, Google.
[30] ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP.* [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/.

uživatele a jeho osobním údajům, jsou riziková. Nelze totiž zpětně ověřit nakládání s takto získanými daty.[31]

Stále oblíbenou zprávou jsou hoaxy, které jsou mylné. Jejich jediným cílem je příjemce ovlivnit k určitému jednání nebo vyvolat strach. Dříve se šířily prostřednictvím e-mailů, nyní se přetransformovaly na sociální sítě. Jelikož jsou tyto zprávy doporučené nebo okomentované známými lidmi, zvyšuje se pocit jejich důvěryhodnosti a tím i jejich nebezpečnost. Vždy je nutné tyto informace nejprve ověřit a považovat je spíše za nevěrohodné.[32]

2.1 Krádež identity

Za krádež identity je považován případ, kdy jsou *„osobní údaje jednotlivce bez jeho souhlasu využity s cílem vydávat se za někoho jiného.“*[33] Motivací pachatelů přitom bývá zisk, snaha zakrýt nebo usnadnit si trestnou činnost, příp. získání nové identity.[34]

Krádeže kybernetické identity jsou již nedílnou hrozbou počítačového prostředí. V podstatě od roku 2009 jejich zastoupení narůstá a hodnotou 9,8 % v roce 2010 se stává třetím nejčastějším zločinem počítačového prostředí (po nedoručené platbě/zboží a tzv. FBI podvodech). Krádež identity se stala nejrychleji se rozvíjejícím druhem kybernetické kriminality. Její nebezpečnost je zřejmá z výše způsobených finančních ztrát.[35] V roce 2014 si stále udržuje vysokou příčku zločinnosti. Dosahuje 4. pozice kriminality s hodnotou 8,9 % a ztrátou 32.845.753 $.[36]

Tento novodobý trend je důsledkem elektronického věku, kdy vzrůstá počet oblastí, které lze vyřídit elektronickou cestou (např. elektronické formuláře, e-mailová pošta

[31] ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP*. [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/.
[32] ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP*. [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/.
[33] GŘIVNA, T. a kol. (2014, s. 345).
[34] (Tamtéž, s. 345).
[35] 2010 Internet Crime Report. *Federal Bureau of Investigation . Internet Crime Complaint Center*. [online]. 2010. [cit. 2015-9-28]. Dostupné z: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.
[36] 2014 Internet Crime Report. *Federal Bureau of Investigation . Internet Crime Complaint Center*. [online]. 2014. [cit. 2015-9-28]. Dostupné z: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf. s. 47.

apod.). Ve spojitosti se sociálními sítěmi není zpravidla zisk, což si ne vždy každý uživatel uvědomuje.

Krádež identity může být dvojího druhu - necílená na konkrétní osobu (předkládaný podpis pachatel záměrně zkouší v referenční databázi, jestli někdo jiný nemá stejný, za toho se následně bude vydávat) a zacílená na konkrétní osobu (pachatel se snaží zcela záměrně napodobit statistické a dynamické charakteristiky podpisu osoby, za kterou se chce vydávat).[37]

Při zneužití osobních údajů dochází nejen ke ztrátě peněz na účtu, ale mnohdy nastanou situace, kdy je potřeba se zodpovídat za nezaplacené výdaje, za různé škody, příp. nést důsledky mnoha trestných činů spáchaných cizí osobou ovšem „s novou identitou". Dokazování neviny přitom není ničím jednoduchým. Podvodníky zajímají zpravidla jméno a příjmení, rodná čísla a čísla osobních dokladů, ale i veškeré údaje, podle kterých je možno konkrétní osobu určit, tedy i čísla PIN a bezpečnostní kódy kreditních karet, adresa bydliště, rodinné či pracovní poměry, detaily o hypotékách a úvěrech apod.[38]

Osobní údaje (zejména rodné číslo využitelné kdekoliv - např. v nemocnici) lze mnohdy nepozorovaně zkopírovat nebo zneužít současně se zjištěním dalších informací, jako např. jaká je finanční situace dané osoby, kolik vlastní nemovitostí, kde pracuje, jaký je její zdravotní stav apod. Rovněž jsou poměrně rozšířené útoky na platební karty nebo kódy PIN k získání přímého zisku formou čtecích zařízení s miniaturním kamerovým systémem na bankomatech nebo instalací plastového obdélníčku, který kartu již nevydá. Další riziko představuje i odhození účtenky po zaplacení nákupu platební kartou. V praxi však nemusí vždy docházet ke zneužití pouze podvodným způsobem. Mnohdy jsou lidé ochotni vyplnit různé osobní formuláře, registrační dotazníky, soutěže, marketingové průzkumy a přitom s využitím svých údajů souhlasí. Vždy je proto důležité zvážit riziko při poskytování citlivých osobních údajů.[39]

[37] RAK, R. a kol. (2008, s. 440).
[38] Ztráta identity. *Policie ČR*. [online]. 2015. [cit. 2015-9-28]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx.
[39] (Tamtéž).

2.2 Kyberšikana

Další negativní problém internetu představuje kyberšikana. Zahrnuje systematickou snahu někoho poškodit prostřednictvím elektronické komunikace (např. sociální sítě). Následky bývají podobného rázu jako u šikany klasické, tedy zejména vyčlenění z kolektivu, urážky, snižování důstojnosti. Určitou „výhodou" kyberšikany je zanechání důkazů proti útočníkovi nebo útočníkům, jelikož zpravidla neužívají falešný profil nebo přístup na síť prostřednictvím proxy serveru. Vždy jde o trestný čin, na což je potřeba pamatovat.[40] Na sociální síti se stává oblibou nenápadná, ale i zcela otevřená kyberšikana. Projevuje se jízlivými komentáři k profilu oběti, posíláním nadávek, zveřejňováním fotografií a videí bez vědomí oběti, vytěsňováním ze skupiny vrstevníků, urážkami a pomluvami. Rovněž sem patří zneužití falešného profilu oběti, který je vytvořen někým jiným, kde se oběť vyjadřuje a projevuje nepřijatelným způsobem.[41]

Byť není kyberšikana spojena pouze s dětmi a mládeží, právě v této věkové kategorii je nebezpečná zejména s ohledem na nízký věk oběti, ale mnohdy i útočníka. *„Dr. Michal Kolář, odborník v oblasti šikany, hovoří o kyberšikaně, pokud dítě nebo skupina dětí úmyslně, zpravidla opakovaně ohrožuje, pronásleduje a týrá psychicky jiné dítě a zneužívá k tomu mobilní přístroje a internet, přičemž hlavním cílem útočníků je ublížit oběti.“*[42]

Kyberšikana přitom může být přímá (prováděna jednotlivcem) nebo vykonávána v zastoupení dalších osob, které často oběť šikanují nevědomě. Oběť útoku se přitom v danou chvíli nemůže bránit.

Častým důsledkem takového jednání bývají narušené vztahy jedince v reálném světě, které si kompenzuje určitým způsobem na internetu a v komunikaci s mobilními telefony.[43]

[40] ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP.* [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/.
[41] ECKERTOVÁ, L., DOČEKAL, D. (2013, s. 74).
[42] (Tamtéž, s. 65).
[43] ČERNÁ, A. a kol. (2013, s. 49).

Dnešní doba v podstatě nutí jedince být jako ostatní, a to zejména v mladém věku, cílem je příliš se neodlišovat od ostatních. S tím souvisí i zvýšená snaha dosáhnout co nejlepšího postavení ve skupině, mít mnoho přátel a příznivců, být populární třeba na sociální síti.[44]

Přestože průběh agresivního jednání prostřednictvím klasické šikany je považován za závažnější pro svou fyzickou podobu, v podobě kyberšikany je útok považován za méně zraňující, vždy jde o nepřístojné jednání a trestný čin dle českého práva. Obě podoby mají jedno společné agresor, původce šikany má nižší míru empatie ve srovnání s ostatními dětmi, proto se ani neumí vcítit do oběti a chápat, jaké zranění jí způsobuje.[45]

2.3 Kybergrooming

V současné době se rozmáhá internetový jev nazvaný kybergrooming. Jde o psychologickou manipulaci oběti, kterou si pachatel najde na internetu a udržuje s ní kontakt prostřednictvím komunikačních technologií. Jeho cílem je u oběti vzbudit důvěru a následně ji donutit k osobní schůzce. Na této schůzce často dochází k sexuálnímu zneužití oběti nebo jinému traumatizujícímu jednání, např. k tvorbě dětské pornografie.[46]

Kybergroomerem jsou muži i ženy, převládají však muži, ne vždy musí jít zároveň o pedofily. Často preferují dospělé sexuální partnery, u kterých mohou být neúspěšní a děti nebo mladiství jsou „pouze“ náhradním objektem. Jinak se od normální většinové populace osobnostně příliš neliší.[47]

Vybraná metodika rozlišuje následující typologii pachatelů kybergroomingu:

- Kvazivoyeur - uspokojuje ho pozorování své oběti prostřednictvím web kamery. Postupně ji vede k co nejintimnějšímu chování a projevům pro uspokojení aktuálních sexuálních potřeb. O osobní setkání se nesnaží.

[44] ŠEVČÍKOVÁ, A. a kol. (2014, s. 129).
[45] (Tamtéž, s. 124, 133).
[46] ŠEVČÍKOVÁ, A. a kol. (2014, s. 89).
[47] *KYBERGROOMING A KYBERSTALKING. Metodický materiál pro pedagogické pracovníky*. Praha: Národní centrum bezpečnějšího internetu, 2012. s. 5.

- Experimentátor - hraje si s obětí, než ji zneužije. Mění portály i vlastní identitu. V kontaktech je aktivní, své jednání plánuje a přizpůsobuje podle situace. Požadavky, návrhy a tlak na oběť cílevědomě zvyšuje, může mít „rozpracováno“ více obětí.
- Kriminálník - svou oběť nebo získaný materiál prodá. Jeho cílem je získat oběť pro páchání trestné činnosti, zpravidla pro výrobu a šíření pornografie nebo prostituci, příp. za úplatu zprostředkovává tipy pedofilům. Vlastní sexuální stimulace je druhotná.
- Duševně nemocný - nemá náhled, chová se podle akutních popudů a pohnutek. Jeho prožívání a chování závisí na typu onemocnění nebo stupni mentální retardace.[48]

Kybergroomer ovládá strategii, bývá zdatným psychologem. Většinou jeho postup na internetu probíhá následovně:

- Vyhlédnutí oběti na sociální síti, chatu nebo na internetové seznamce.
- Oslovení, navázání komunikace.
- Budování důvěry a „přátelského“ vztahu.
- Vytváření emocionální závislosti oběti na kybergroomerovi.
- Snaha o izolaci oběti zejména utajením vzájemného výjimečného vztahu.
- Komunikace směřuje na erotiku.
- Vyžadování intimních fotografií a videí pro příští nátlak.
- Manipulace dárky, penězi s cílem zvýšit závislost oběti.
- Přitvrzování komunikace, vydírání, vyhrožování.
- První a často poslední osobní schůzka.
- Další schůzky, útok/napadení (sexuální nátlak, pohlavní zneužití, znásilnění, zneužití dítěte k výrobě pornografie, kuplířství).[49]

[48] *KYBERGROOMING A KYBERSTALKING. Metodický materiál pro pedagogické pracovníky*. Praha: Národní centrum bezpečnějšího internetu, 2012. s. 6.

Všechny uvedené fáze zanechávají na nezralé osobnosti (zejména dítěti) negativní psychické následky.

