Kovářová, Pavla

Informační bezpečnost a digitální stopy

In: Kovářová, Pavla. *Informační bezpečnost žáků základních škol : lekce v knihovnách.* Vydání první Brno: Filozofická fakulta, Masarykova univerzita, 2019, pp. 13-50

ISBN 978-80-210-9270-9; ISBN 978-80-210-9271-6 (online : pdf)

Stable URL (handle): https://hdl.handle.net/11222.digilib/141117
Access Date: 19. 02. 2024
Version: 20220831

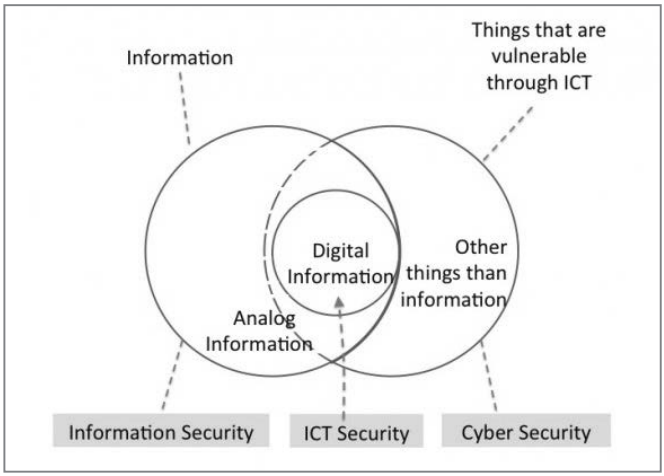
1 INFORMAČNÍ BEZPEČNOST A DIGITÁLNÍ STOPY

Označení *informační bezpečnost*, podobně jako digitální stopy (kap. 1.2), se objevuje v laickém vyjadřování spíše v intuitivním pojetí. I v odborných publikacích nepanuje shoda na obsahu termínu, k čemuž v českém prostředí přispívá jazykové omezení pro přenos ze zahraničních poznatků. Z historického pohledu se pojem vázal na technické zabezpečení informačních systémů, čímž problematika jednoznačně spadala do oblasti zájmů počítačové vědy (informatiky). Se zvyšujícím se počtem uživatelů v elektronickém prostředí, rozmachem internetu a následně Webu 2.0 se výrazně zvyšoval vliv člověka jako prvku informačního systém[12], a tak docházelo k postupnému vývoji od *information security* (ve smyslu technického zabezpečení) k *information safety* (bezpečí v informačním prostředí na úrovni sociální). Právě na druhou oblast je kladen důraz v této publikaci. Nicméně obě oblasti není možné zcela oddělovat, protože se úzce doplňují a prolínají. Kromě základního vymezení lze i v oblasti technického zabezpečení najít při konkrétnější terminologii doklad, že problematika informačního zabezpečení má jasnější vztah k informační než počítačové vědě, jelikož není omezena na spojení s IT, jak dokládá Obrázek 1 Informační bezpečnost ve vztahu k IT.

Informační bezpečnost je možné chápat jako ochranu před ohrožením způsobeným informacemi a s nimi spojenými technologiemi (pro účely publikace je pojem informační bezpečnost používán ve smyslu bezpečí s vědomím souvisejících prvků zabezpečení, obecně zahrnuje oba tyto významy). S rozvojem využití IT ve všech oblastech života se zvyšuje význam právě oblasti digitálních informací, a to od velmi malých dětí (Chang[13] uvádí vystavení dětí internetu od dvou let) po seniory.

12 POŽÁR 2005, s. 54–55.

13 CHANG 2010, s. 501.



Obrázek 1 Informační bezpečnost ve vztahu k IT[14]

Bezpečnostní problémy mohou vznikat v rámci různých fází práce s informacemi. V souladu se standardem mediální a informační gramotnosti[15] je možné klasifikovat tyto fáze jako získání, evaluace a tvorba. Již získávání informací je regulováno zákonnými a etickými pravidly, především v kontextu dodržování autorských práv, ale třeba i v rámci komunikace (např. využití manipulativních technik). Po získání informací by mělo následovat jejich posouzení, jehož výsledek je často klíčový pro odpovědné chování při práci s informacemi. Evaluace je proto významnou složkou jak práce se získanými informacemi, tak jejich tvorby. Ve chvíli, kdy jsou vytvořené informace zaznamenány, je lze označovat jako digitální stopy. Právě ty tvoří základ, příp. faktor zvyšující úspěšnost většiny informačních útoků, které jsou dnes diskutovány nejen ve směru k dětem na základních školách. Dítě by mělo vědět, jak se může bránit z pozice možné oběti, ale i jak se nestát útočníkem. S ohledem na standard mediální a informační gramotnosti a na analýzu RVP (viz kap. 2.1.2) byly proto pro koncepci definovány dva základní tematické ohruhy v rámci informační bezpečnosti: získávání a hodnocení informací a digitální stopy a bezpečná komunikace.

1.1 Získávání a hodnocení informací a jejich zdrojů

Pro tvorbu informací i představy o světě, učení, profesní i osobní život je vždy nutné vycházet z předchozích informací a v případě pocitu jejich nedostatku získat

14 IRGENS 2013.

15 Global Media and Information Literacy (...) 2013.

takové, které aktuální poznání vhodně obohatí. Pro získávání informací je možné využít různých typů informačních zdrojů, mezi kterými vzhledem k rychlosti, ceně, rozsahu a dalším výhodám dominuje internet. Získávání informací nejen z internetu je ale ovlivněno tím, že dostupný je i nelegální nebo pro děti nevhodný obsah. V případě, že dítě tento obsah získá a využije, porušuje etická a někdy i zákonná pravidla.

Aby rozšíření současných znalostí bylo efektivní, je nutné vycházet z vhodných informací, které nejsou zkreslené, ale důvěryhodné. Různé typy informačních zdrojů mají různý účel, kterým může být nejen zjednodušení faktů s ohledem na přiblížení určitého tématu širší veřejnosti, ale i cílená manipulace. Důležité je proto být si vědom kredibility získaných informací, ale i jejich zdrojů nebo poskytovatelů, a tomu přizpůsobit nakládání s nimi.

1.1.1 Získávání informací

Z hlediska informační gramotnosti a bezpečnosti by informace měly být získávány v souladu s pravidly etiky a zákona. V případě, že jsou tato pravidla porušena, jedná se o nevhodný nebo nelegální obsah, jehož získáním dítě může poškozovat někoho jiného (především ve vztahu k autorským právům), nebo samo může být negativně ovlivněno a za určitých okolností je narušen jeho psychický vývoj (např. pornografie, agresivní obsah, extremismus, sekty apod.). I když pro ochranu dětí je možné využít technické nástroje (různé typy filtrů obsahu, bezpečné vyhledávání na Google apod.), s ohledem na jejich limity (viz kap. 1.3.2) jejich bezpečnost ovlivňuje především chování. Pokud děti usilují o získání konkrétního obsahu, jsou vždy schopny najít způsob, jak toho dosáhnout (např. na počítači kamaráda).

Nelegální stahování cizích autorských děl je časté, podle finského výzkumu[16] 71 % dospívajících (15–16 let) ve vzorku během posledního roku nelegálně stáhlo soubor, přičemž 14 % dospívajících to dělá denně. Čím intenzivnější byla tato nelegální aktivita, tím silněji ji dospívající vnímali jako přijatelné chování. Celkově ale 60 % dospívajících vnímalo stahování hudby nebo filmů jako do určité míry nemorální. Dle staršího amerického výzkumu[17] 91 % dětí (8–18 let) si uvědomovalo autorská práva, ale přesto stahovaly soubory, více než polovina hudbu a třetina hry, o něco méně dětí pak komerční software a filmy. Nejčastěji uváděné důvody pro nelegální stahování softwaru byly ty, že nemají peníze na zaplacení (51 %), nepoužívaly by ho, kdyby za něj museli platit (35 %), a že to dělá hodně lidí (33 %). Oproti tomu třetina dětí si nebyla jistá, zda je v pořádku nahrát software na internet bez placení, a třetina si byla jistá, že je to v pořádku.

16 AALTONEN 2013.

17 Majority of Youth Understand (...) 2004.

Z hlediska autorského zákona je proto nutné věnovat se jak aspektu získávání, tak i dalšího sdílení, které (pokud se nejedná o dílo s to umožňující licencí nebo o vlastní autorské dílo) je nelegální (viz kap. 1.3.1). Při sdílení nestačí jen vymezit úpravu v autorském zákoně, ale především praktickou aplikaci např. pro uvědomění si, že i při stahování může uživatel současně ještě nestažený soubor sdílet (peer-to-peer sítě, včetně torrentů). Řada děl využívá technologickou ochranu autorských práv (především tvrdé nebo sociální DRM), která může bránit využití staženého souboru. K porušení autorského zákona pak může dojít i tím, že je tato ochrana odstraněna, např. pomocí speciálního softwaru pro kopírování nosičů, využitím nezakoupeného sériového čísla nebo smazáním jména legálního vlastníka e-knihy (sociální DRM). Woolley[18] doporučuje soustředit se na hlubší uvědomování si etického aspektu digitálního pirátství, protože děti sledují spíše osobní zisk, který z toho mají. Současně hrozba potrestání jim připadá vzdálená. V rámci osvěty je proto vhodné poukázat na případové studie, ideálně co nejbližší dětem (tj. situované do České republiky, s nezletilým pachatelem).