2.4 Kyberstalking

„Stalking (lov, pronásledování) je termín, který označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu.“ [50]

Pronásledovatel svou oběť dlouhodobě sleduje, zahlcuje zprávami, e-maily, telefonáty, příp. nechtěnými dárky. V elektronickém prostředí jde o tzv. kyberstalking. Tady jsou oběti zasílány různé zprávy prostřednictvím ICQ, chatu, VoIP technologií,[51] sociálních sítí apod. Cílem útočníka je vyvolat pocit strachu. Nejčastějšími oběťmi stalkingu jsou známé osobnosti (zpěváci, herci, politici), expartneři apod.[52]

Jak lze poznat, že se již jedná o kyberstalking? Základní znaky shrnuje Kopecký následovně:

- Opakované a dlouhodobé pokusy kontaktovat oběť (velké množství e-mailů, telefonátů, SMS zpráv, vzkazů na ICQ, Skype, na chatu). Obsah těchto zpráv může být příjemný až veselý nebo urážející až zastrašující. Jejich snahou je jakoukoliv formou kontaktovat oběť.
- Demonstrování moci a síly stalkera - stalker ukazuje svoji sílu prostřednictvím přímých i nepřímých výhrůžek, které opírá o poznatky o oběti (vím, kde jsi, co děláš, vidím tě, vím, co máš na sobě…). Rovněž může vyhrožovat fyzickým útokem na oběť či její blízké.
- Uskutečňování výhrůžek - při selhání dosavadního kontaktu může dojít k naplnění výhrůžek. Zpravidla se stalkeři zaměřují na poškozování a ničení majetku, příp. na fyzický útok na oběť nebo její blízké.

---

[49] *KYBERGROOMING A KYBERSTALKING. Metodický materiál pro pedagogické pracovníky*. Praha: Národní centrum bezpečnějšího internetu, 2012. s. 7.
[50] KOPECKÝ, K. (2010. s. 3).
[51] Voice over Internet Protocol (VoIP) je technologie, která umožňuje přenos digitalizovaného hlasu prostřednictvím počítačové sítě nebo jiného média, zejména internetu, intranetu nebo jakéhokoliv jiného datového spojení.
[52] KOPECKÝ, K. (2010, s. 3).

- Stalker se vydává za oběť a snaží se obrátit veřejné mínění na svoji stranu. Sám se označuje za oběť.
- Snaha poškodit reputaci oběti - např. vytvořením falešné internetové stránky/blogu, kde o oběti zveřejňuje nepravdivé informace ve snaze snížit její důvěryhodnost, reputaci apod.[53]

V praxi tedy musí dojít alespoň k deseti pokusům o kontakt, pronásledování musí trvat minimálně čtyři týdny a jasně jsou nastaveny role pachatele (agresora) a oběti.[54]

Pro naplnění skutkové podstaty trestného činu nebezpečné pronásledování (§ 354) podle zákona č. 40/2009 Sb., trestního zákoníku, však musí být dodrženy zejména tři podmínky:

1. Musí být jednoznačné, že pronásledovatel tak činí proti vůli oběti.
2. Pronásledování musí být intenzivní.
3. Pronásledování musí být dlouhodobé (min. 4-6 týdnů). Přitom lhůta se počítá až od 1. 1. 2010, kdy byl stalking stanoven jako trestný čin.

Kyberstalking se od klasického stalkingu liší tím, že pronásledování se uskutečňuje na dálku prostřednictvím informačních technologií. Přitom fyzicky útočící stalker poměrně běžně ke svým útokům využívá kyberstalking.[55]

Kyberstalkeři k získání co největšího množství informací o oběti a k jejímu kontaktování využívají diskusní fóra, kde komunikují pod falešnou identitou. Rovněž často využívají různé typy spywarových programů.[56]

Podle organizace Bílý kruh bezpečí se obětí stalkingu může stát kdokoliv bez rozdílu věku, pohlaví, sociálního postavení, kulturního zázemí, vzhledu nebo sexuální orientace. Ze statistik vyplývá, že nejčastější obětí pronásledování se stává svobodný člověk žijící bez partnera nebo osoba krátce po partnerském rozchodu. Podle celosvětových výzkumů má se stalkingem vlastní zkušenost kolem 10 % populace. Z hlediska četnosti útoků anglosaské studie udávají, že zhruba 4–7,2 % mužů

[53] KOPECKÝ, K. (2010, s. 3-4).
[54] KYBERGROOMING A KYBERSTALKING. Metodický materiál pro pedagogické pracovníky. Praha: Národní centrum bezpečnějšího internetu, 2012. s. 14.
[55] KYBERGROOMING A KYBERSTALKING (2012, s. 14).
[56] KOPECKÝ, K. (2010, s. 7).

a 12–17,5 % žen se alespoň jednou se stalkingem osobně setkalo. V první německé studii o stalkingu uvedlo 11,6 % dotázaných, že byli minimálně jednou v životě obětí stalkera. Oběťmi jsou nejčastěji ženy (87,2 %).[57] Podle uvedených statistických čísel je zřejmé, že stalking je poměrně rozšířeným jevem.

2.5 Riziko soukromí

Soukromí osob na sociálních sítích je mnohdy narušováno samotným uživatelem, jelikož si ne vždy uvědomuje, jaké informace o sobě veřejně zpřístupňuje. V rámci základních informací o svém bydlišti a vystavených fotografií často ukazuje vybavení bytu, příp. dokonce informuje o své nepřítomnosti, odjezdu na dovolenou apod.

Nelze zapomínat, že soukromé informace na Facebooku jsou dostupné nejen nejbližším přátelům. Kasík publikoval provedený test zaměřený na důvěryhodnost této nejnavštěvovanější sociální sítě. Z výsledků vyplynulo, že mladí čeští uživatelé si své soukromí příliš nehlídají. Proto se vystavují riziku šmírování, příp. i vážnějším hrozbám. Většina náhodně vybraných uživatelů Facebooku si přidala mezi přátele neexistující dívku (u neexistujícího mladíka se jednalo o 42 % uživatelů). Zároveň většina nachytaných umožnila tomuto „příteli“ přístup ke všem svým datům na síti, tj. k soukromým fotografiím, fotografiím přátel, e-mailu, telefonu, škole, v několika případech dokonce k celé domovní adrese. V tomto případě nepomohou žádné ochranné nástroje, pokud si uživatel dobrovolně přidá cizího člověka mezi své přátele. Při snaze o přátelství se pouze asi pětina dotazovala, odkud se znají. Více než polovina se vůbec nezabývala otázkou zjišťování identity a automaticky si přidala neznámého (v tomto případě neexistujícího) člověka mezi své přátele. Mezi důvěřivé patřili zejména mladší lidé ve věkovém spektru mezi 15 - 30 lety. Poměrně jednoduše lze tedy nahlížet do soukromé fotogalerie zcela neznámých lidí.[58]

Provedený průzkum rovněž ukázal, jak snadno lze provést útok na konkrétního uživatele Facebooku. Nejprve se zjistí z veřejného profilu přátelé oběti. Poté si stalker vytvoří první falešný profil a tyto přátele si zkusí přidat. U těch, kteří ho pustí, prohledá

[57] Dressing, Kuehner, Gass Lifetime prevalence and impact of stalking in a European population. British Journal of Psychiatry, 2005. In KOPECKÝ, K. (2010, s. 7).
[58] KASÍK, P. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet.cz* [online]. 2009. [cit. 2015-9-28]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka.

jejich fotky a najde mezi nimi i fotky oběti. Je však potřeba najít fotku někoho, kdo ještě na Facebooku není, přesto je ale z okolí oběti. Jeho fotku a jméno stalker použije následně pro vytvoření druhého falešného profilu. Přidá si známé oběti a poté i samotnou oběť. Té se zobrazí tvář známého člověka, známé jméno a několik společných přátel. Jak se dá bránit? Zásadní je zabezpečení profilu proti prohlížení cizími lidmi. V případě snahy o přátelství je vhodné si nejprve ověřit, že se skutečně jedná o danou osobu. Další důležitou oblastí je neprobírat soukromé nebo dokonce intimní informace v komentářích, na zdi nebo statusu. Jsou veřejně dostupné, ale ne vždy vhodné pro každého. Průzkum přinesl i pozitivní zjištění. Většina uživatelů (přes 90 %) měla svůj profil uzavřen pro zcela neznámé lidi. Ke zpřístupnění soukromých informací nebo fotografií se dostanou pouze jimi schválení lidé. Různé profily s různými oprávněními používá pouze málo uživatelů.[59]

[59] KASÍK, P. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet.cz* [online]. 2009. [cit. 2015-9-28]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka.

3 OCHRANA SOUKROMÍ

Sociální sítě umožňují komunikovat s řadou uživatelů, poskytují rychle potřebné informace. Představují však nejen rizika, ale určitým způsobem narušují soukromí uživatelů. Je možné se nějak účinně bránit?

Již Listina základních práv a svobod[60] (dále jen Listina) zaručuje nedotknutelnost osoby a jejího soukromí. K omezení může dojít pouze ze zákonných důvodů. Samotný pojem soukromí však není nikde právně definován, přitom je spojován i s dalšími právy uvedenými v Listině, např. s listovním tajemstvím. Jelikož článek 13 Listiny stanoví, že nedotknutelnost listovního tajemství se nevtahuje pouze na tištěné dokumenty, ale i na jiné písemnosti a záznamy uchovávané v soukromí nebo zasílané poštou anebo jiným způsobem, patří sem i e-mailové zprávy, zprávy podávané telefonem, telegrafem nebo jiným obdobným zařízením. Výjimky tvoří pouze případy a způsoby vyňaté ze zákona.

Ochrana osobnosti je rovněž obsažena v ustanoveních občanského zákoníku. Podpora v dalším zákoně, jenž by doplnil Listinu, vyžadovala reakce *„na skutečnost, že osobní údaje na straně jedné tvoří součást soukromé (osobnostní) sféry a současně na straně druhé mohou působit a dokonce i vznikat bez vůle a vědomí toho, o kom informují.“*[61]

Je potřeba si uvědomit, že při kontaktu se soukromou věcí či informací by mělo být vždy zřejmé, že se vstupuje do cizího prostoru, protože tam, kde končí soukromí jednoho, začíná soukromí druhého. Právo na soukromí je základní právo pro všechny zakotvené v Listině: *„Právo na soukromí je chápáno jako nejuniverzálnější nebo nejrozsáhlejší ze všech tak zvaných osobnostních práv, chráněných občanským právem. Je tomu tak proto, že pokud je postiženo soukromí, dochází tím i k zásahu do všech ostatních osobnostních práv.*“[62]

Práva na ochranu osobnosti upravuje Listina ve svých článcích 1 a 3, kde je zejména upravena rovnost lidí v důstojnosti, právech a svobodách. Článek 17 Listiny zaručuje právo na svobodný přístup k informacím: *„svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice států“,* což je omezeno zákonem

[60] Ústavní zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod.
[61] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 7).
[62] MATES, P. (2002, s. 37).

pro dosažení ochrany práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Proto kromě některých výjimek není stanovena povinnost nikomu sdělovat informace.[63]

S problematikou soukromí úzce souvisí i pojem osobních údajů. Článek 10 odst. 3 Listiny zaručuje ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě. Je proto nutné zacházet s těmito údaji, zejména citlivými, velmi uvážlivě.

V českém prostředí se ochranou soukromí zabývají ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů. Jeho cílem je zajistit zákonné, řádné a pro soukromí co možná nejméně invazivní zpracování osobních údajů.[64] Legislativně jsou upraveny základní pojmy a dále práva a povinnosti v oblasti zpracovávání osobních údajů. Tento zákon rovněž stanoví podmínky pro předávání osobních údajů do zahraničí.

3.1 Ochrana osobních údajů

Podle zákona o ochraně osobních údajů je osobní údaj charakterizován jako jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Přitom se za určený nebo určitelný subjekt údajů považuje takový, který lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[65]

Kučerová pojem osobní údaj specifikuje jako *„každý údaj, který se týká konkrétní – identifikované nebo identifikovatelné fyzické osoby. Pokud je vlastníkem vozidla fyzická osoba, pak údaj o tom, kdo a jaké vozidlo vlastní nebo provozuje, je jejím osobním údajem ve smyslu zákona o ochraně osobních údajů.“*[66]

Z předmětného vymezení pojmu tedy vyplývá, že za osobní údaj je považován každý údaj, který je ve vztahu k nějaké fyzické osobě.[67]

Pokud tedy může být fyzická osoba přímo nebo nepřímo ze zpracovávaných údajů identifikována, jedná se o osobní údaje.[68]

[63] MATES, P. (2002, s. 40).
[64] NONNEMANN, F. In KUČEROVÁ, A. a kol. (2012, s. 206).
[65] § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění.
[66] KUČEROVÁ, A.; NONNEMANN, F. (2010, s. 11).
[67] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 19).

Osobní údaje vzniklé díky novým informačním technologiím jsou specifickou kategorií, která je mimo typologii osobních údajů. Matoušová takováto data definuje jako „šedou zónu“. [69]

Zvláštním druhem osobních údajů jsou citlivé údaje. Jejich zneužití mnohdy znamená závažné dopady. V mezinárodním právu jsou zahrnuty zejména v Úmluvě č. 108 v článku 6 a ve směrnice č. 95/46/ES v článku 8. V ČR je definuje zákon o ochraně osobních údajů. Jedná se o údaje, které lze zneužít k diskriminaci či sociálnímu vyčlenění jedince ze společnosti bez vazby na hodnoty dalších osobních údajů téhož subjektu. Náboženské nebo etnické údaje mohou být zneužity k diskriminaci.[70]

Vhodná je na tomto místě specifikace pojmů *určený* a *určitelný* subjekt údajů. Za *určený* nebo *určitelný* subjekt údajů se považuje takový, který lze identifikovat např. podle prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Nejvyšší správní soud tuto specifikaci objasnil tak, že „*plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného, než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu.*“[71]

Nejvyšší správní soud rovněž došel k závěru, že osobním údajem je i telefonní číslo. Jeho prostřednictvím lze subjekt kontaktovat, tím je subjekt dosažitelný, a tedy i jistým způsobem určitelný.[72] Z toho lze odvodit, že i e-mailová adresa je osobním údajem, pokud se skládá ze jména, příjmení a názvu firmy. V tomto spojení je totiž osoba identifikovatelná. Obdoba bude platit i v případě, že nepůjde o spojení s označením firmy, ale např. s doménou poskytovatele služeb elektronických komunikací. Musí zde však figurovat jméno a příjmení dané fyzické osoby. Jinak nelze považovat jiný tvar e-mailové adresy za osobní údaj (např. poskytovatel1@poskytovatel.cz).[73]

---

[68] KUČEROVÁ, A.; NONNEMANN, F. (2010, s. 11).
[69] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 31).
[70] (Tamtéž, s. 80).
[71] Rozsudek Nejvyššího správního soudu ze dne 12. února 2009, sp. zn. 9 As 34/2008.
[72] KUČEROVÁ, A.; NONNEMANN, F. (2010, s. 51).
[73] BARTÍK, V.; JANEČKOVÁ, E. (2013, s. 12).

Další významný údaj v elektronickém prostředí nabízí IP adresa. Nejvyšší správní soud se při posuzování povahy IP adresy podpůrně odkazoval na judikaturu Soudního dvora Evropských společenství z roku 2008, který ve svém rozhodnutí pro identitu osob, u nichž byla známá pouze IP adresa a čas připojení, tyto údaje považoval za osobní údaje ve smyslu předpisů na ochranu osobních údajů. Z uvedeného závěru lze tedy vyvodit, že pokud lze za určitých okolností považovat IP adresu za osobní údaj, tedy údaj přímé či nepřímé identifikace osoby, lze tento údaj použít i v přestupkovém řízení, i kdyby jako nepřímý důkaz.[74]

Určenost osoby je vždy objektivním faktem, tedy rozpoznatelná v konkrétní skupině osob. Osobu lze identifikovat podle subjektivních znaků daných známým údajem. „*Osobní údaj je vždy vztahem mezi reálnou fyzickou osobou a hodnotou údaje.*“[75]

Přitom údaje osobní povahy se člení do několika skupin. Identifikační údaje *„vyjadřují nějakou vlastnost nebo jinou charakteristiku, která se rozlišuje u všech lidí patřících do určité komunity a jejíž používání je formálně podporováno.“* [76]

Teorie navíc rozlišuje objektivní určenost (např. podle DNA) a neurčenost (jméno fiktivního filmového hrdiny).

Určitelnost subjektu údajů může být identifikována i podle menšího počtu údajů, kdy se hovoří o určení nepřímém.[77]

Většina států, tedy i Česká republika, umožňuje používat osobní údaje jiných lidí. Jak již bylo řečeno, existují však omezení, aby se zabránilo jejich zneužití a aby byly zpřístupněny pouze k legálním účelům. Např. Úmluva č. 108 přijatá Radou Evropy 28. ledna 1981 je zaměřena na ochranu osob se zřetelem na automatizované zpracování osobních dat a zahrnuje ustanovení o fyzické osobě, její národnosti, úctě k jejím právům a základním svobodám, o právu na soukromý život, klade důraz na automatizované zpracování osobních údajů vztahujících se k této osobě.[78]

Ochranu osobních údajů lze vnímat v několika samostatných rovinách. Jednu rovinu tvoří základní lidská práva a svobody, další rovinu zahrnuje tzv. rovina právní, kam

[74] BARTÍK, V.; JANEČKOVÁ, E. (2013, s. 12-13).
[75] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 18).
[76] (Tamtéž, s. 21).
[77] BARTÍK, V.; JANEČKOVÁ, E. (2013, s. 11).
[78] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 2,3).

patří ochrana osobních údajů. Již přijetí České republiky do Evropské unie bylo podmíněno náležitou úrovní ochrany osobních údajů opřenou v právních předpisech. Kromě zmiňovaného základního zákona o ochraně osobních údajů je tato problematika upravena i v dalších předpisech, např. v zákoně č. 21/1992 Sb. o bankách je upravena ochrana osobních údajů při provádění bankovní činnosti.[79]

Ochrana osobních údajů a nakládání s nimi existuje již dávno. Reálná hrozba zneužití osobních údajů se pojí s historií teprve nedávnou, např. ve spojitosti s druhou světovou válkou. *„Vždyť např. holocaust nacistického režimu byl u nás významně usnadněn tím, že existovaly nejen matriky, ale dochovaly se i údaje ze statistických sčítání z 30. let, v nichž dotazovaní uvedli údaje o náboženství.“* [80]

Práva a povinnosti při zpracování osobních údajů vyplývají ze zákona o ochraně osobních údajů.

Z hlediska ochrany osobních údajů je rovněž důležitá oblast jejich zpracování. Obecně se rozlišují způsoby automatizované a neautomatizované, příp. manuální. Právní ochrana osobních údajů se často zaměřuje na automatizované zpracování z jeho ekonomického hlediska. Za zpracování osobních údajů se považuje shromažďování listinných dokumentů, jejichž obsahem jsou osobní údaje, např. různé formuláře. Cílem těchto osobních údajů je jejich využití pro další operace v datovém souboru a hromadnou úschovu na nosiči informací.[81] O zpracování osobních údajů se jedná tedy při monitorování kamerami se záznamem pořizovaných snímků, které slouží k případné identifikaci fyzických osob. V tomto případě je správce povinen plnit všechny povinnosti vyplývající ze zákona o ochraně osobních údajů v plném rozsahu. Musí stanovit legitimní účel využití předmětných záznamů, prostředky a způsob zpracování osobních údajů.[82]

Podobné omezení se týká i správce sítě. Je omezen ve svých aktivitách, zejména je povinen stanovit účel, k němuž mají být osobní údaje zpracovány. Rovněž je může uchovávat pouze po dobu, která je nezbytná k účelu jejich zpracování.

[79] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 14).
[80] MATES, P. (2002, s. 38).
[81] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 139, 140, 141).
[82] BARTÍK, V.; JANEČKOVÁ, E. (2010, s. 105).

Samotný internet tedy vyvolává řadu otázek týkajících se soukromí a způsobu, jak je s ním naloženo. Pro děti a dospívající představuje internet nejvýznamnější komunikační kanál, proto je zde na místě jejich obezřetné chování a vnímání rizika narušení soukromí. Proces sebeodkrývání se liší podle uživatelského prostoru a konkrétní aplikace. Jak je tato oblast riziková, naznačuje provedený průzkum projektu EU Kids Online II z roku 2010, z něhož vyplynulo, že v roce 2010 mělo 38 % evropských dětí ve věku 9-12 let profil na nějaké sociální síti, v ČR se jednalo o 52 %, ve věkové kategorii 13-16 let byl zájem 77 % v Evropě a v ČR šlo dokonce o 90 %.[83]

Podle zákona o ochraně osobních údajů je subjektem údajů žijící fyzická osoba bez omezení národností, věkem nebo jinými kritérii ve vztahu k osobním údajům. Po úmrtí subjektu údajů zůstávají v platnosti ustanovení zákona, která nejsou závislá na skutečnosti, jestli je subjektem údajů osoba žijící, nebo zemřelá.[84]

Odpovědnost, která správci a zpracovateli osobních údajů vyplývá ze zákona o ochraně osobních údajů, je odpovědnost objektivní, tzn. odpovědnost za následek jednání nebo opomenutí (za protiprávní stav). V rámci odpovědného subjektu bývá pak odpovědnost delegována na nižší složky, tedy na pracovníky, kteří mají oprávnění zpracovávat osobní údaje. Pokud však správce osobních údajů neprokáže, že dané pracovníky v této oblasti proškolil, považují se veškeré prováděné úkony při zpracování osobních údajů za postupy správcem údajů schválené, tedy v souladu s § 13 odst. 1 zákona o ochraně osobních údajů. Jakmile dojde k ohrožení, nebo dokonce neoprávněnému nakládání s osobními údaji na základě těchto postupů, odpovědnost je na správci osobních údajů.[85]

Přenesení odpovědnosti za zpracování údajů na zpracovatele umožňuje v praxi např. spolupráce s externím specialistou. Tehdy může dojít ke dvěma situacím. Buď půjde o vztah správce – zpracovatel (pouze zpracovatel), nebo správce – správce (jakožto zpracovatel z pohledu primárního správce údajů). Rozdíl spočívá v účelu a prostředcích zpracování osobních údajů, kdy si je určí původní správce nebo pověřený subjekt. K tomu je potřeba dodržovat zákonné podmínky - stanovení účelu a získání souhlasu správce a případně i subjektů údajů. Rovněž zde platí zásada, že správce ve vztahu

[83] MACHÁČKOVÁ, H. Soukromí a sebe-odkrývání na online sociálních sítích. In ŠEVČÍKOVÁ A. a kol. (2014, s. 55, 58).
[84] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 191).
[85] BARTÍK, V.; JANEČKOVÁ, E. (2010, s. 91-93).

k nějakému zpracování nemůže být současně (sám sebou pověřeným) zpracovatelem. Obrácené pořadí možné je. Zpracovatel může být pro jiný účel zpracování správcem.[86]

Přitom zpracovatel pověřený správcem nemůže mít více oprávnění, než mu tento správce předá. Na druhou stranu má více povinností dle zákona o osobních údajích. Ze smlouvy (pověření) o zpracování musí být navíc patrné, v jakém rozsahu, za jakým účelem a na jakou dobu se smlouva uzavírá, rovněž záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. Smlouva je obligatorní i v případě, že právní předpis přímo nestanoví subjektu, který má z povahy věci postavení správce, že bude zpracování osobních údajů provádět subjekt jiný, mající postavení zpracovatele osobních údajů. Pokud totiž zmocnění neplyne z právního předpisu a není stanovena přímo povinnost zpracovávat údaje správcem, může správce svěřit zpracování jiné osobě. [87]

Zákon o ochraně osobních údajů ukládá správci povinnost při shromažďování osobních údajů subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů srozumitelně informovat o jeho právu přístupu k osobním údajům, právu na jejich opravu, jakož i o dalších právech stanovených v § 21 tohoto zákona.

Pokud tedy subjekt údajů požádá o informaci ze svých zpracovaných osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat, a to navíc v rozsahu stanoveného účelu zpracování osobních údajů za pomoci veškerých dostupných informací o jejich zdroji. V průběhu shromažďování osobních údajů by informace měly být poskytovány automaticky. Pokud však o informaci požádá sám subjekt, jde o povinnost zaměstnavatele dle § 12 zákona o ochraně osobních údajů, kde není forma žádosti zákonem stanovena. Tento zákona kontroluje a ověřuje řádný postup zaměstnavatele. Přitom je správce oprávněn požadovat za poskytnutí informace náhradu

[86] MATOUŠOVÁ, M.; HEJLÍK, L. (2008, s. 200).
[87] KUČEROVÁ, A.; BARTÍK, V. a kol. (2003, s. 111).

nákladů v přiměřeném rozsahu, tj. náhradu ve výši, která nepřevyšuje náklady nezbytné na poskytnutí informace.[88]

Při zpracování údajů je rovněž potřeba pamatovat na povinnost mlčenlivosti v oblastech, kde je zákonem uložena informační povinnost.[89] Porušením povinnosti zachovat mlčenlivost se naplňuje skutková podstata přestupku podle § 44 odst. 1 zákona o ochraně osobních údajů. Výše pokuty je limitována částkou 100 000,- Kč.