Zatímco v případě porušování autorských práv dochází jen k budování nevhodných návyků, v případě jiného typu závadného obsahu může dojít k problematičtějšímu ovlivnění psychického vývoje dítěte. Přesto, že tento obsah může mít negativní vliv na vývoj dítěte, samy děti o něj mají zájem. Vaníčková[19] například uvádí, že si pornografii opakovaně prohlíží 93 % patnáctiletých chlapců a přibližně 60 % dívek. Dle EU Kids online[20] 21 % dětí v posledních 12 měsících vidělo některý z potenciálně poškozujících obsahů (12 % nenávistné zprávy, 10 % omezování příjmu potravy, 7 % fyzické poškozování sebe sama, 7 % zkušenosti s drogami a 5 % spáchání sebevraždy), přičemž Česká republika byla na 1. místě mezi státy z hlediska počtu dětí, které některý ze sledovaných typů obsahu viděly. Pornografie, agresivní obsah, extremismus nebo třeba sekty mohou při dlouhodobém působení vést k tomu, že dítě začne dané jednání považovat za normální. To jej může dovést k nevhodnému chování v reálném prostředí (např. pornografie k prostituci). Dítě si ale také formuje obraz sebe sama, například dospívající může být ovlivněn modelem ideálního vzhledu (což opět může vést k problémům v tradičním prostředí, např. poruchám příjmu potravy).

Jedním z možných řešení je zákaz vyhledávání problematického obsahu dětmi. Toto řešení má ale řadu problémů (náhodný přístup, přístup u kamaráda, nemožnost řešit problém s rodičem kvůli porušení jeho zákazu apod.). Jak ukazuje kap. 1.3, děti by měly vědět, jak na nevhodný a nelegální obsah reagovat, pokud by se s ním setkaly, a aby věděly, že samy nemají zájem o přístup k němu. Základem je proto komunikace s dítětem. Důležité je přitom upozornit, že tento obsah může

18 WOOLLEY 2015.

19 VANÍČKOVÁ 2005, s. 28–29.

20 LIVINGSTONE 2011, s. 98–99.

nabývat různých forem, např. prezentace extremistických názorů může mít formát nejen webové stránky organizace, ale i hudební produkce nebo počítačových her, jejichž primárním cílem je právě přivést děti k přijetí těchto názorů ztotožněním se s daným obsahem.

1.1.2 Hodnocení informací

Při hodnocení informací je nutné přemýšlet nejen nad nimi samotnými, ale i nad jejich zdroji a nad subjekty, které vstupují do procesu distribuce od autora k příjemci. Pro hodnocení není podstatná jen kredibilita informací, ale především to, jak dané sdělení vnímá konkrétní člověk. Při tomto subjektivním hodnocení probíhá cyklus, který Harris[21] nazval zkratkou CAFE (Challenge, Adapt, File, Evaluate). Prvním krokem je výzva k autorovi informace (kdo to je, proč mu věřit apod.), následuje adaptace (skeptické přijetí s ohledem na předchozí znalosti), uložení (zapamatování si se zvažováním dále přijímaných informací) a vyhodnocení (zvážení přínosu informace pro vlastní osobu). V rámci všech kroků dochází ke komparaci poznatků z více zdrojů a zvážení, která informace bude akceptována v případě protichůdných zjištění. Pro vymezení jednotlivých kroků jsou popsány postupy hodnocení informací od těch nejobecněji využitelných až po subjektivní zhodnocení konkrétního argumentu.

Řada informačních zdrojů je spojena se zprostředkovatelem informací. Do této pozice se dostává například knihovna, která ovlivňuje to, jaké informace budou dostupné ve fondu. Při výběru (akvizice) může dojít k tomu, že část informací k tématu bude z různých důvodů chybět. Podobně je tomu například s redakční radou, příp. šéfredaktorem nebo vlastníkem u periodik, kdy opět může být ze zprostředkování odstraněna určitá informace. Důvody vyřazení informace mohou být různé – finanční, politické nebo osobní přesvědčení. Například zprostředkovatel se může obávat, že by zpráva vedla k růstu xenofobie, proto se rozhodne neinformovat o agresi člena minority. Z toho je patrné, že nejde jen o úmyslně manipulativní jednání, výběr informací může být ovlivněn i dobrou vůlí. Zprostředkovatelem může být také internetový vyhledávač, např. Google z finančních důvodů upřednostňoval některé výsledky vyhledávání[22]. Proto je vhodné při hodnocení informací přemýšlet nad tím, kdo je zprostředkovatelem informací a zda mohou existovat důvody ovlivňující způsob prezentace určité informace.

21 HARRIS 2015.

22 Antitrust: Commission probes allegations (...) 2010.

Dalším krokem je hodnocení informačního zdroje, např. článku, videa, ale třeba i diskuzního fóra. Metzger a Flanagin[23] řadí mezi nejčastěji využívané heuristiky:

- reputace (autorita autora, ale i informačního zdroje),
- potvrzení (doporučení známými nebo množstvím neznámých lidí),
- konzistence (potvrzení v jiných, nezávislých zdrojích),
- sebepotvrzení (soulad s předchozími informacemi),
- narušení očekávání (věrohodnost snižují jazykové, typografické a další chyby, pokud zdroj nepůsobí profesionálně, totéž ale platí i naopak – profesionální vzhled nekvalitního zdroje zvyšuje důvěru u příjemce informace),
- přesvědčivost úmyslu (negativní vliv má reklama, komerčnost zdroje apod., pokud tyto prvky nejsou zřejmé, příjemce má opět větší tendenci informaci věřit).

Jako pomůcka pro hodnocení informací bylo formulováno nesčetné množství různých klasifikací kritérií[24]. Mezi často zmiňované, které lze použít na libovolný informační zdroj, patří CRAP test[25] a CARS test[26], které si jsou obsahově podobné, jen dílčí hodnocené prvky jsou utříděné do jiných kategorií:

Currency	Datum publikování, aktualizace, zastarávání tématu	Credibility	Odbornost autora, kontrola kvality (např. recenzní řízení), formální kvalita, emocionální zkreslení
Reliability	Kompletnost a kvalita informací (obsahová i formální)	Accuracy	Aktuálnost, komplexnost, cílová skupina a účel, více úhlů pohledu
Authority	Identifikovatelnost autora, jeho odbornost, vydavatel, sponzor	Reasonableness	Férovost argumentace, konzistence, objektivita, přiměřenost fungování světa
Purpose	Důvod tvorby autorem, žánr (fakta, názor), stereotypy	Support	Dokumentace zdrojů, podepření dalšími zdroji, externí konzistence

Obecné testy je sice možné využít na libovolný zdroj (včetně komunikace, např. v diskuzních fórech[27]), neupozorňují ale na specifika důležitá pro hodnocení konkrétních typů zdrojů. V tom mohou pomoci specializované hodnotící testy, např. SMELL test pro masmédia (viz s. 266).

Po zhodnocení informačního zdroje následuje evaluace konkrétních informací, tedy posouzení argumentace a možné manipulace. Kvalitní argumentace je předpokladem pro přesvědčení příjemce informací o oprávněnosti sdělení. I bez

23 METZGER 2013.

24 CHOI 2015.

25 MCKENZIE 2013.

26 HARRIS 2015.

27 Viz SAVOLAINEN 2011.

ní může informaci přijmout, pokud odpovídá jeho smýšlení, navazuje na to, co již ví, nebo mu ji předkládá někdo, komu důvěřuje (viz heuristiky výše), může se ale jednat o zkreslené pojetí. Pro podložené obhájení věrohodnosti informací je správná argumentace klíčová.

Argumentaci je možné definovat jako „*verbální činnost, která se uskutečňuje prostřednictvím jazyka, a sociální aktivita, která je zpravidla zaměřená na ostatní lidi, a racionální činnost, která je obvykle založena na intelektuálních úvahách*."[28] Argumentace tedy vyjadřuje osobní stanovisko autora určené jiným lidem, proto by ho měl podložit důkazy. Typickým příkladem, kdy se objevují dvě protichůdné argumentace s cílem někoho přesvědčit, je soudní spor – obě strany předkládají podložená tvrzení ke stejné situaci. A rozhodnutí záleží na přesvědčivosti těchto tvrzení.

Pro hodnocení kvality argumentu je možné využít Toulminův model argumentace. Ten definuje několik prvků dobré argumentace[29]:

- Názor, tvrzení: vyjádření závěru, který následně budeme obhajovat;
- Data: fakta podporující tvrzení;
- Záruky: logické spojení mezi daty a tvrzením;
- Podklady: zdroje opravňující záruky;
- Kvalifikátory: určení síly tvrzení (pravděpodobně, téměř...);
- Vyvrácení: vyvrácené argumenty nebo výjimky.