Při výkladu nejednoznačné právní úpravy nebo u nové právní úpravy napomáhá svými stanovisky Úřad pro ochranu osobních údajů. V jeho kompetenci je i vydávání právních předpisů ve formě vyhlášky. Stanoviska tohoto úřadu ale nejsou obecně právně závazná.[90]

Obecně zaručuje ochranu před neoprávněným nakládáním s osobními údaji zákon č. 40/2009 Sb., trestní zákoník ve svém ustanovení § 180, který považuje i nedbalostní šíření osobních údajů za trestný čin.

Na závěr je vhodné uvést rady Policie ČR, jak se lze účinně bránit zcizení identity (osobních údajů):

- *„věnujte svým dokladům náležitou pozornost a pravidelně kontrolujte, zda Vám žádný z nich nechybí,*
- *chraňte své doklady před kapesními zloději a ukládejte si je výhradně ve vnitřních kapsách blízko těla,*
- *buďte vždy ostražití a při sdělování osobních údajů nezapomínejte na svůj zdravý rozum,*
- *při vyplňování různých dotazníků velmi zvažujte jakékoliv poskytnutí svých údajů,*
- *se svými osobními údaji nikdy nehazardujte, nikomu je nesdělujte výměnou za potenciální možnost finanční odměny, nabídku výhry či získání něčeho zdarma,*
- *vždy se zajímejte, kdo (jaká osoba nebo instituce) zpracovává Vaše údaje, při nákupu prostřednictvím internetu si vždy pozorně čtěte obchodní podmínky,*

[88] KUČEROVÁ, A.; NONNEMANN, F. 2010, s. 81.
[89] KUČEROVÁ, A.; BARTÍK, V. a kol. (2003, s. 142).
[90] KUČEROVÁ, A.; NONNEMANN, F. (2010, s. 82).

- *pravidelně si kontrolujte bankovní účty,*
- *pokud máte pocit, že při výběru peněz z bankomatu Vás někdo sleduje, transakci raději stornujte,*
- *Váš PIN – osobní identifikační číslo nikomu nesdělujte, ani rodinným příslušníkům, Policii ČR, bance. Nikdo nemá právo ho po Vás vyžadovat,*
- *PIN si dobře zapamatujte, ale nikdy nenoste vypsaný na papírku uloženém společně s Vaší platební kartou,*
- *nevyhazujte doklady od provedených transakcí, dokumenty s Vašimi osobními údaji, podpisovými vzory – ty si po nějakou dobu uschovejte. Po čase je nutné je zničit – skartovat, spálit - nikdy neodhazujte písemnosti, dokumenty s osobními údaji např. i potvrzení o výběru z bankomatů do koše, nevíte, kdo je může nalézt a k jakému účelu je později použít proti Vám,*
- *v případě ztráty či odcizení citlivých osobních údajů vyhledejte neprodleně pomoc Policie ČR nejlépe v místě, pokud místo víte, kde k odcizení či ztrátě došlo, nebo nahlaste na linku 158.“*[92]

3.2 Ochrana proti kyberšikaně

Problematika nebezpečných komunikačních jevů je relativně „nová“, prevenci se proto zatím nevěnuje dostatečná pozornost. Přestože 100% ochrana neexistuje, lze alespoň minimalizovat rizika. Ze zahraničních výzkumů prováděných v Anglii, USA, Kanadě a Austrálii v letech 2005-2007 vyplývá, že 25-35 % obětí kyberšikany představují děti. Proto je zásadní dodržovat určitá základní pravidla:

- Vždy respektujte ostatní uživatele.
- Dobře si rozmyslete, co odesíláte a komu – v oblibě je rozesílání sexuálně laděných fotografií, videí či zpráv, ale i jakýchkoli citlivých informací kohokoliv.

[92] Ztráta identity. *Policie ČR*. [online]. 2015. [cit. 2015-9-28]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx.

- Nakládejte se svým heslem jako s vlastním životem - obdobně jako s PIN kreditní karty.
- Nikdy nikomu neznámému nesdělujte své osobní údaje - na dalších veřejných vyhledávačích si lze následně poskládat citlivé informace.
- Seznamte se s pravidly chatu či diskuze, ať víte, co je zakázáno dělat - tím se lze vyvarovat jednání v rozporu s danou službou.
- Seznamte se s riziky, která souvisí s elektronickou komunikací - je třeba být připraven rozpoznat nevhodné projevy.[93]

Jako u všech nežádoucích vlivů působících na dítě je však základním faktorem rodina. Ani u kyberšikany tomu není jinak. Proto je důležité být dítěti správným vzorem k napodobování. Dostupné příručky pro rodiče uvádí následující pravidla pro účinnou prevenci:

- Rodič má být příkladem v používání nových technologií.
- Neměl by zlehčovat pomluvy na internetu.
- Má sledovat online aktivity svého dítěte.
- Má se zajímat, k čemu dítě mobilní telefon nebo internet používá.
- Používat blokační a filtrační software.
- Všímat si neobvyklých varovných signálů.
- Pozorovat chování dítěte při elektronické komunikaci.
- Udržovat a kultivovat s dítětem upřímnou a otevřenou komunikaci.
- Ubezpečit dítě, že má v rodičích důvěru a může přijít s jakýmkoliv problémem.[94]

[93] Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům. *e-Bezpečí.* cz[online]. 2009. [cit. 2015-9-28]. Dostupné z: http://cms.e-bezpeci.cz/content/view/27/6/lang,czech/.
[94] Jak postupovat. *Prevence-info.cz.* [online]. 2015. [cit. 2015-7-20]. Dostupné z http://www.prevence-info.cz/jak-postupovat-3.

Pokud již k ohrožení kybergroomerem dojde, měla by reakce dítěte probíhat ve třech fázích:

- Rozpoznání - je nutné zachovat klid, uvědomit si, že situace je řešitelná. Přesto situaci nezlehčovat.
- První obrana - ukončit komunikaci, nereagovat, neodpovídat ani na nejlákavější sliby nebo nejsilnější pohrůžky. Současně by dítě mělo vyhledat pomoc dospělého a blokovat útočníka. Nezbytné je zajištění důkazů.
- Řešení situace - je nutné nahlásit útok Policii ČR a poskytovateli služeb.[95]

3.3 Ochrana v sociálních sítích

Sociální sítě se staly nerozlučnou součástí každodenního života nejen mladých, ale celé populace. Přibývá počet různých útoků, proto je více než kdy dříve nutná prevence. Zásadní ochranou je opatrnost a obezřetnost při sdělování osobních údajů a informací. Zejména u malých dětí je nezbytné, aby byly seznámeny s tím, co by neměly sdělovat na internetu. Jedná se zejména o adresu bydliště a školy, příjmení, přístupová hesla, rodné číslo, číslo mobilního telefonu, osobní e-mail, věk, intimní fotografie, videa a informace, rodinnou finanční a vztahovou situaci. Bez obav mohou sdělovat křestní jméno své a členů rodiny nebo domácího mazlíčka, své zájmy apod., ovšem bez dalších identifikačních údajů.[96]

Každý uživatel bez rozdílu musí brát v potaz, že sám nese zodpovědnost za informace, které prostřednictvím sociální sítě sdílí s ostatními uživateli. Proto si musí regulovat nastavením informace, které chce zveřejňovat a komu. Určitě je vhodné nezveřejňovat intimní informace a nechlubit se soukromým rodinným životem. Před registrací je nutné si důkladně pročíst podmínky použití a zásady ochrany osobních údajů. Doporučuje se vystupovat pod pseudonymem a určitě nezveřejňovat celé své jméno a příjmení. Přezdívka ochrání soukromí a identitu osoby a navíc zaručí, že přátelé jsou opravdu přátelé.[97]

[95] *KYBERGROOMING A KYBERSTALKING.* (2012, s. 18).
[96] (Tamtéž, s. 10).
[97] Online as soon as it happens. *ENISA* [online]. 2010. [cit. 2015-09-28]. Dostupné z WWW: https://www.enisa.europa.eu/publications/archive/onlineasithappens. s. 36.

Mezi své kontakty (přátele) je bezpodmínečně nutné zařazovat pouze osoby, které uživatel opravdu zná. Při velkém množství kontaktů nelze zaručit, že jsou všichni opravdu známí a v budoucnosti zpřístupněný obsah nezneužijí. Nebezpečnost tohoto jevu není pouze pro uživatele samotného, ale i pro všechny uživatelovy kontakty (přátele). Je zde možnost šíření virů nebo spamů právě prostřednictvím kontaktů.[98]

Dále by si uživatelé měli dávat pozor na to, co publikují na svém profilu. Určitě stojí za úvahu, jestli vloženým obsahem neohrozí sebe nebo osoby kolem sebe, a to i v budoucnu. Proto rovněž existuje nastavení svého soukromí v sociální síti z hlediska vymezení zpřístupnění profilu nikoliv pro každého, ale pouze pro své přátele. Rozhodně se nesděluje přihlašovací jméno ani heslo, a to ani svým blízkým přátelům. Rovněž se nedoporučuje zveřejňovat kontaktní informace, které by mohly vést k identifikaci bydliště nebo pracoviště či školy uživatele. Stejným tabu by měly být informace o odjezdu na delší dovolenou.[99]

Jelikož osobní počítač disponuje velkým množstvím nejen osobních, ale i citlivých dat, není vhodné nechávat další uživatele přihlašovat se ke svým účtům. Na různé druhy reklam by se také nemělo reagovat, pokud nemá uživatel dostatečnou ochranu bezpečnostních systémů. Není ani vhodné nastavovat možnost pamatování si hesla, které usnadňuje přihlášení k účtu pod jinou identitou. Proto je přirozené po každém odchodu ze sítě se také odhlásit. Pro sociální síť by neměla sloužit pracovní e-mailová adresa, ani by neměla být volně dostupná pro svoji poměrně jednoduchou identifikaci konkrétní osoby. S tím úzce souvisí i skutečnost nesdílet žádné informace o zaměstnání nebo firemní kultuře. Neměly by být současně zveřejňovány žádné fotografie, kde je viditelné např. logo nebo adresa firmy. Je rovněž žádoucí neslučovat pracovní kontakty se svými přáteli, a to nejen z hlediska kontroly jednotlivých dat, ale i ohledně obsahu, který není vždy vhodný pro každého.[100]

[98] Online as soon as it happens. *ENISA* [online]. 2010. [cit. 2015-09-28]. Dostupné z WWW: https://www.enisa.europa.eu/publications/archive/onlineasithappens. s. 36.
[99] Online as soon as it happens. *ENISA* [online]. 2010. [cit. 2015-09-28]. Dostupné z WWW: https://www.enisa.europa.eu/publications/archive/onlineasithappens. s. 36.
[100] (Tamtéž, s. 36).

3.4 Ochrana hesla

Jak již bylo několikrát řečeno, heslo se nesmí s nikým sdílet. Patří totiž mezi nejdůležitější prvky ochrany počítače nejen před hackery. K zajištění co nejvyšší ochrany před jeho prolomením je již nutností používání silného hesla. Pravidla pro jeho tvorbu jsou shrnuta v tabulce 1.