Při hodnocení kvality argumentu tedy příjemce sleduje, jak se pracuje se zdroji dat k tvrzení, jestli z informací závěr logicky vyplývá a zda se správně pracuje s kvalifikátory (např. neoprávněné zevšeobecnění). Naopak varovnými signály by měly být tzv. argumentační fauly, mezi které patří důraz na rozum („každý rozumný člověk ví..."), na emoce, chybná práce s příčinou nebo důsledkem, obsahové chyby, útoky na osoby[30].

Setkat se lze ale i s vyloženě manipulativními přístupy. Ty jsou podobné argumentačním faulům, jde ale o cílené využití jejich podstaty. Může jít také o nesrozumitelnost (např. aby text působil odborně, byť je fakticky chybný), účelový výběr (informací, zdrojů..., včetně toho, že je např. uvedena informace s účelově vybraným původcem, ke kterému má příjemce informací negativní vztah), účelové řazení (např. zařazení nežádoucí zprávy mezi nezajímavé) nebo využití obrazové manipulace. Právě práce s obrazem může být přesvědčivá, zejména u fotografií a videozáznamů stále převažuje tendence důvěry (text je možné manipulovat snáz) a současně jsou lákavější než strohý text. Zkreslení obrazových informací nemusí být náročné, jak ukazuje např. manipulace s fotkou oslav 2. výročí komunistické revoluce, ze které byly postupně odstraňovány politicky nevhodné osoby, až v roce

28 EEMEREN 2004.

29 TOULMIN 2003.

30 Řadu příkladů argumentačních faulů je možné najít v infografice MCCANDLESS 2012.

1967 zůstal na fotce jen Lenin[31]. Ještě snazší je manipulace pomocí grafů, které jsou často přijímány podle prvního dojmu, i když to je zkreslující (např. nezobrazená celá osa, velikost neodpovídající měřítku, 3D zešikmení zvětšující bližší výseky)[32].

Kvalitní hodnocení informací zahrnuje zvážení všech výše uvedených kroků. Při výuce by praktické vyzkoušení mělo být spojeno s informacemi, jejich zdroji a zprostředkovateli, které daná cílová skupina využívá. Pro všechny věkové a profesní skupiny je vhodné upozornit na to, jak hodnotit informaci při vyhledávání na Google[33] nebo jak nakládat s mediálními zprávami, v případě vysokoškolských studentů má smysl věnovat se kritériím hodnocení v odborných databázích nebo hodnocení kvality vědeckých článků. Správná volba praktické situace je klíčová pro efektivitu vzdělávání (viz konstruktivistická výuka v kap. 3.1).

1.2 Digitální stopy jako riziková tvorba informací

Digitální stopy definoval Fish jako: „*záznam vašich interakcí s digitálním světem a jak data, která jsou zanechána za nimi, mohou být využita.*“[34] Tato definice akcentuje pozici člověka jako subjektu vytvářejícího aktivně digitální stopy s možností tuto aktivitu korigovat (byť jen do určité míry). Při zvážení definic z jiných oborů (kriminalistika, marketing, počítačová věda) lze konstatovat, že digitální stopy jsou informace v digitální podobě s vypovídací hodnotou o konkrétní osobě, primárně fyzické, ale i právnické a s reálným potenciálem využití třetí stranou a se zpětným vlivem na osobu, o které vypovídají. Vypovídací hodnota může být zprostředkována elektronickou reprezentací (např. nelze jej identifikovat ve smyslu osobních údajů) nebo spojením digitálních stop z více zdrojů. Reálný potenciál využití vylučuje údaje o uživateli, které jsou v současnosti využitelné jen hypoteticky nebo velmi omezeně. Využití je možné jen při zahrnutí všech tří činností spojených s digitálními stopami, tj. uložení, analýza a vytvoření hodnoty[35]. Zpětná vazba k dané osobě vylučuje anonymizované datové soubory (personifikace, ne personalizace), důraz je kladen na udržení spojení digitální stopy a konkrétní osoby, resp. persony (digitální reprezentace konkrétní osoby).

Pew Research Center[36] dělí digitální stopy na aktivní („*Osobní informace zpřístupněné online záměrným odesláním nebo sdílením informace uživatelem.*“[37]) a pasivní

31 MACDONALD 2007, s. 17.

32 Příklady chyb v grafech, které mohou být využity i jako manipulace viz MAREK 2015.

33 TAYLOR 2014.

34 FISH, Tony. Definition of a digital footprint (again). In: EKE 2012.

35 FISH 2009, s. 21.

36 MADDEN 2007.

37 MADDEN 2007, s. 4.

(„*Osobní informace zpřístupněné online bez jakékoli záměrné intervence od jedince.*“[38]). Aktivní stopy mohou mít různou podobu. Na jedné straně se jedná o informace, které o sobě člověk sám uvádí, např. blogy, informace v registračním formuláři, fotografie, e-maily apod. Proti tomu pasivní vytváří technická zařízení při jejich používání, např. soubory Cookies, záznamy IP adres a činností na navštívených webových serverech, souřadnice GPS (např. pro sledování pomocí mobilního zařízení s GPS přijímačem), videozáznamy z kamer atd. Z hlediska definice je možné mezi pasivní digitální stopy zařadit také informace, které o člověku zpřístupnil online někdo jiný, typově jde ale spíše o údaje blízké aktivním digitálním stopám. Vzhledem k této nejasnosti publikace nebude s pojmy aktivní a pasivní digitální stopa příliš operovat. Toto dělení ale pomáhá vymezit zaměření publikace, která se soustředí na aktivní digitální stopy, jenž ovlivňuje především sám uživatel, příp. digitální stopy, které o uživateli vytvořil někdo jiný.

Jiné dělení, podstatné pro tuto práci, je podle zneužitelnosti informací obsažených v digitálních stopách. Jedno z nich uvádí Král:

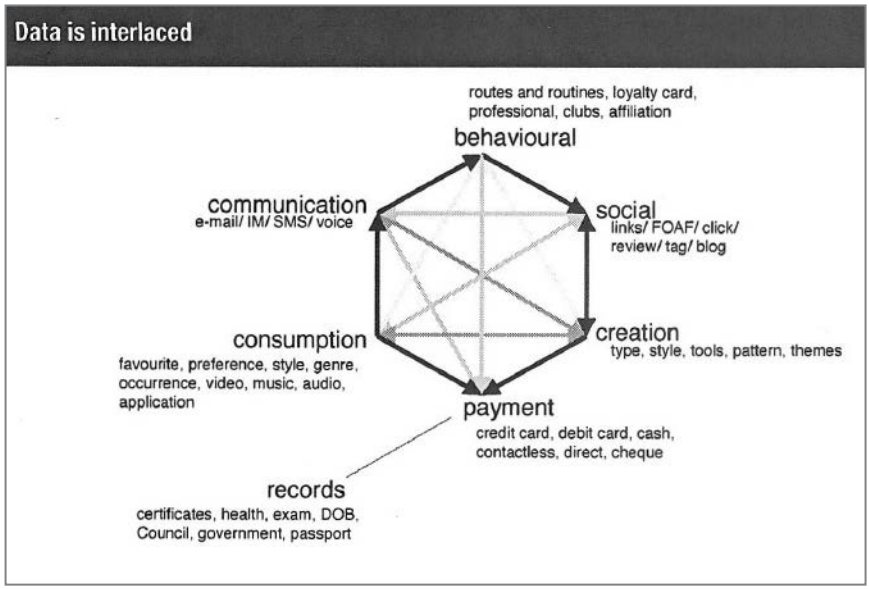
> *„Červená – rodné číslo, číslo pojištění, identifikační čísla (PIN) účtů, rodné jméno matky, informace o zdravotním stavu, trestní rejstřík, podrobné informace o financích, cestovní plány, seznam předchozích zaměstnání, informace o rodině a přátelích vč. jejich telefonních čísel, e-mailových i skutečných adres, atp.*
> *Oranžová (žlutá) – telefonní číslo, adresa, datum narození, stav, zaměstnavatel, vzdělání, e-mailová adresa, oblíbené nákupy, číslo kreditní karty, zájmy a koníčky, spolky a sdružení, navštívené WWW stránky, apod.*
> *Zelená – směrovací číslo, věk, přibližná výše platu, povolání, průzkumy veřejného mínění, atd., pokud tyto informace nejsou ve spojení s jinými, choulostivějšími údaji z předchozích skupin.*“[39]

Problémem tohoto členění je silné zaměření na fyzickou osobu, přestože informace stejného typu a stejných možností využití mohou být spojeny s personou (např. heslo k elektronické službě). Na příkladu e-mailové adresy, která se nachází v prvních dvou kategoriích, je zřejmé, že informace může být zneužitelná na různých úrovních v závislosti na okolnostech. Spojování nevýznamných a významnějších informací vede k vyšší míře užití digitální stopy (viz Obrázek 2). Toto spojení digitálních stop může vést k identifikaci jedince i po anonymizaci datových souborů (odstranění tradičních identifikátorů jako jméno, datum narození apod.)[40].

38 MADDEN 2007, s. 3.

39 KRÁL 2006, s. 100.

40 OHM 2009.



Obrázek 2 Typologie digitálních stop se zdůrazněním spojení[41]

Uvedená kategorizace slouží spíše jako vodítko, vždy záleží na uvážení hodnoty pro konkrétní osobu a situaci, např. při žádosti o zaměstnání je nutné uvažovat jinak než při zakládání profilu v online hře. Především pro děti by měly být za problematické považovány informace o denní rutině a rozvrhu[42]. Podstatné je neopomenout, že se může jednat i o metadata (např. místo pořízení fotky) nebo odvozenou hodnotu (např. lokalizace počítače pomocí IP adresy).

Přestože digitální stopy mohou mít jak jak korektní využití (např. nabídka reklamy odpovídající zájmům), tak i takové, které je pro uživatele nepříjmené, pro tuto práci je podstatnější právě druhá uvedená možnost. Lze konstatovat, že se jedná o zásah do soukromí, jelikož hodnotou informace je její spojení s konkrétní osobou. Pojem soukromí je možné vymezit jako nárok jednotlivců, skupin či institucí sám určit, kdy, jak a v jakém rozsahu jsou informace o nich šířeny dál[43]. Problémem ovšem zůstává, jak dopředu posoudit, zda bude zásah nežádoucí. V uvedené definici by i žádoucí zásah byl narušením soukromí, ale nebyl by pravděpodobně vnímán jako bezpečnostní incident. Dále v publikaci narušení soukromí označuje nežádoucí užití digitálních stop bez ohledu na právní dopad.

41 FISH 2009, s. 79.

42 GRAYSON 2011, s. 24.

43 Volně dle WESTIN 1967.

1.2.1 Vznik a získání digitální stopy

Vznik aktivních digitálních stop závisí většinou na vlastním rozhodnutí člověka, proto by si měl být vědom důsledků, ke kterým jejich zpřístupnění může vést. Digitální stopy člověk zpřístupňuje dvěma základními způsoby:

a) Zveřejněním je informace uložena tak, že je dostupná každému, kdo má odpovídající autorizaci (v případě veřejné informace není nutná) a je možné ji vyhledat a získat. Tyto postupy jsou často legální, pokud nedojde k narušení informačního systému, např. prolomením hesla (viz kap. 1.3.2).
b) V přímé komunikaci může být zpřístupněná informace obsažena v obsahu sdělení (např. text e-mailu) nebo v metadatech[44] (např. kontaktní údaje dalších adresátů v hlavičce odeslaného e-mailu).

S rozvojem Webu 2.0 se výrazně zvýšila možnost uživatele publikovat libovolné informace. Může se jednat o komentáře v diskuzních fórech, fotoalba, vlastní videonahrávky, deníčky (blogy) a další digitální stopy. Tyto informace je pak možné vyhledat, pokud je ponechána často přednastavená možnost veřejného přístupu nebo nedůsledně hlídána autorizace (např. povolení přístupu mobilní aplikace k facebookovému profilu uživatele). Význam autorizace a autentizace si lidé často neuvědomují. Podle Technet.cz[45] přijalo 60 % českých dospívajících mužů a 42 % žen (15–20 let) na sociální síti žádost o přátelství od neznámého člověka druhého pohlaví. Americký průzkum[46] ukázal, že za poukaz na kávu za tři dolary sdělilo své heslo 66 % dotázaných a dalších 19 % jeho formát. V kap. 1.2.3 jsou rozvedeny podrobnosti ke zveřejňování osobních a citlivých informací dětmi, včetně např. fotografie se sexuálním podtextem (pro získání pozitivního ohlasu na vzhled či vyjádření zájmu o vztah, který je pro dospívajícího podstatný pro budování statusu ve vrstevnické komunitě a sebevědomí[47]).

Sociální sítě mohou být snadným zdrojem informací pro internetový útok, protože umožňují získat mnoho údajů na jednom místě. Jedná se také o častý způsob komunikace dítěte (viz Tabulka 1), přes který je snadno dosažitelné a který je pro něj důležitý, je proto problém se v případě útoku (např. kyberšikany) od něj odpoutat. Přitom mnoho profilů obsahuje identifikující informace, 20 % dotazovaných z České republiky má jako součást profilu adresu nebo telefonní číslo a v průměru 2,7 ze šesti sledovaných typů informací[48]. Podle jiného výzkumu[49] byli

44 Přestože tyto typy údajů jsou jen omezeně chráněny zákonem (viz kap. 1.3.1), jejich hodnota může být vysoká, jak zdůrazňuje FISH 2009, s. 19, 44, 177.

45 KASÍK 2009.

46 LEYDEN 2005.

47 Tyto a související psychologické charakteristiky dospívání vedoucí k zveřejňování problematických informací podrobněji popisuje např. ŠIMÍČKOVÁ – ČÍŽKOVÁ 2003.

48 LIVINGSTONE 2011.

49 WALRAVE 2012.

dospívající (10–19 let) ochotni zveřejnit 13 z 18 sledovaných osobních informací a ve srovnání s dospělými statisticky méně často využívali nastavení soukromí. Oolo a Siibak[50] se zaměřili na děti ve věku 14–16 let, které již více využívají postupy pro ochranu soukromí, k čemuž aplikují různorodé strategie od omezování uváděných informací po jejich skrývání mezi jinými informacemi (tzv. sociální steganografie). Zmínit lze také například to, že třetina dospívajících sdílí své internetové heslo s přáteli a čtvrtina neví, že obsah nahraný na internet nemůže být permanentně smazán[51]. Téměř čtvrtina studentů si není vědoma toho, jak snadno může neznámý dospělý získat na sociálních sítích přístup k jejich osobním informacím nebo s nimi zahájit chat[52].

Tabulka 1 Profil dětí na sociálních sítích dle EU Kids Online[53]

	9–10 let	11–12 let
Profil na sociální síti	26 %	46 %
Zcela veřejný profil	28 %	26 %
Částečně veřejný profil	19 %	24 %
Neví o vlastním nastavení profilu	9 %	4 %

Při zohledňování výsledků mezinárodních výzkumů je nutné postupovat uvážlivě, protože byly prokázány rozdíly mezi státy. Pro tuto publikaci jsou podstatné výsledky z ČR[54], která patří ke státům, kde má nejvíce dětí zkušenost s jedním nebo více rizikovými faktory. Na druhou stranu je u nich zjištěn jeden z nejvyšších průměrů v množství online dovedností.

Podle výzkumu Kopeckého[55] sdílí nebo na žádost internetového známého zašle významné množství českých dětí (8–17 let) své osobní informace (v Grafu 1 jsou uvedeny jen informace s výskytem větším než 5 %). Vzhledem k tomu, že tento výzkum je opakován každoročně od roku 2010, po mírném snižování sdílených a zasílaných osobních informací je možné od roku 2013 sledovat zvýšení tohoto rizikového jednání.

50 OOLO 2013.

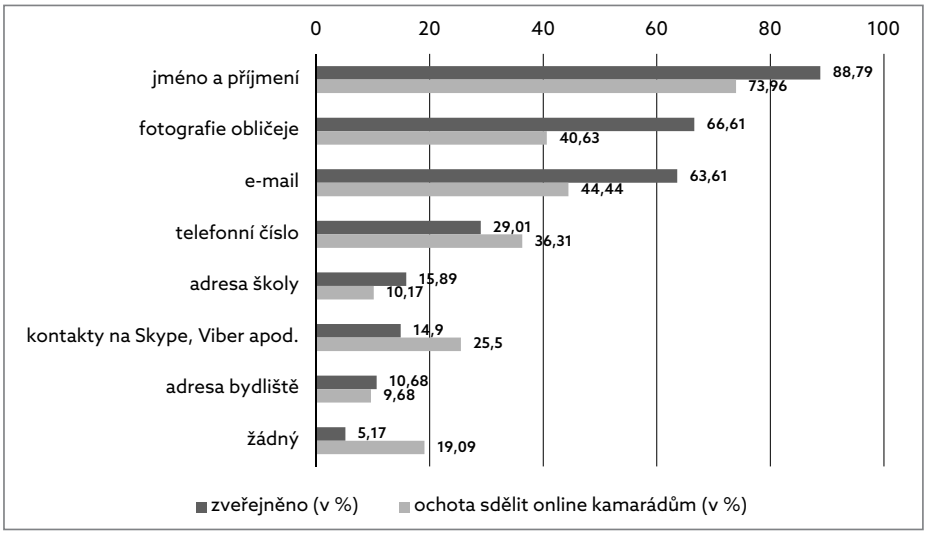
51 JOINER 2005.

52 WEEDEN 2013.

53 LIVINGSTONE 2011; Sběr dat pro tento klíčový výzkum probíhal v letech 2009–2011. Navazující výzkum (LIVINGSTONE 2012) se sběrem dat z roku 2014 byl realizován jen v sedmi státech, kdy nebyla pokryta Česká republika. Vzhledem k dříve zjištěným rozdílům mezi státy a nastavení koncepce vzdělávání na východiska v ČR jsou relevantní spíše starší výsledky, které ČR pokrývají.