Za heslo je považován řetězec znaků, který slouží k přístupu k informacím nebo k počítači. Přístupové heslo bývá delší než běžné, zahrnuje několik slov, jejichž složení tvoří výsledné heslo. Poskytuje totiž vyšší zabezpečení. Hesla a přístupová hesla pomáhají zabránit neoprávněnému přístupu k souborům, programům a dalším elektronickým nástrojům. Proto je při jejich tvorbě nutné vytvořit silné heslo, které nelze snadno uhodnout ani prolomit. Silná hesla se používají u všech uživatelských účtů v počítači, většinou také v podnikové síti.[101]

Tabulka 1: Pravidla pro hesla

Silné heslo splňuje tyto podmínky:	**Silné přístupové heslo splňuje tyto podmínky:**
• Je alespoň osm znaků dlouhé. • Neobsahuje uživatelské jméno, skutečné jméno nebo jméno společnosti. • Neobsahuje úplné slovo. • Je výrazně odlišné od předchozích hesel.	• Je 20 až 30 znaků dlouhé. • Představuje sérii slov, která tvoří frázi. • Neobsahuje obvyklé fráze, se kterými se lze setkat v literatuře či hudbě. • Neobsahuje slova, která lze najít ve slovníku. • Neobsahuje uživatelské jméno, skutečné jméno nebo jméno společnosti. • Je výrazně odlišné od předchozích hesel nebo přístupových hesel.

Zdroj:[102]

[101] Tipy pro vytváření silných přístupových hesel. *Microsoft* [online]. 2015 [cit. 2015-09-28]. Dostupné z WWW: http://windows.microsoft.com/cs-cz/windows7/tips-for-creating-strong-passwords-and-passphrases.

[102] Tipy pro vytváření silných přístupových hesel. *Microsoft* [online]. 2015 [cit. 2015-09-28]. Dostupné z WWW: http://windows.microsoft.com/cs-cz/windows7/tips-for-creating-strong-passwords-and-passphrases.

3.5 Pomoc pro rodiče, jak chránit své děti na sociálních sítích

„Na soukromí lze nahlížet jako na proces udržování interpersonální hranice, v níž jedinec či skupina reguluje interakci s ostatními.“ [103]

Soukromí v životě každého jedince je velmi důležité. Možná ještě důležitější je si ho také udržet. Soukromím si udržujeme odstup od okolního prostředí. Často je však soukromí narušováno, zejména u mediálně známých osob. Ostatní jedinci hltají informace o těchto osobách, chtějí je napodobovat, a proto si ani neuvědomují, že i ony mají právo na své soukromí. Přesto s určitým narušením a veřejným sdílením musí počítat. Jde o určitou daň za slávu. Zobecníme-li právo na soukromí, je na každém jedinci, tedy i na osobách známých, jestli všechny informace o sobě sdělí svému okolí, či nikoliv. Každý si určuje hranici, s čím se veřejnosti svěří. Čím více se však dělí o svůj soukromý život, tím více ztrácí vlastní identitu. A právě otázka udržování soukromí je úzce spjata i se sociální sítí.[104]

Facebook umožňuje nastavení svého soukromí prostřednictvím omezení přístupů, o čemž již byla zmínka v předchozím textu. Realita však ukazuje na nepoučitelnost zejména maminek, které veřejně vystavují pokroky svých malých dětí prostřednictvím fotografií a videí na sociální síti. Radost, pýcha a touha pochlubit se vítězí nad snahou ochránit své dětí. Přitom si snad ani ony samy neuvědomují rizika, kterým své děti vystavují. Nelze se divit, že pak jsou tyto fotografie a videa zneužity cizími osobami, příp. samy děti se mohou stát středem zájmu psychicky narušených jedinců. Další hazard představují veřejně přístupné informace, např. bydliště, příp. s konkrétní adresou. Nejhorší variantou je pak veřejné oznámení na zdi, že v konkrétním období uživatel sítě odjíždí, to vše doplněné dostupnými fotografiemi bytu. To však již bylo v textu řečeno.[105]

Je zkrátka potřeba nesdělovat všechny informace o sobě na veřejně přístupných místech v sociálních sítích, jelikož vždy se zde může pohybovat potencionální nebezpečný jedinec, s nímž je spojeno riziko zneužití daných informací. Přitom se tak nemusí stát

[103] ŠEVČÍKOVÁ, A. a kol. (2014, s. 57).
[104] (Tamtéž, s. 56).
[105] (Tamtéž, s. 56-60).

vzápětí, ale někdy v budoucnu, kdy už sám uživatel na zveřejnění těchto informací dávno zapomněl.

Internet je totiž velmi zrádný z hlediska jasné a plné kontroly nad tím, kdo má ke sdělovaným informacím přístup. Situace není lepší ani v případě komunikace s omezenou skupinkou lidí.[106]

Přes všechna řečená pravidla a možná rizika je závěrem nutno shrnout tzv. „sedm zlatých pravidel online komunikace“, která vyjadřují její specifika:

1. Na internetu je jednoduché vydávat se za někoho jiného. Nelze nikdy s určitostí říct, kdo je kdo.
2. Při online komunikaci se nikdy nesdělují informace, podle kterých je možné uživatele identifikovat (příjmení, adresa bydliště, telefonní číslo, název školy, datum narození apod.).
3. Opatrnost při sdělování informací platí i vůči rodině, např. práce rodičů, odjezdy, každodenní zvyklosti. Snadno se dají zneužít např. zloději.
4. Je nutné zabezpečit profily v sociálních sítích proti veřejnému přístupu cizích lidí ke kontaktním údajům, fotografiím a dalším informacím ze soukromí.
5. Nikde na internetu, zejména ve svých profilech na sociálních sítích, nikdy nezveřejňovat intimní fotografie nebo videa, ani např. fotky v plavkách z dovolené. Mohou být v budoucnu zneužity např. k vydírání.
6. Webkamera se užívá opravdu pouze s osobou, kterou dobře známe (např. při telefonování přes Skype se spolužákem). Na veřejném chatu nebo v kontaktu s cizími lidmi se nedoporučuje zapínat.
7. V žádném případě se před webkamerou nedoporučuje svlékat. Takovéto video lze velmi snadno archivovat a lze ho snadno v budoucnu zneužít.[107]

Shrneme-li již řečené, je bezpodmínečně nutné na internetu:

- Obezřetně zacházet s osobními a citlivými údaji.
- Využívat plně nastavení soukromí.

[106] ŠEVČÍKOVÁ, A. a kol. (2014, s. 56-60).
[107] *KYBERGROOMING A KYBERSTALKING.*(2012, s. 17).

- Seznamovat se s podmínkami užívání, zejména v oblasti poskytování údajů třetím osobám.
- Vždy zachovat chladnou hlavu, nepouštět se do sporů a neoplácet stejnou mincí.
- Nedělat na internetu to samé, co v reálném životě.
- Průběžně sledovat svou digitální stopu, tedy co lze o sobě na internetu nalézt.
- Využívat možnosti technické ochrany počítače (kvalitní a aktualizovaný antivirový program, aktualizovaný operační systém, aktivovanou bránu firewall, programy rodičovské kontroly).[108]

Pokud dojde k nezákonné situaci, je vždy nutné pořídit všechny dostupné důkazy. Zároveň je důležité nahlásit nezákonný obsah poskytovateli služby nebo na kontaktní místo www.horkalinka.net. U trestných činů je zapotřebí kontaktovat Policii České republiky. Jakmile hrozí dítěti psychická újma, doporučuje se vyhledat pomoc psychologa. U kyberšikany mezi spolužáky je vhodné o celé věci vyrozumět školu prostřednictvím výchovného poradce nebo školního psychologa.

[108] MÁCA, R. Děti a rizika sociálních sítí. *Šance dětem* [online]. 2014 [cit. 2015-09-28]. Dostupné z WWW: http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html.

PRAKTICKÁ ČÁST

4 VÝZKUM

4.1 Cíl výzkumného šetření

Výzkum byl proveden formou dotazníkového šetření na vybraných středních školách v Ústí nad Labem a Litoměřicích v období listopad 2015 – prosinec 2015. Výzkumu se zúčastnilo 100 respondentů ve věku 15 – 20 let. Dotazník vyplnilo všech 100 respondentů, z nichž bylo 43 chlapců a 57 dívek. Pro účely dotazníkového šetření jsem na základě konzultace s vybranými pedagogy vytvořila konečnou podobu dotazníku s 20 otázkami zaměřenými na studenty využívající internetové sociální sítě.

Samotný výzkum probíhal téměř dva měsíce. Jeho námětem bylo zaměření na problematiku internetových sociálních sítí s cílem zjistit jejich vliv na studenty středních škol. Učitelé mi vyšli velice vstříc, věnovali mi svůj volný čas i čas ve svých hodinách pro vyplnění dotazníků. Po vyplnění a setřídění dotazníků následovala nejtěžší část celé mé práce, vyhodnocení odpovědí a interpretace získaných výsledků.

K výzkumu této práce bylo využito materiálů, jež byly uplatněny v dřívějších výzkumech těmito autory: Jan Václav Kašpar, Bc. Lubomír Bureš.

4.2 Hypotéza

Aby bylo možné naplnit cíle výzkumu, byly zformulovány následující předpoklady, které se výzkum snaží potvrdit, nebo vyvrátit. Pro můj výzkum jsem si stanovila následující hypotézy:

Hypotéza č. 1 (dále jen „H1“): Každý student střední školy v Ústí nad Labem a Litoměřicích je uživatelem některé z uvedených internetových sociálních sítí (Facebook, YouTube, Twitter, LíbímSeTi, Lidé…….).

Hypotéza č. 2 (dále jen „H2“): Téměř polovina studentů středních škol v Ústí nad Labem a Litoměřicích se již setkala se šikanou přes internetové sociální sítě.

Hypotéza č. 3 (dále jen „H3“): Facebook je nejvyužívanější sociální sítí.

Hypotéza č. 4 (dále jen „H4“): Většina studentů středních škol publikuje obsah na sociálních sítích veřejně.

4.3 Výsledky

Při prezentaci výsledků dotazníkového šetření se držím pořadí, ve kterém byly otázky předkládány respondentům. Odpovědi budou v tabulkách většinou seřazeny od nejvíce častých po nejméně časté. Co se týká výsledků v procentech, ty vypočteme třemi způsoby podle toho, zda si respondenti museli zvolit pouze jednu z nabízených odpovědí (viz otázky číslo 1, 2, 3, 4, 6, 7, 11, 14, 15, 16, 19), nebo jim bylo umožněno zvolit více odpovědí (viz otázky číslo 5, 13, 18), případně museli odpovědět na otevřené otázky (viz otázky číslo 8, 9, 10, 12, 20). V prvním případě jsou počty procent vypočítány ze základu, který tvoří součet odpovědí, a tak se součet procent u jednotlivých položek vždy rovná 100. Ve druhém případě, kdy lze zvolit více odpovědí, vypočítáváme procenta ze základu, který netvoří součet odpovědí, ale je tvořen 100 studenty sociálních sítí. Součet procent jednotlivých položek se tedy nerovná 100. Musím konstatovat, že 2 studenti odpověděli u otázky číslo 6, že nejsou uživateli sociální sítě, odpověděli i na otázku číslo 7 – „proč?“. Dále pak ale odpovídali i na ostatní otázky, které se týkaly studentů - uživatelů sociální sítě. Předpokládám tedy, že tito dva studenti nevěnovali dostatečnou pozornost této otázce, a tudíž jsem pro své vyhodnocení dotazníku počítala s celkovým počtem uživatelů sociálních sítí 100.

Otázka číslo 1 „Pohlaví studentů“ a otázka číslo 2 „Věk studentů“ byly pouze informativní.

Tabulka 2: Pohlaví studentů

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Chlapec	43	43 %
Dívka	57	57 %

Zdroj:[109]

[109] Autor práce, 2016 (vlastní šetření).

Tabulka 3: Věk studentů

KATEGORIE	ČETNOST ODPOVĚDÍ	%
15 let	1	1 %
16 let	18	18 %
17 let	33	33 %
18 let	36	36 %
19 let	11	11 %
20 let	1	1 %

Zdroj:[110]

Otázka číslo 3 „Používáš ve svém volném čase internet?“ byla položena se záměrem zjistit, kolik z dotazovaných studentů používá ve svém volném čase internet.

Tabulka 4: Používáš ve svém volném čase internet?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Ano	100	100 %
Ne	0	0 %

Zdroj:[111]

Odpovědi studentů na tuto otázku nejsou příliš překvapující, neboť z praxe víme, že v dnešní době internet používá skoro každý, protože poskytuje svým uživatelům mnoho užitečných služeb.