54 LIVINGSTONE 2011.

55 KOPECKÝ 2017.



Graf 1 Zpřístupňování osobních informací na internetu dětmi[56]

Hledání zveřejněných digitálních stop je totožné jako u jiných informací. Mnoho lze získat přímo při hledání v nejčastěji využívaných službách, jako je Facebook, příp. přes vyhledávače, které indexují i veřejné informace na sociálních sítích. Problém se může objevit při velkém množství výsledků, ze kterých je těžké získat žádoucí informace, příp. v určení, zda patří ke sledované osobě a ne např. jmenovci. Pro toto ověření se využívá shody informací v různých zdrojích, vzhledu (fotografie apod.), přezdívky, e-mailové adresy a dalších kontaktních údajů. Možnost pro získání smazaných informací, tj. i digitálních stop, představují webové archivy, např. WayBackMachine. Při vyhledání je možné použít různých nástrojů, které mají primárně sloužit jako bezpečnostní opatřední (viz egosurfing v kap. 1.3.3). Pro tento účel lze využít i speciální vyhledávače, tzv. People search engines[57], které se uplatňují především v USA, v českém prostředí nelze využít všech funkcí (např. hledání v databázi kriminálních činů v People Finders). Jejich výhodou je zaměření na digitální stopy fyzických osob, proto jsou výsledky spíše faktografické nejen seznam zdrojů.

Jak bylo popsáno při vymezení digitálních stop (kap. 1.2), může být zjišťována jakákoli informace. Rozdíl je ale ve snadnosti jejich zneužití, ke kterému někdy může dojít až při spojení s dalšími zjištěnými údaji. Proto vznikají cykly zjišťování informací, kdy dříve zjištěné digitální stopy jsou uplatněny pro zvýšení úspěchu dalšího kroku. Důležité je, že citlivější informace takto mohou být získány složitějšími postupy, kdy každý cyklus představuje možnost odhalení útoku na informace.

56 KOPECKÝ 2017, s. 21.

57 Např. Pipl, Spock nebo Spokeo.

Tyto cykly, obvykle začínající u rešerše volně dostupných informací, jsou typické také pro sociální inženýrství. To představuje „*využití podvodu, přesvědčování, vydávání se za jinou osobu, emocionální manipulaci a zneužití důvěry pro získání informace nebo přístupu k počítačovému systému přes člověka.*“[58] Jeho úspěch stojí na přesvědčivých, ale falešných žádostech. Jedná se tedy spíše o psychologický útok, kdy informační technologie jsou jen možným prostředkem. Thomson[59] uvádí, že právě knihovny mohou být jednoduchým zdrojem informací o třetích stranách při sociálním inženýrství. Náchylné jsou především na situace, kdy se jedná o vděk (sociotechnik potřebuje pomoc, protože něco zapomněl a měl by problém), protože základní funkcí knihovny je uspokojování informačních potřeb. K úspěchu také přispívá vydávání se za jinou osobu (např. pracovníka IT oddělení ve velké knihovně), kdy k důvěryhodnosti využívá znalost jazyka, zavedených postupů a osobních informací.

Sociální inženýrství obecně vychází z toho, že prostředkem k získání informace je člověk, jehož slabiny se projevují především vlivem emocí. Aby sociotechnik působil důvěryhodně, musí vystupovat sebevědomě a způsobem, jaký je očekáván, kdyby se nejednalo o falešnou situaci (vč. grafické šablony, která je obvykle využívána osobou, za kterou se sociotechnik vydává). Při samotné interakci usiluje o vyvolání emočního nátlaku, který může být pozitivní (zájem o lákavou nabídku, zvědavost, empatie apod.) nebo negativní (strach z finančního či jiného postihu, krátký časový limit, nebezpečí)[60]. Sociální inženýrství je využíváno, aby byla sdělena informace (např. phishing), ale také aby byl vykonán nějaký čin (např. otevřena příloha e-mailu pro infikování malwarem). Vzhledem ke své efektivitě je podstatou nebo alespoň zvýšením úspěšnosti mnoha internetových útoků.

Protože děti a dospívající mají omezené životní zkušenosti, mohou být více ovlivněny sociálním inženýrstvím, zejména pokud je využito psychických charakteristik typických pro tato vývojová období. Děti, především citově deprivované, mohou být ovlivnitelné z důvodu usilování o uznání a náklonost, roli může hrát také výchova dětí k respektu k autoritám, kdy dítě může podlehnout osobě, která se za autoritu (např. učitele) vydává. V případě dospívajícího roste význam společenských kontaktů a budování vlastního společenského postavení, kdy může podlehnout nabídce, která jej podle jeho názoru přiblíží žádoucímu statusu. Nutné je ovšem připomenou, že navzdory charakteristikám vývojových období je každý jedinec odlišný působením biologických, sociálních a psychologických faktorů. Pro omezení vlivu sociálního inženýrství je zásadní dodržování pravidel bezpečného chování (viz kap. 1.3.3).

Přestože pasivní digitální stopy nejsou pro obsah této publikace tak významné, s aktivními digitálními stopami se ovlivňují a při útoku mohou být využity oba

58 THOMPSON 2013, s. 222.

59 THOMPSON 2013, s. 223–224.

60 MITNICK 2003.

typy. Základní, ale tím také nejvyužitelnější informace nabízí internetový prohlížeč. Další informace poskytují zařízení podle toho, jaké senzory obsahují (např. mobilní telefon může informovat o aktuální pozici, různé softwary a online nástroje mohou zasílat autorovi informace, např. pro zkvalitňování produktu, řešení problémů apod.). Tyto postupy a informace by měly být popsány v licenčních podmínkách daného produktu, které ale většina uživatelů nečte[61]. To je problém především samotného uživatele, ale do určité míry i autora produktu, protože tak lze pochybovat, že byl opravdu udělen informovaný souhlas se zpracováním těchto informací[62]. Svou roli hraje i dynamika dokumentů, opakovaně vznikají nové verze. Opustit zavedenou službu ale nemusí být snadné, i když uživateli přestanou vyhovovat nově nastavené podmínky v oblasti soukromí, jak ukázal pokus Facebooku se službou Beacon[63]. Přitom součástí podmínek nemusí být jen využití digitálních stop provozovatelem produktu, ale také třetí stranou. Podle Bechmann je rozhodnutí o přijetí podmínek využití digitálních stop především u sociálních médií (vč. social-pluginů, např. *Like* nebo *Tweet* na stránkách třetích stran) podmíněno ne jejich obsahem, ale předchozím přijetím přáteli, kterým člověk důvěřuje[64].

1.2.2 Legální narušení informačního soukromí

Narušení informačního soukromí mohou představovat informační incidenty (viz kap. 1.2.3), ale také legální, v některých případech i zákonem dané postupy, např. vyšetřování internetového trestného činu s využitím digitálních stop. K pochopení důvodů proč věnovat pozornost informační bezpečnosti přispívá znalost možných důsledků obou forem využití[65].

Legálně dostupné digitální stopy, především zveřejněné či poskytnuté se souhlasem člověka, kterého se týkají (subjekt údajů), mohou mít vysokou hodnotu pro jejich zpracovatele, ale subjekt údajů může považovat jejich (byť legální) využití za narušení svého soukromí. V marketingu se dlouhodobě prosazuje využití podobných postupů, které jsou popsány u sociálního inženýrství v kap. 1.2.1[66]. Cílený marketing je přizpůsoben zájmům člověka. To je pozitivní jak pro subjekt údajů i pro prodejce, protože se omezí množství reklamy, které je člověk vystaven

61 BECHMANN 2014, s. 22.

62 Toto je nutný předpoklad pro legální zpracování osobních údajů podle práva Evropské unie dle Směrnice Evropského parlamentu a Rady 95/46/ES.

63 FISH 2009, s. 109.

64 BECHMANN 2014, s. 35.

65 CHANG 2010, s. 526.

66 MCLUHAN 2008, s. 20.

a kterou prodejce platí, na tu s větší pravděpodobností úspěchu[67]. To odpovídá přímému prodeji, kdy dobrý prodavač odhaduje na základě pozorování a zkušenosti charakteristiky možného kupujícího[68]. Intenzivnější formu představuje behaviorální marketing[69], který je založený na analýze chování pro jeho predikci. Pokročilá predikce staví na psychografických charakteristikách (nejčastěji dle marketingové segmentace PRIZM do 66 typů) a aktuálně vykonávaných činnostech (od vyhledávacích dotazů, přes geografickou polohu po fyzickou aktivitu, např. zatloukání hřebíků)[70].

Cílený marketing k dětem je často diskutován kvůli etice. Děti mohou být předmětem analýz stejně jako jiní lidé, ale někdy jsou úmyslně využívána prostředí a zájmy spojené primárně s dětmi, např. internetové hry se sociálními prvky pro virální šíření. Informace z profilu dítěte slouží jako zdroj pro cílenou reklamu. Ve hře může být zobrazena reklama formou tzv. product placement, dětem jsou nabízeny produkty s nízkou finanční hodnotou (např. poukaz na hamburger) za informace nebo šíření reklamy. Sofistikované spojení těchto metod bývá označeno jako *game-vertising*[71]. Jinou variantou ceny za produkt je stažení žádaného softwaru[72].

Jako zdroj informací pro marketing i další využití jsou nejvíce využívány vyhledávače (záznamy vyhledávacích dotazů, např. pro včasné detekování počátku chřipkové epidemie[73]) a sociální sítě (např. pro predikci vývoje společenské situace v politicky nestabilních oblastech[74] nebo nezaměstnanosti[75]). Jedná se v zásadě o monitoring společnosti pro předvídání nežádoucích jevů a možnost včasného zásahu. Pro tento účel slouží monitoring digitálních stop i na úrovni jednotlivců. Například senioři jsou monitorováni především pro kontrolu zdravotního stavu (tzv. telemonitoring)[76], v případě dětí se spíše jedná o monitoring místa pohybu, ale také různých činností online (viz mediační strategie v kap. 1.3). Často je využíváno mobilní zařízení, které v současnosti obvykle obsahuje všechny potřebné senzory. Při tomto opatření se někdy děti úmyslně rozhodnou *zapomínat* mobilní telefon doma, aby si uchránily své soukromí před rodiči[77] (viz kap. 1.3.2). Podobně je tomu u monitoringu zaměstnanců, který ale slouží spíše pro ochranu zaměstna-

67 WEAVER 2007, s. 326.

68 MÜLLER 2011, s. 83–85.

69 Part IV: Marketing & Promotion 2006; SULLIVAN, 2011.

70 MÜLLER 2011, s. 87–90.

71 CHESTER 2008.

72 CHESTER 2008.

73 GINSBERG 2008.

74 SUJA 2011.

75 NIKOS 2009.

76 VÁLEK 2009.

77 FISH 2009, s. 64.

vatele. Sledována je pracovní činnost na služebních zařízeních. Mezi eticky i právně problematické postupy patří např. čtení e-mailů[78] v pracovní schránce, ale také v osobní poště otevřené v pracovní době na pracovním počítači, bezproblémové není ani využití kamerových systémů. Podobné prostředky využívají školy pro monitoring chování svých žáků, zejména na sociálních sítích[79].

Ve vztahu zaměstnavatel – zaměstnanec není monitoring jediným využitím digitálních stop. Dle výzkumů jsou často využity digitální stopy při rozhodování o přijetí zaměstnance, s čímž operuje také vzdělávání k digitálnímu občanství[80] (viz kap. 2.3). Vlivem impulzivnosti a experimentování dospívajících[81] a omezené možnosti odstranit vzniklou digitální stopu, může dospívajícím neuvážeností vzniknout problém, který si uvědomí až po letech právě při hledání zaměstnání. Mezi typické nežádoucí záznamy lze zařadit[82] informace o depresích, myšlenkách na sebevraždu, uvěznění, potratu, těhotenství nebo závislosti, ale i fotografie užívání alkoholu či drog a jiného nevhodného chování, nevhodné komentáře, špatné vyjadřování o předchozím zaměstnavateli, nekvalitní sebeprezentace (i jazyková), příp. nepravdivé údaje o kvalifikaci. Na druhou stranu je nutné upozornit, že digitální stopy mohou mít i pozitivní vliv ve vztahu k potenciálnímu zaměstnavateli, když prezentují schopnosti daného člověka. Rozšířenost užití digitálních stop pro tento účel lze doložit výzkumy:

- 59 %[83] – 75 % potenciálních zaměstnavatelů dělá rešerši žadatelů o zaměstnání na sociálních sítích[84];
- totéž dělá 91 % personalistů, využívají především Facebook (76 %), Twitter (53 %) a až následně specializovanou profesní sociální síť LinkedIn (48 %), 69 % dotázaných někdy odmítlo žadatele kvůli jeho digitální stopě[85];
- 26 % manažerů si ověřovalo digitální stopy žadatelů o zaměstnání a 63 % z nich se kvůli výsledku rozhodlo někoho nepřijmout; podobně 26 % administrativních pracovníků vysokých škol hledalo digitální stopy žadatelů o studium.[86]

Monitoring v řízení lidských zdrojů, ať žadatelů o zaměstnání nebo zaměstnanců, slouží jako prevence problému. Když už k němu dojde, přichází ke slovu jiné

78 POŽÁR 2005, s. 282.

79 WEAVER 2010, s. 26.

80 GRAYSON 2011, s. 9–10.

81 VÁGNEROVÁ 2000, s. 210.

82 MOORE 2012, s. 86; SWALLOW 2011.

83 Careerbright. You have been searched – What did we find about you? In: EKE 2012.

84 GRAY, Deborah M. A Linda CHRISTIANSEN. A call to action: The privacy dangers adolescents face through use of Facebook.com. In: MOORE 2012, s. 86.

85 SWALLOW 2011.

86 GRAYSON 2011, s. 9.

uplatnění digitálních stop, a to vyhledávání, analyzování a vyhodnocení v rámci forenzního, příp. kriminálního vyšetřování. Mohou prokázat jak alibi, tak i spáchání nežádoucího jednání. V evropském i českém prostředí bylo diskutováno tzv. data retention, tj. poskytování provozních a lokalizačních údajů od poskytovatelů připojení k internetu a mobilních operátorů pro účely vyšetřování dle zákona č. 127/20058 Sb., o elektronických komunikacích, který byl po zásahu Ústavního soudu[87] právě v této oblasti upraven pro větší ochranu soukromí. Mobilní zařízení lze při vyšetřování využít i jako mikrofony, a to i při vypnutí po vzdálené aktivaci[88]. Na straně pachatelů i vyšetřovatelů jsou používány sofistikované metody práce s digitálními stopami[89]. Rak a Porada[90] uvádějí, že digitální stopy při šetření neslouží jen pro doložení klíčových činností, ale i pro budování profilů zájmových osob, např. pomocí záznamů e-komerce.

Kriminalistika spadá pod výkon veřejné správy. V ní digitální stopy slouží pro ochranu zájmů státu nebo jiných lidí než subjektu údajů (např. ve veřejných informačních systémech typu katastr nemovitostí si může kupující ověřit majitele a případná břemena na nemovitosti). Podle zákona o informačních systémech veřejné správy musí být všechny veřejné rejstříky a systémy dostupné i přes internet. Stát ale i pro své potřeby vytváří nebo požaduje po uživateli vytvoření digitálních stop, které sám využívá[91]. Jedná se například o různé elektronické identifikační karty nebo EET (elektronická evidence tržeb). Stát se tak stává správcem rozsáhlé databáze digitálních stop o každém občanovi, které mohou být zneužity, např. nesprávným chováním úředníka[92].

1.2.3 Informační útoky se zaměřením na dětské oběti

Přestože jedinec může pociťovat narušení soukromí, řada institucí využívá jeho digitální stopy legálně. Způsoby užití digitálních stop uvedené v předchozí kapitole jsou korektní při splnění zákonem daných podmínek (např. omezení cílové skupiny při obsahově nevhodné reklamě, informovaný souhlas při zpracování osobních údajů atp.). Určité typy digitálních stop vznikají i proti vůli člověka, kterého se týkají, většinu ale může ovlivnit. V případě internetových útoků hraje klíčovou roli uvážlivé jednání člověka. Digitální stopy jsou často zneužívány při internetových

87 Nález Ústavního soudu ze dne 22. 3. 2011, spis. zn. Pl.ÚS 24/10.

88 GRAYSON 2011, s. 11-12.

89 Formou kazuistik prezentuje LATTA 2011.

90 PORADA 2006, s. 14.

91 Výhody i nevýhody v oblasti omezení soukromí podrobně popisuje LYON 1994.

92 V roce 2007 společnost HM Revenue and Customs (britská organizace pro oblast daní) ztratila dvě CD s osobními a bankovními informacemi o 25 milionech žadatelů o příspěvek na dítě. Viz NIXON 2010, s. 177.

útocích z jejich podstaty nebo pro podpoření efektivity, roli při tom hraje zkvalitňování technického zabezpečení[93] a omezená informační gramotnost uživatelů. Stále silněji se projevuje, že nejslabším článkem zabezpečení je člověk[94].

Sama ztráta či získání informace je *„významným motivačním faktorem pro páchání trestné činnosti“*[95]. Cílem může být získání dalších, citlivějších informací (viz kap. 1.2.1) nebo poškození uživatele či jeho zařízení (především dat). Obecně mohou být internetové útoky cílené nebo necílené (plošné, např. hoax). Často se ale jedná o stav mezi těmito extrémy, protože určitá cílenost může být dána již jazykovou mutací. Čím méně je útok cílený, tím je méně efektivní, proto oslovuje více potenciálních obětí. Proti tomu cílené útoky jsou sice náročnější, ale o to úspěšnější. Dále jsou popsány vybrané typy informačních útoků, se kterými se mohou běžně setkat děti a dospívající.