Cílem otázky číslo 4 „Kolik času trávíš na internetu?“ a číslo 5 „Jaké stránky nejčastěji používáš?“ bylo zjištění četnosti využívání internetu a poukázání na nejpoužívanější sociální síť mezi studenty středních škol.

Tabulka 5: Kolik času trávíš na internetu?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
2 až 5 hod.	75	75 %
6 až 8 hod.	14	14 %
0 až 1 hod.	7	7 %
12 a více hod.	3	3 %
9 až 11 hod	1	1 %

Zdroj:[112]

[110] Autor práce, 2016 (vlastní šetření).
[111] Autor práce, 2016 (vlastní šetření).
[112] Autor práce, 2016 (vlastní šetření).

Tabulka 6: Jaké stránky nejčastěji navštěvuješ?

KATEGORIE	ČETNOST ODPOVĚDI	%
Facebook	97	97 %
YouTube	56	56 %
Jiné	44	44 %
Seznam.cz	12	12 %
Twitter	4	4 %
Líbím se ti	0	0 %
Lidé	0	0 %
Myspace	0	0 %

Zdroj:[113]

Odpovědi dotazovaných byly v souladu s poznatky z praxe. Je více než zřejmé, že internet je součástí každodenního života a pomalu se na něm studenti stávají závislými. Zde hovoří čísla jasně. Drtivá většina, tři čtvrtiny dotazovaných středoškoláků, tráví na internetu denně dvě až pět hodin. Varovných je také 14 % těch, kteří z celého dne chatují šest až osm hodin. Dané je to také tím, že většina studentů je nyní připojena k internetu téměř všude, kde je signál. Mladí využívají každé volné minuty, jen aby byli online.

Otázka číslo 6 „Jsi uživatelem některé sociální sítě?“ byla položena se záměrem zjistit, kolik z dotazovaných studentů je uživateli internetových sociálních sítí. Tato otázka rozdělovala studenty do dvou skupin. Studenti, kteří kladně odpověděli na tuto otázku, že jsou uživateli, pokračovali otázkou číslo 8. Studenti, kteří odpověděli, že nejsou uživateli, pokračovali následující otázkou číslo 7.

Tabulka 7: Jsi uživatelem některé sociální sítě?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Ano	100	100 %
Ne	0	0 %

Zdroj:[114]

[113] Autor práce, 2016 (vlastní šetření).
[114] Autor práce, 2016 (vlastní šetření).

Tabulka 8: Jestli nejsi, tak proč?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Nemám čas	0	0 %
Nechci sdílet svůj osobní život	0	0 %
Nezajímá mě to	0	0 %
Jiné	0	0 %
Nevím	0	0 %

Zdroj:[115]

Na tuto otázku studenti odpověděli opět zcela podle očekávání. Již dříve jsem uvedla, že z praxe víme, že se sociální sítě stávají stále oblíbenějšími mezi mladými lidmi a nabízejí jim nové komunikační možnosti. Říká se, že kdo v dnešní době nemá Facebook nebo nevyužívá jinou sociální síť, jako by nebyl. Sociální sítě poskytují uživatelům nejenom zábavu formou her, ale také možnosti komunikace s přáteli, seznámení se s novými lidmi z celého světa, sdílení dat a získávání informací.

Otázka číslo 8 „Na jaké sociální síti?“ nás informuje o nejpoužívanější sociální síti mezi studenty středních škol.

Tabulka 9: Na jaké sociální síti?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Facebook	100	100 %
Instagram	31	31 %
YouTube	21	21 %
Twitter	4	4 %
Snapchat	3	3 %
Jiné	2	2 %

Zdroj:[116]

U této otázky vidíme, že nejvíce hlasů získaly odpovědi „Facebook“ a „Instagram“, což je i hlavním smyslem těchto sociálních sítí. Odpovědi dotazovaných studentů opět nepřekvapily, jelikož už dříve jsme zaznamenali, že sociální sítě jsou u studentů pravidelnou součástí jejich dne a pomalu se na nich stávají závislými. Největší četnost odpovědí u Facebooku není zarážející, neboť i celosvětové statistiky tuto sociální síť uvádějí jako nejrozšířenější.

[115] Autor práce, 2016 (vlastní šetření).
[116] Autor práce, 2016 (vlastní šetření).

Otázka číslo 9 „Kolikrát se na profil připojíš?“ zjišťovala četnost využívání sociálních sítí.

Tabulka 10: Kolikrát se na profil připojíš?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
10krát	23	23 %
1 až 2krát	22	22 %
3 až 5krát	20	20 %
celý den	18	18 %
6 až 8krát	17	17 %

Zdroj:[117]

Podle těchto odpovědí studentů můžeme soudit, že sociální sítě jsou v dnešní době fenoménem. Používá je většina studentů, kteří jsou připojeni velkou část svého volného času pomocí počítače nebo notebooku, mobilu či tabletu.

Otázky číslo 10 „Máš svůj profil veřejný, nebo soukromý?“ a číslo 11 „Jak omezujete dostupnost svých příspěvků? “se zaměřily na to, jestli studenti sdílí své informace na sociálních sítích veřejně nebo soukromě.

Tabulka 11: Máš svůj profil veřejný nebo soukromý?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Soukromý	78	78 %
Veřejný	22	22 %

Zdroj:[118]

Tabulka 12: Jak omezuješ dostupnost svých příspěvků?

KATEGORIE		ČETNOST ODPOVĚDÍ	%
Statusy	Vybraní přátelé	18	18 %
	Všichni přátelé	70	70 %
	Přátelé přátel	3	3 %
	Neomezuji, sdílím veřejně	1	1 %
	Nesdílím s nikým	8	8 %
Fotky	Vybraní přátelé	16	16 %
	Všichni přátelé	72	72 %
	Přátelé přátel	4	4 %

[117] Autor práce, 2016 (vlastní šetření).
[118] Autor práce, 2016 (vlastní šetření).

	Neomezuji, sdílím veřejně	1	1 %
	Nesdílím s nikým	7	7 %
Ohlášení své polohy	Vybraní přátelé	10	10 %
	Všichni přátelé	53	53 %
	Přátelé přátel	0	0 %
	Neomezuji, sdílím veřejně	1	1 %
	Nesdílím s nikým	36	36 %
Osobní informace	Vybraní přátelé	20	20 %
	Všichni přátelé	67	67 %
	Přátelé přátel	1	1 %
	Neomezuji, sdílím veřejně	0	0 %
	Nesdílím s nikým	12	12 %

Zdroj:[119]

Z tabulek můžeme vyčíst, že většina studentů má svůj profil soukromý, a co se týče dostupnosti jejich příspěvků na profilech, studenti je obvykle sdílí se všemi přáteli na profilu. V dnešní době si lidé již pomalu začínají uvědomovat rizika sociálních sítí, proto většina lidí nemá profil veřejný.

Otázka číslo 12 „Za jakým účelem sis vytvořil účet?“, otázka číslo 13 „Které z níže uvedených služeb sociálních sítí využíváš?“ a otázka číslo 14 „ Jak většinou trávíš čas na svém profilu?“ nás informuje o důvodu přihlášení respondentů k sociální síti a o jejich obvyklém způsobu trávení času zde.

Tabulka 13: Za jakým účelem sis vytvořil/a účet?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Komunikace	45	45 %
Kamarádi	35	35 %
Nevím	13	13 %
Jiné	11	11 %
Škola	6	6 %

Zdroj:[120]

[119] Autor práce, 2016 (vlastní šetření).
[120] Autor práce, 2016 (vlastní šetření).

Tabulka 14: Které z níže uvedených služeb sociálních sítí využíváš?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Zprávy a chaty	80	80%
Hlavní zeď	70	70%
Fotky	45	45%
Hry	32	32%
Poslech hudby	30	30%
Události	24	24%
Kontrola/návštěva profilů přátel	11	11%
Videokonference	5	5%
Ohlášení své polohy	1	1%

Zdroj:[121]

Tabulka 15: Jak většinou trávíš čas na svém profilu?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Dopisováním	92	92 %
Jiné	15	15 %
Prohlížením profilů	6	6 %
Komentováním fotografií	2	2 %

Zdroj:[122]

Dle četnosti odpovědí můžeme konstatovat, že studenti středních škol si zakládají účet především kvůli hudbě, filmu, komunikaci s kamarády a k hraní her. Sociální sítě využívají především k psaní zpráv a chatům, neboť - jak tvrdí - psaní/komunikaci mezi sebou máme „zadarmo“. Nejméně využívanými službami jsou videokonference a ohlášení své polohy. Zde bych vyzdvihla 13 % těch, kteří odpověděli, že neví. To je ta skupina respondentů, jež si vytvořila účet jen proto, že ho ještě neměla a že nechtěla být tím pádem vyčleněna z kolektivu. Ani tento výsledek není překvapivý. Primárně slouží sociální sítě k tomu, aby se na nich mohli uživatelé bavit mezi sebou, popřípadě sdílet fotky či psát, co vše se jim „honí hlavou“.

[121] Autor práce, 2016 (vlastní šetření).
[122] Autor práce, 2016 (vlastní šetření).

Otázka číslo 15 „Našel/a sis kamaráda nebo kamarádku přes internet?“ a otázka číslo 16 „Viděli jste se někdy osobně?“. Tyto otázky byly položeny s úmyslem zjistit, zda se studenti seznamují na sociálních sítích, poté zda se i setkávají osobně.

Tabulka 16: Našel/a sis kamaráda nebo kamarádku přes internet?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Ano	45	45 %
Ne	55	55 %

Zdroj:[123]

Tabulka 17: Viděli jste se někdy osobně?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Ano	38	84,4 %
Ne	5	11,1 %
Chystáme se	2	4,4 %

Zdroj:[124]

V dnešní době už není překvapivé, že již polovina studentů má zkušenost se seznámením se s kamarády přes internet. Dochází dokonce k osobním setkáním, což může být rizikové (zde je to téměř 50 na 50). Musíme však vzít v potaz, že není jasné, zda studenti hledají na sociálních sítích staré známé kamarády, které již delší dobu neviděli, nebo zda si cíleně vytipovávají nové „objekty“, se kterými by se mohli seznámit, popřípadě zda byli sami zkontaktováni cizí osobou.

Otázka číslo 17 „Máš zkušenost se zneužitím svých osobních údajů? Jestli ano, jakou?“, otázka číslo 18 „Zažil/a jsi na vlastní kůži, že tě někdo na sociálních sítích …?“ a otázka číslo 19 „Zažil někdo z blízkých ve tvém okolí něco podobného?“ Tyto tři otázky se zaměřují na internetovou šikanu a nebezpečné jevy na sociálních sítích.

Tabulka 18: Máš zkušenosti se zneužitím svých osobních údajů? Jestli ano, jaké?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Ne	94	94 %
Ano - zfalšování profilu	3	3 %
Ano - ukradení fotek	2	2 %
Ano - falešný účet	1	1 %

Zdroj:[125]

[123] Autor práce, 2016 (vlastní šetření).
[124] Autor práce, 2016 (vlastní šetření).

Tabulka 19: Zažil/a jsi na vlastní kůži, že tě někdo na sociálních sítích....?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Nezažil/a	48	48 %
Pomlouval	35	35 %
Psal nepravdivé věci o tvé osobě	18	18 %
Obtěžoval	17	17 %
Ztrapňoval	10	10 %
Vyhrožoval	6	6 %
Vydíral	5	5 %
Jiné	5	5 %
Zastrašoval	3	3 %
Využíval	2	2 %

Zdroj:[126]

Tabulka 20: Zažil někdo z blízkých ve tvém okolí něco podobného?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Nevím	48	48 %
Ano	42	42 %
Ne	10	10 %

Zdroj:[127]

Z tabulky 18 je patrné, že téměř polovina dotazovaných má zkušenost s negativními a nebezpečnými jevy na sociálních sítích. Nejčastěji se studenti setkávají s pomluvami, psaním lží o své osobě nebo obtěžováním. Odpovědi na otázku číslo 18 a 19 nám dokazují, že se negativní a nebezpečné jevy na sociálních sítích vyskytují. Internet je plný lží a polopravd, dá se na něj napsat cokoli, veškeré etické kodexy jdou stranou. Svoboda slova je tu neomezená. Proto se pak mnozí diví, že si na internetu o sobě přečtou lži či pomluvy. Z ankety vyplývá, že se s podobnou situací setkal skoro každý druhý. Zde bych mohla parafrázovat staré přísloví, které říká „O kom se píše, žije“. Záleží potom na jedincích, zda chtějí veřejně druhé lidi pomlouvat, či chválit.

Otázkou číslo 20 „Jak trávíš svůj volný čas na počítači?“ jsme zjišťovali, jak respondenti tráví svůj volný čas na počítači.

[125] Autor práce, 2016 (vlastní šetření).
[126] Autor práce, 2016 (vlastní šetření).
[127] Autor práce, 2016 (vlastní šetření).

Tabulka 21: Jak trávíš svůj volný čas na počítači?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Hudba	46	46 %
Film	43	43 %
Chat - komunikace	38	38 %
Hry	33	33 %
Jiné	15	15 %
Škola	11	11 %
Fotky	4	4 %
Facebook	3	3 %
Blogy	3	3 %
Nakupování	1	1 %
Knihy	1	1 %

Zdroj:[128]

Studenti středních škol volili všechny možnosti odpovědí s tím, že nejvíce svého volného času tráví posloucháním hudby, sledováním filmů, komunikací a hraním her. Za těmito aktivitami následovala možnost odpovědi „Dělám věci do školy“.

Z tabulek vyplývá, že studenti středních škol ze sociálních sítí nejvíce využívají síť Facebook.

4.4 Diskuze

Dotazník vyplňovali žáci středních škol z Ústí nad Labem a Litoměřic. Již samotný dotazník bylo velmi náročné vytvořit, neboť jsem chtěla zapojit do jeho vyplňování vždy všechny studenty třídy bez rozdílu, tedy ať už jsou, nebo nejsou uživateli sociálních sítí. S vyplňováním dotazníku jsem byla celkem spokojena. Při mém vyhodnocování výsledků se objevily určité nedostatky, které vyplynuly z nedostatečných zkušeností s vytvářením dotazníků, jako např. ne zcela ideální seřazení otázek a možnosti nabídnutých odpovědí. Samotný dotazník sloužil pouze jako základ, jelikož postupem času a při hodnocení odpovědí jsem si uvědomovala potenciál možnosti rozšíření některých mnou uváděných problémů. Celkově se ale domnívám, že dotazník byl pro studenty středních škol vhodný a že ho všichni přijali velmi kladně

[128] Autor práce, 2016 (vlastní šetření).

především díky zvolenému tématu - Problematika sociálních sítí - a také anonymnímu způsobu vyplňování.

Otázka číslo 6 zjišťovala, kolik studentů je uživateli sociálních sítí. V tomto případě jsem si stanovila následující hypotézu H1: Všichni žáci středních škol v Ústí nad Labem a Litoměřicích jsou uživateli některé z uvedených internetových sociálních sítí (Facebook, YouTube, Twitter, Líbím se Ti, Lidé…….).

Výzkum mé tvrzení **potvrdil**, všichni dotázaní studenti jsou uživateli sociálních sítí, což ukazuje i následující „Tabulka číslo 7".

Tabulka 22: Jsi uživatelem některé sociální sítě?

KATEGORIE	ČETNOST ODPOVĚDI	%
Ano	100	100 %
Ne	0	0 %

Zdroj:[129]

U otázky číslo 6 a otázky číslo 8 jsem si potvrdila, že mladí lidé – žáci středních škol využívají sociální sítě, přičemž nejpoužívanější je síť „Facebook", která patří k nejrozšířenějším. Mezi dalšími sociálními sítěmi byly nejúspěšnější „Instagram" a „YouTube".

Na otázku číslo 12 a 13 studenti nejvíce uváděli jako důvod přihlášení a využití sociálních sítí komunikaci mezi přáteli – tzv. chat. Jako další volili kamarády, poslech hudby, hraní her, sledování filmů.

Otázka číslo 9 byla zaměřena na četnost využívání sociálních sítí. Podle hodnot můžeme vidět, že jsou žáci středních škol sociálními sítěmi „**pohlceni**". Respondenti se k sociálním sítím zpravidla připojují pomocí počítače nebo notebooku, mobilu či tabletu.

Otázka číslo 17, 18 a 19 se týkaly mé hypotézy H2: Téměř polovina studentů středních škol v Ústí nad Labem a Litoměřicích se již setkala se šikanou přes internetové sociální sítě. Víme, že šikana na sociálních sítích existuje. Ze 100 studentů zvolilo možnost „nezažil/a" 48 studentů, což moji hypotézu **potvrdilo**, viz „Tabulka číslo 19".

[129] Autor práce, 2016 (vlastní šetření).

Tabulka 23: Zažil/a jsi na vlastní kůži, že tě někdo na sociálních sítích…?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Nezažil/a	48	48 %
Pomlouval	35	35 %
Psal nepravdivé věci o tvé osobě	18	18 %
Obtěžoval	17	17 %
Ztrapňoval	10	10 %
Vyhrožoval	6	6 %
Vydíral	5	5 %
Jiné	5	5 %
Zastrašoval	3	3 %
Využíval	2	2 %

Zdroj:[130]

Žáci nejčastěji uváděli, že se setkávají s pomluvami, psaním nepravdivých věcí o sobě a obtěžováním. Podle těchto výsledků jsou na sociálních sítích vystaveni nebezpečným jevům, které by se neměly brát na lehkou váhu. Žáci však jsou o šikaně dostatečně informováni a vědí, jak proti tomuto problému bojovat.

Otázka číslo 8 „Na jaké sociální síti?“ se týkala mé třetí hypotézy H3: Facebook je nejvyužívanější sociální sítí.

Tabulka 24: Na jaké sociální síti?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Facebook	100	100 %
Instagram	31	31 %
YouTube	21	21 %
Twitter	4	4 %
Snapchat	3	3 %
Jiné	2	2 %

Zdroj:[131]

Výzkum **potvrdil** mou třetí hypotézu, že Facebook je nejvyužívanější sociální sítí. 100 % respondentů se k této síti připojuje každý den nebo skoro každý den. Tato tabulka ukazuje a potvrzuje návštěvnost sociálních sítí.

[130] Autor práce, 2016 (vlastní šetření).
[131] Autor práce, 2016 (vlastní šetření).

Otázka číslo 10 „Máš svůj profil veřejný, nebo soukromý?“ se týkala mé čtvrté, poslední hypotézy H4: Většina studentů středních škol publikuje obsah na sociálních sítích veřejně.

Tabulka 25: Máš svůj profil veřejný, nebo soukromý?

KATEGORIE	ČETNOST ODPOVĚDÍ	%
Soukromý	78	78 %
Veřejný	22	22 %

Zdroj:[132]

Výzkum mé tvrzení **nepotvrdil**. 78 % respondentů ze středních škol využívá svůj profil jako soukromý. Na jednu stranu chce mladý člověk být na sociální síti, zároveň si chce chránit soukromí a své fotografie či statuty nevystavuje celému světu, ale jen svým „přátelům“. Poslední dobou se sociální sítě snaží co nejlépe zabezpečit uživatelům účet. Pokud bych zpracovávala anketu za rok, věřím, že procento u veřejných profilů bude ještě nižší.

[132] Autor práce, 2016 (vlastní šetření).

ZÁVĚR

Bakalářská práce se zabývá ochranou sociálních sítí a ochranou soukromí. Sociální sítě jsou velmi populární a téměř každý člověk v civilizovaném světě je používá denně. Některé sociální sítě jsme rozebrali a přiblížili. Dále jsem se zabývala výskytem rizik na sociálních sítích, kterých není málo, a jak jim případně předcházet.

Výskyt rizik na internetu se týká všech lidí v jakémkoliv věku na tomto světě, kteří používají počítače, tablety či mobilní telefony. Nejvíce zranitelné jsou samozřejmě děti, protože nemají tolik zkušeností, a proto by se rodiče měli zajímat o to, co jejich potomek dělá nebo vyhledává na internetu a sociálních sítích. Každou nepříjemnou zkušenost si dítě ponese po celý život a může ho to také nepříznivě ovlivnit.

Nebezpečím na sociálních sítích jsem se zabývala ve výzkumné části své bakalářské práce, která potvrdila obrovský zájem o sociální sítě a o vytváření profilů. Důležité zjištění také bylo, že děti se opravdu setkávají s riziky a jsou vystaveny nebezpečím na internetu. Některá zjištění byla až zarážející, jaké zkušenosti děti vlastně mají a čím si doposud prošly. Problémem v dnešní době je, že si rizika bohužel dostatečně neuvědomujeme.

Děti by měly trávit více času se svými rodiči a častěji s nimi komunikovat a svěřovat se. Pozornost a zájem rodičů, co dělají jejich děti, se vždy vyplatí a méně často dochází k negativní zkušenosti dítěte, kterou by si neslo po celý život.

RESUMÉ

Bakalářská práce přibližuje aktuální problém současnosti, a to vliv sociálních sítí a ochranu soukromí. V mé práci poukazuji na sociální sítě a rizika a také popisuji, jak jim předcházet. Výzkum, který jsem prováděla pomocí dotazníkového šetření, se týkal studentů středních škol v Ústí nad Labem a Litoměřicích. Zaměřila jsem se na jejich vztah k sociálním sítím a uvádění osobních údajů a zjištění možné šikany či jiného rizika na těchto sítích.

Bachelor thesis describes the actual problém and that is the influence of social networks and privacy protection. In my work I show on social networks and risks that appear here. I draw attention to them and describe how to avoidthese risks. The research realized throught questionnaire was focus on the students of high school in Ústí nad Labem and Litomerice.I focused on their relationship to social networks, mentioning their person data and the detection of occurence of bullying or other risks on these networks.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

ANDERSON (1996) In DIVÍNOVÁ, R. *Cybersex* : *Forma internetové komunikace*. Praha: TRITON s.r.o., 2005. 167 s. ISBN 80-7254-636-8.

BARTÍK, V.; JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. Praha: Linde, 2010. 263 s. ISBN 978-80-7201-813-0.

BARTÍK, V.; JANEČKOVÁ, E. *Ochrana osobních údajů v životě podnikatele.* Praha: ANAG 2013. ISBN 978-80-7266-811-6.

BURIAN, P. *Internet inteligentních aktivit*. 1. vyd. Praha: Grada, 2014. 332 s. ISBN 978-80-247-5137-5.

ČERNÁ, A. a kol. *Kyberšikana: průvodce novým fenoménem*. 1. vyd. Praha: Grada, 2013. 150 s. ISBN 978-80-210-6374-7.

DAVIDSON, E.; VAAST, E. Tech Talk: An Investigation of Blogging In Technology Innovation Discourse. IEEE Transactions on Professional Communications, 2009, vol 52, no 1. In MATOUŠEK, K.; DOLEŽAL, J. Analýza portálů sociálních sítí pro vědu, výzkum a inovace. *SYSTEMS INTEGRATION*. 2010.

DIVÍNOVÁ, R. *Cybersex* : *Forma internetové komunikace*. Praha: TRITON s.r.o., 2005. 167 s. ISBN 80-7254-636-8.

ECKERTOVÁ, L., DOČEKAL, D. *Bezpečnost dětí na internetu, rádce zodpovědného rodiče*. Brno: Computer Press, 2013, s. 74. ISBN 978-80-251-3804-5.

GŘIVNA, T. a kol. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. 536 s. ISBN 978-80-7478-614-3.

KOPECKÝ, K. STALKING A KYBERSTALKING - NEBEZPEČNÉ PRONÁSLEDOVÁNÍ (studie). Olomouc: NET UNIVERSITY s.r.o., 2010. ISBN 978-80-254-7737-3.

KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. První vydání. Praha: Grada Publishing, a.s., 2015. 183 s. ISBN 978-80-247-5453-6.

KUČEROVÁ, A.; BARTÍK, V. a kol. *Zákon o ochraně osobních údajů. Komentář*. Praha: C. H. Beck, 2003. 388 s. ISBN 80-7179-762-6.