Běžný útok pro získání informací nebo jiné formy poškození uživatele představuje využití malwaru (škodlivého kódu). Různé typy malwaru se mohou objevit i na nedostatečně zabezpečeném veřejném počítači, např. v knihovně, kde používání stejného počítače mnoha uživateli znamená přínos pro útočníka. K nákaze může dojít různými způsoby, aktuálně je běžné infikování přes USB disk považovaný za ztracený (např. knihovník jeho užitím chce zjistit, komu disk vrátit), přes software stažený ze služby pro sdílení souborů, přílohu v e-mailu, neošetřenou zranitelnost v prohlížeči, přehrávači videí, klienta pro zprávy atd.[96]

Jak je uvedeno v kap. 1.2.1, mezi útoky pro získání citlivějších informací je možné zařadit phishing a pharming, které jsou založeny na kontaktování uživatele a jeho přesvědčení pomocí sociálního inženýrství o nutnosti zadat autentizační a případně i další údaje do připraveného (podvrženého) formuláře. Získané autentizační údaje jsou obvykle využity ke krádeži identity (viz níže). Často, i když ne nezbytně[97], jsou tyto útoky ve spojení s finančními institucemi. Phishing využívá pro sběr dat podvrženou webovou stránku, proto je možné ho odhalit díky nesprávné URL adrese. Proti tomu pharming využívá tzv. *DNS cache poisoning*, kdy dojde ke změně záznamů DNS pro převod jmenných adres na IP adresy[98], a to buď uložených v počítači uživatele, nebo přímo v DNS serveru. Při pharmingu je pak po zadání správné URL adresy zobrazena podvržená stránka, odhalení je tím náročnější. K získání autentizačních údajů může dojít i uhodnutím či zjištěním specializovaným softwarem. O tento útok se často pokouší i děti, které se tak

93 Institute of Management & Administration. Six Security Threats That Will Make Headlines in ’05. In: THOMPSON 2013, s. 222 .

94 MITNICK 2003.

95 POŽÁR 2005, s. 53.

96 KIM 2011, s. 684.

97 KIM 2011, s. 677.

98 KRÁL 2006, s. 230.

stávají útočníky. Podle výzkumu[99] ve Velké Británii 25 % dospívajících někdy zkusilo prolomit přístup do facebookového účtu jejich kamaráda, přestože si byli vědomi toho, že to není správné. Jak by mělo vypadat silné heslo, aby se omezilo, až znemožnilo prolomení, popisuje kap. 1.3.2.

Při zjištění dostatku informací o oběti se za ni může začít útočník vydávat (krádež identity). Podle toho, jaké údaje zjistil, a kde se jimi může dostatečně prokázat, může vykonávat různé škodlivé činnosti. Pokud byly zjištěny autentizační údaje k elektronickému bankovnictví, může z účtu oběti posílat peníze, žádat o půjčku apod. V případě, že získal přístup do profilu oběti na sociální síti, nabízí se mnoho možností pro kyberšikanu. Pro krádež identity ale nejsou nutné jen autentizační údaje, může se jednat např. o osobní informace, se kterými je vytvořen falešný účet na jméno oběti. Náprava důsledků krádeže identity je velmi složitá, Identity Theft Resource Center odhaduje její časovou náročnost v průměru na 330 hodin[100].

Krádež nebo vytvoření falešné identity může útočník využít i při sexuálně orientovaných útocích často spojovaných s dětmi, což je především grooming a sexting. Je běžné, že útočník mění své jméno, věk i pohlaví[101]. Problém je v tom, že děti se často mylně domnívají, že by v komunikaci dospělého poznaly[102], čímž se zvyšuje rizikové chování. K tomu je vhodné uvést, že 33,2 % dětí na internetu říká vždy pravdu a naopak 2,49 % respondentů absolutně věří tomu, co jim o sobě někdo na internetu říká[103].

Grooming představuje získávání digitálních stop, často z přímé komunikace mezi obětí a útočníkem, kdy cílem je sexuální zneužití dítěte. To nemusí probíhat jen pohlavním aktem ve fyzickém prostředí, může mít i nekontaktní formu, jako svlékání dítěte před webkamerou (sexting, viz další odstavec) nebo vystavení dítěte obscénní komunikaci[104]. Kybergrooming není jen záležitost preferenčních pedofilů[105], pro snadnost úspěchu jej využívají i osoby neschopné navázat partnerství s dospělou osobou, morálně narušení či sexuálně nevyzrálí jedinci experimentující s dětmi a osoby trpící duševní poruchou.

Pokud má dojít ke kontaktnímu zneužití, bývá dlouhodobě budována důvěra dítěte, aby souhlasilo se schůzkou. Při budování vztahu mezi útočníkem a dítětem má opět silný vliv sociální inženýrství, uplatňuje se především při tzv. zrcadlení (útočník se snaží přesvědčit oběť, že má stejné zájmy i problémy, takže si dokonale rozumí). K dospívání totiž patří zájem o hledání (určitou dobu platonického)

99 WEAVER 2010, s. 27.

100 KIM 2011, s. 678.

101 Využití internetu dětmi ve věku od 12 do 17 let 2006.

102 Safer Internet for Children 2007.

103 SZOTKOWSKI 2013.

104 VANÍČKOVÁ 1997, s. 12.

105 VANÍČKOVÁ 1999, s. 33.

partnera[106]. Komunikaci s neznámými uživateli internetu přiznalo 48,59 % dětí, přičemž podle 22,92 % jejich internetový známý žádal, aby jejich komunikace byla udržena v tajnosti. Dalším krokem ke kybergroomingu je osobní schůzka, kterou by odmítlo 50,3 % dětí (17,78 % by ji akceptovalo, 31,02 % nedokáže posoudit, jak by se rozhodlo)[107]. Schůzka je možná i v případě, že útočník o oběti zjistí, kde se nachází, což může být snadné díky již zmíněné oblibě sociálních sítí a zveřejňování místa bydliště, školy a kroužků. Na druhou stranu i děti někdy podléhají kybergroomingu s jasným vědomím situace, např. s vidinou odměny ve formě financí, dárků, nebo jen zájmu, u dospívajících může být pohlavní styk dobrovolný z přesvědčení, že se jedná o lásku[108].

S groomingem souvisí sexting, tj. zasílání sexuálně explicitního obsahu spojeného s obětí[109], který může být následně zveřejněn. Problém se obvykle vyskytuje u dospívajících (méně často dospělých, častěji žen), kteří si tyto záznamy posílají v partnerském vztahu. Po jeho ukončení ale může s cílem pomsty dojít ke zpřístupnění materiálu dalším lidem. Toto byl případ Jessicy Logan a Hope Witsell, které v důsledku sextingu spáchaly sebevraždu[110]. Sexting je problémem i u českých dětí. Podle výzkumu Kopeckého 12,14 % dotazovaných dětí poslalo a 7,41 % zveřejnilo fotografii nebo video, na kterém byly zobrazeny částečně či zcela nahé[111]. I v tomto směru výzkum prokázal výraznou růstovou tendenci v posledních letech. V roce 2012 odeslalo sexuálně laděné materiály 8,99 % dětí, v roce 2014 to bylo 12,14 % a v roce 2017 již 15,47 % dětí[112]. Mezi nejčastější důvody sextingu v ČR patří dárek pro přítele/přítelkyni (38,53 %), flirt (35,47 %) a odpověď na zaslanou „sexy" fotografii, video a podobně (33,73 %). Podle National Center for Missing & Exploited Children 51 % dívek, které takové materiály poslaly, k tomu byly tlačeny chlapcem[113]. Vzhledem k obsahu materiálů u dospívajících při sextingu v podstatě dochází k šíření dětské pornografie, což je trestné.

Zneužití sexuálního zobrazení dítěte zase naplňuje podstatu kyberšikany, která spočívá v poškození s využitím informačních technologií[114], ať už má formu ponižování, pomluvy, pronásledování, sexuálního harašení, záznamu násilí nebo jinou. Kyberšikana proti tradiční šikaně má specifika, která zesilují důsledky pro oběť, jež jsou vázány především na neustálou dostupnost komukoli. Ke kyberšikaně se tak

106 ŘÍČAN 1990, s. 197.