KUČEROVÁ, A.; NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: BOVA POLYGON, 2010. 150 s. ISBN 978-80-7273-163-3.

MACHÁČKOVÁ, H. Soukromí a sebe-odkrývání na online sociálních sítích. In ŠEVČÍKOVÁ A. a kol. *Děti a Dospívající online – vybraná rizika používání internetu.* Praha: Grada Publishing, 2014. 184 s. ISBN 978-80-2107527-6.

MATES, P. *Ochrana osobních údajů*. Praha: Karolinum, 2002. 76 s. ISBN 80-249-0469-8.

MATOUŠEK, K.; DOLEŽAL, J. Analýza portálů sociálních sítí pro vědu, výzkum a inovace. *SYSTEMS INTEGRATION*. 2010.

MATOUŠEK, K., DOLEŽAL, J., KUBALÍK, J., NEČASKÝ, M. Analýza portálu pro podporu sítě informatiků v ČR. In MOLNÁR, Z. Jak využít sociální sítě v podnikání. *SYSTÉMOVÁ INTEGRACE* 1/2011.

MATOUŠOVÁ, M.; HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. ISBN 978-80-7357-322-5.

MOLNÁR, Z. Jak využít sociální sítě v podnikání. *SYSTÉMOVÁ INTEGRACE* 1/2011.

NONNEMANN, F. In KUČEROVÁ, A. a kol. *Zákon o ochraně osobních údajů: komentář.* 1. vyd. Praha: C. H. Beck, 2012. 516 s. ISBN 978-80-7179-226-0.

RAK, R. a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008. 631 s. ISBN 978-80-247-2365-5.

SMEJKAL, V. *Internet @ §§§.* 1. Praha: Grada Publishing, 1999. 168 s. ISBN 80-7169-765-6.

ŠEVČÍKOVÁ, A. a kol. *Děti a dospívající online: vybraná rizika používání internetu*. 1. vyd. Praha: Grada, 2014. 184 s. ISBN 978-80-2107527-6.

ŠMAHEL, D. Děti na internetu. In ŠEVČÍKOVÁ, A. a kol. *Děti a Dospívající online – vybraná rizika používání internetu.* Praha: Grada Publishing, 2014. 184 s. ISBN 978-80-2107527-6.

Seznam použitých internetových zdrojů

ČERNÁ, M.; ČERNÝ, M. Úvod do sociálních sítí: největší rizika. *Metodický portál RVP*. [online]. 2012. [cit. 2015-7-20]. Dostupné z: http://clanky.rvp.cz/clanek/k/g/15077/UVOD-DO-SOCIALNICH-SITI-NEJVETSI-RIZIKA.html/

HOROWITZ, B. Everything in its right place. *Google. Official Blog.* [online]. 2015 [cit. 2015-09-27]. Dostupné z: http://googleblog.blogspot.cz/2015/07/everything-in-its-right-place.html

Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům. *e-Bezpečí.* cz[online]. 2009. [cit. 2015-9-28]. Dostupné z: http://cms.e-bezpeci.cz/content/view/27/6/lang,czech/

Jak se mění facebook. *Úřad pro ochranu osobních údajů.* [online]2013. [cit. 2015-9-27]. Dostupné z: https://www.uoou.cz/jak-se-meni-facebook/ds-2457/archiv=0&p1=2589

JAVŮREK, K. MySpace žije! Měsíčně ho navštíví 50 milionů uživatelů. *Zive.cz* [online]. 2015 [cit. 2015-09-27]. Dostupné z: http://www.zive.cz/bleskovky/myspace-zije-mesicne-ho-navstivi-50-milionu-uzivatelu/sc-4-a-176906/default.aspx#utm_medium=selfpromo&utm_source=zive&utm_campaign=copylink

KASÍK, P. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet.cz* [online]. 2009. [cit. 2015-9-28]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka

MÁCA, R. Děti a rizika sociálních sítí. *Šance dětem* [online]. 2014 [cit. 2015-09-28]. Dostupné z WWW: http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html

Ochrana soukromí na Facebooku?. *Úřad pro ochranu osobních údajů.* [online] 2010. [cit. 2015-9-27]. Dostupné z: https://www.uoou.cz/ochrana-soukromi-na-facebooku/ds-2463/archiv=0&p1=2589

OLANOFF. D. For the last time, let's all say it together: "Google+ is NOT a Social Network". In The Next Web [online]. 2012 [cit. 2015-09-29]. Dostupné z: http://thenextweb.com/socialmedia/2012/03/08/for-the-last-time-lets-all-say-it-togethergoogle-is-not-a-social-network

Online as soon as it happens. *ENISA* [online]. 2010. 49 s. ISBN-13 978-92-9204-036-9 [cit. 2015-09-28]. Dostupné z WWW: https://www.enisa.europa.eu/publications/archive/onlineasithappens

Statistiky sociálních sítí.*Effectix.com.* [online]. [cit. 2015-9-27]. Dostupné z: http://www.doba-webova.com/cs/statistiky-pro-socialni-sit

Tipy pro vytváření silných přístupových hesel. *Microsoft* [online]. 2015 [cit. 2015-09-28]. Dostupné z WWW: http://windows.microsoft.com/cs-cz/windows7/tips-for-creating-strong-passwords-and-passphrases

WOLF, K. Jak překonat nástrahy Facebooku a vytěžit z něj co nejvíce - díl 2. *LUPA.cz* [online]. 2009 [cit. 2015-09-27]. Dostupný z WWW: http://www.lupa.cz/clanky/jak-prekonat-nastrahy-facebooku-dil-2/

WOLF, K. Soukromí a bezpečnost v sociálních sítích prakticky – Facebook díl 1. *LUPA.cz* [online]. 2009 [cit. 2015-09-27]. Dostupný z WWW: http://www.lupa.cz/clanky/soukromi-v-socialnich-sitich-prakticky-facebook/

Ztráta identity. *Policie ČR*. [online]. 2015. [cit. 2015-9-28]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx

2010 Internet Crime Report. *Federal Bureau of Investigation . Internet Crime Complaint Center*. [online]. 2010. [cit. 2015-9-28]. Dostupné z: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

2014 Internet Crime Report. *Federal Bureau of Investigation . Internet Crime Complaint Center*. [online]. 2014. [cit. 2015-9-28]. Dostupné z: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf

Ostatní zdroje

Rozsudek Nejvyššího správního soudu ze dne 12. února 2009, sp. zn. 9 As 34/2008.

Ústavní zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod.

Zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění.

SEZNAM OBRÁZKŮ A TABULEK

Seznam obrázků

Obrázek 1: Návštěvnost vybraných sociálních sítí 12

Seznam tabulek

Tabulka 1: Pravidla pro hesla 41
Tabulka 2: Pohlaví studentů 46
Tabulka 3: Věk studentů 47
Tabulka 4: Používáš ve svém volném čase internet? 47
Tabulka 5: Kolik času trávíš na internetu? 47
Tabulka 6: Jaké stránky nejčastěji navštěvuješ? 48
Tabulka 7: Jsi uživatelem některé sociální sítě? 48
Tabulka 8: Jestli nejsi, tak proč? 49
Tabulka 9: Na jaké sociální síti? 49
Tabulka 10: Kolikrát se na profil připojíš? 50
Tabulka 11: Máš svůj profil veřejný nebo soukromý? 50
Tabulka 12: Jak omezuješ dostupnost svých příspěvků? 50
Tabulka 13: Za jakým účelem sis vytvořil/a účet? 51
Tabulka 14: Které z níže uvedených služeb sociálních sítí využíváš? 52
Tabulka 15: Jak většinou trávíš čas na svém profilu? 52
Tabulka 16: Našel/a sis kamaráda nebo kamarádku přes internet? 53
Tabulka 17: Viděli jste se někdy osobně? 53
Tabulka 18: Máš zkušenosti se zneužitím svých osobních údajů? Jestli ano, jaké? 53
Tabulka 19: Zažil/a jsi na vlastní kůži, že tě někdo na sociálních sítích....? 54
Tabulka 20: Zažil někdo z blízkých ve tvém okolí něco podobného? 54
Tabulka 21: Jak trávíš svůj volný čas na počítači? 55
Tabulka 22: Jsi uživatelem některé sociální sítě? 56
Tabulka 23: Zažil/a jsi na vlastní kůži, že tě někdo na sociálních sítích…? 57
Tabulka 24: Na jaké sociální síti? 57
Tabulka 25: Máš svůj profil veřejný, nebo soukromý? 58

SEZNAM PŘÍLOH

Příloha A – Dotazník I

Příloha A – Dotazník

1. **Pohlaví:**
   a) Muž
   b) Žena

2. **Věk:**

3. **Používáš ve svém volném čase internet?**
   a) Ano
   b) Ne

4. **Kolik času na internetu trávíš?**
   a) 0-1 h
   b) 2-5 h
   c) 6-8 h
   d) 9-11 h
   e) 12 h a více

5. **Jaké stránky nejčastěji navštěvuješ?**
   a) Facebook
   b) YouTube
   c) Seznam.cz
   d) Líbím se ti
   e) Lidé
   f) MySpace
   g) Twitter
   h) jiné

6. **Jsi uživatel některé sociální sítě?**

a) Ano
b) Ne

7. Jestli nejsi tak proč?

a) Nemám čas
b) Nechci sdílet svůj osobní život
c) Nezajímá mě to
d) Nevím
e) Jiné

8. Na jaké sociální síti?

9. Kolikrát se na profil připojíš za den?

10. Máš svůj profil veřejný nebo soukromý?

11. Jak omezuješ dostupnost svých příspěvků?

1. ***Statusy:***
   a) Vybraní přátelé
   b) Všichni přátelé
   c) Přátelé přátel
   d) Neomezuji, sdílím veřejně
   e) Nesdílím s nikým

2. ***Fotky:***
   a) Vybraní přátelé
   b) Všichni přátelé
   c) Přátelé přátel
   d) Neomezuji, sdílím veřejně
   e) Nesdílím s nikým

3. ***Ohlášení své polohy:***
   a) Vybraní přátelé
   b) Všichni přátelé
   c) Přátelé přátel
   d) Neomezuji, sdílím veřejně
   e) Nesdílím s nikým

4. ***Osobní informace:***
   a) Vybraní přátelé
   b) Všichni přátelé
   c) Přátelé přátel
   d) Neomezuji, sdílím veřejně
   e) Nesdílím s nikým

12. Za jakým účelem sis si vytvořil účet?

13. Které z níže uvedených služeb sociálních sítí využíváš?

a) Hlavní zeď
b) Zprávy a chaty
c) Videokonference
d) Fotky
e) Ohlášení své polohy
f) Události
g) Hry
h) Poslech hudby
i) Kontrola/návštěva profilů přátel

14. Jak většinou trávíš čas na svém profilu?

a) Dopisováním
b) Prohlížením profilů
c) Komentováním fotografií
d) Jiné

15. Našel/a sis kamaráda nebo kamarádku přes internet?

a) Ano
b) Ne

16. Viděli jste se někdy osobně?

a) Ano
b) Ne
c) Chystáme se

17. Máš zkušenosti se zneužitím svých osobních údajů? Jestli ano, jaké?

18. Zažil/a jsi, na vlastní kůži, že tě někdo na sociálních sítích…….?

a) Obtěžoval
b) Vyhrožoval
c) Pomlouval
d) Ztrapňoval
e) Zastrašoval
f) Vydíral
g) Využíval
h) Psal nepravdivé věci o tvé osobě
i) Jiné
j) Nezažil/a

19. Zažil někdo z blízkých ve tvém okolí něco podobného?

a) Ano
b) Ne
c) Nevím

20. Jak trávíš svůj volný čas na počítači?

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Sabina Eisnerová
Obor: Sociální a mediální komunikace
Forma studia: Kombinované studium
Název práce: Sociální sítě a ochrana soukromí
Rok: 2016
Počet stran textu: 60
Celkový počet stran příloh: 5
Počet titulů českých použitých zdrojů: 24
Počet internetových zdrojů: 17
Vedoucí práce: Mgr. Tatiana Iskanderová, Ph.D.