107 SZOTKOWSKI 2013.

108 LEANDER 2008, s. 1261.

109 DÖRING 2014.

110 DÖRING 2014.

111 KOPECKÝ 2015.

112 KOPECKÝ 2017.

113 GRAYSON 2011, s. 30.

114 LIVINGSTONE 2011, s. 61.

mohou přidat nejen děti z okolí, ale miliony lidí na internetu, únik je v podstatě nemožný. Protože při kyberšikaně vznikají digitální stopy jednání způsobujícího oběti újmu, problémem je dlouhodobější působení na oběť a pravděpodobnost, že se poškozující obsah může objevit kdykoli znovu. I v tomto případě již mezi důsledky kromě psychických obtíží patří i sebevraždy dětí, např. Megan Meier[115]. Původci kyberšikany si často nejsou vědomi toho, že jinému ubližují, považují své jednání za nevinnou hru[116]. S kyberšikanou úzce souvisí stalking, nebezpečné pronásledování, které oběť také poškozuje, protože stalker chce, aby o jeho činnosti věděla. Podle Moore[117] zatím stalkeři neobjevili plně sílu IT a stále se silně váží na tradiční metody, proto je pravděpodobné, že se rozšířenost tohoto typu útoků bude zvyšovat. Stalking je v České republice trestný čin, ale až po překročení stanovené úrovně (dlouhodobé, min. 4–6 týdnů, opakované, min. 10 pokusů, obtěžování přítomností útočníka s důvodnou obavou o život či zdraví oběti či jejích blízkých)[118].

Mezi další internetové útoky, se kterými se děti běžně setkávají, by bylo možné zařadit různé typy nevyžádaných zpráv. Ty se šíří přeposíláním, kdy přeposílající neopodstatněně důvěřuje uvedeným informacím (např. řetězové zprávy nebo hoax). Druhou variantou je zneužití kontaktních údajů, které jsou často shromážděny automaticky pomocí robotů (např. rozpoznání typického tvaru e-mailové adresy při procházení webu) nebo jsou prodávány jejich databáze. Rozpoznání těchto zpráv je založeno na identifikaci manipulativních technik (viz kap. 1.2.1), základním bezpečnostním opatřením je tedy hodnocení informací a jejich zdrojů.

1.3 Bezpečnostní opatření

Digitální stopy mohou být využity i zneužity. Bez ohledu na jejich obsah lze najít způsob, jak hodnotu vytěžit. Zanechání pozitivní digitální stopy je žádoucí, ale i ta je výsledkem odpovědného chování při produkci digitálních stop. Je proto vhodné znát a aplikovat bezpečnostní opatření, která omezí možnosti nežádoucího užití digitálních stop.

Jak je uvedeno v kap. 1.2, některé digitální stopy vznikají bez ohledu na přání člověka, kterého se týkají. I když nebude sám využívat žádné elektronické zařízení, s největší pravděpodobností o něm budou existovat stopy, které vytvořil někdo jiný, např. stát. Podstatné tedy není to, jestli digitální stopa člověka existuje, ale jak vypadá na úrovni kvantitativní i kvalitativní. Z hlediska kvalitativního lze rozlišovat, jak snadno informace umožňují identifikaci nebo využití třetí stranou.

115 KIM 2011, s. 679.

116 Safer Internet for Children 2007.

117 MOORE 2012, s. 90.

118 ŠÁMAL 2010, s. 3006–3008.

Kvantitativní rozměr je podstatný proto, že čím více informací o subjektu údajů je dostupných, tím snazší je jejich využití[119].

Pro podporu informační bezpečnosti lze využít různé typy opatření. Chování člověka při práci s IT by nemělo být paranoidní, ale uvážlivé. Pro podporu bezpečnosti lze využít i různých softwarů a online nástrojů, které mohou přispět v různých, ale spíše dílčích směrech. Jako prevence, ale také pro řešení dopadů informačního útoku, mohou pomoci právní předpisy. Všechny tři směry mohou nabývat různé úrovně sofistikovanosti a specifická opatření jsou závislá i na prostředí, do kterého jsou začleněna (např. v zaměstnání). S ohledem na zaměření této publikace budou tři jmenované směry popsány na úrovni, kterou by měly znát děti a dospívající pro omezení nejčastějších typů hrozeb (viz kap. 1.2.3). Současně se jedná o opatření, která jsou určitým způsobem ukotvena v navržených lekcích (kap. 3.2).

Děti, stejně jako rodiče, učitelé nebo knihovníci, mají možnost využít různých opatření pro zvýšení informační bezpečnosti dětí. Bezpečnostní opatření ale mohou snižovat komfort (např. požadavek opakované autentizace) nebo i možnost svobodného přístupu k informacím (např. filtry obsahu), což je zásadní hodnota demokratické společnosti, a také hodnota reprezentující knihovnu. Je proto klíčové zvážit, která opatření aplikovat, aby bylo dosaženo co největší rovnováhy mezi přístupem k informacím a bezpečností. Opatření, která lze aplikovat, jsou předmětem následujících podkapitol.

Není možné definovat jednotnou šablonu vhodných opatření, vždy záleží na individuálním posouzení, např. na základě dřívějšího chování dětí, jejich věku nebo psychických dispozicích. Lidé, kteří pracují s dětmi (zde především učitelé a knihovníci) by také měli zvážit, do jaké míry akcentují právo dítěte na soukromí a nakolik je toto právo omezeno tím, že na informace o dítěti má nárok i jeho rodič[120]. Poskytnutí informací by mohlo poznamenat důvěru dítěte v knihovnu nebo školu.

Mediační strategie knihoven v oblasti práce na internetu jsou popsány jen omezeně[121]. Více pozornosti je věnováno školám[122], primárně se ale odborné publikace zaměřují na rodiče[123], jako klíčové subjekty při řízení přístupu dětí k internetu. Při stanovování možností mediací knihovnou se proto lze inspirovat právě strategiemi odlišných subjektů. Pro přiblížení typů mediačních strategií pro informační bezpečnost je využito klasifikace z výzkumu EU Kids Online[124]:

– Aktivní mediace používání internetu (bez omezení na informační bezpečnost): rozmluva o činnostech dítěte na internetu, přítomnost (rodiče) při

119 ANGWIN 2010.

120 WOLD 2010, s. 72.

121 WOLD 2010.

122 LIVINGSTONE 2011, s. 121-127.

123 LIVINGSTONE 2011, s. 103.

124 LIVINGSTONE 2011, s. 103–130.

používání internetu dítětem, podpora samostatného objevování a učení o internetu, sezení vedle dítěte při používání internetu, společné sdílení aktivit na internetu;
- Aktivní mediace dětské internetové bezpečnosti: vysvětlení, proč jsou některé stránky dobré nebo špatné, pomoc při obtížích udělat nebo najít něco na internetu, navrhování způsobů bezpečného používání internetu, doporučení způsobů chování k jiným lidem online, mluvení o reakcích na pocit poškození něčím na internetu, pomoc s něčím, co dítě v minulosti na internetu poškodilo;
- Restriktivní mediace: stanovení pravidel pro uvedené činnosti, zejména zpřístupňování osobních informací, sdílení fotek, videí nebo hudby, stahování hudby nebo filmů přes internet, vlastní profil na sociální síti, sledování videoklipů na internetu, používání komunikačních služeb;
- Monitoring: kontrola navštívených webových stránek, profilu dítěte na sociální síti nebo v online komunitě, přátel nebo kontaktů přidávaných k profilu na sociální síti, zpráv v komunikačních službách využívaných dítětem;
- Technická mediace: software pro prevenci proti malwaru a nevyžádaným zprávám, filtr obsahu (zejména webu), prostředek sledování navštívených webových stránek, prostředek omezení doby strávené na internetu.

Při volbě mediační strategie by knihovna, stejně jako rodiče, měli zvážit možnosti různých přístupů, jejich výhod i nevýhod a možností kombinací. Vliv může mít prostředí, tedy co je pro danou komunitu obvyklé a akceptované. Podle EU Kids Online[125] patří Česká republika ke státům, kde je nejvíce zastoupena aktivní mediace internetové bezpečnosti (94 % rodičů), naopak restriktivní strategie patří mezi nejméně využívané (78 % rodičů). V oblasti monitoringu a technické mediace Česká republika vykazuje srovnatelné zastoupení s jinými státy. Využití všech mediačních strategií s rostoucím věkem dětí ubývají, především mezi 14. a 15. rokem života[126]. Při hodnocení dle socio-ekonomického statusu nejsou rozdíly kromě aktivní mediace, která se při vyšším statusu také objevuje častěji. To naznačuje skupiny dětí, na které by bylo vhodné zaměřit aktivní mediaci zajištěnou jiným subjektem než rodiči. Přístupy rodičů se liší také podle jejich věku, vzdělání, místa bydliště a dalších faktorů (např. charakteristik, které se u dítěte časem mění, jako délka času strávená na internetu nebo ročník ve škole), které se promítají do úrovně digitální propasti (viz kap. 2.1). Proto je vhodné zvážit i tyto faktory při nastavování mediační strategie knihovny[127].

Dle 72 % dětí by se neměly měnit rodičovské mediace, snížení nebo zvýšení zájmu rodiče o dítě na internetu se objevují ve srovnatelném množství ve zbývají-

125 LIVINGSTONE 2011.

126 LIVINGSTONE 2011.

127 ÁLVAREZ 2013.

cích odpovědích[128]. V ČR přitom zájem o zvýšení zájmu patří mezi nejméně projevované (7 % dětí), naopak ve srovnání s jinými státy české děti pociťují výraznější omezení rodičovskými mediacemi (48 % dětí) a nejčastěji ze všech států ignorují, co jim rodiče o chování na internetu říkají (54 % dětí). To opět podporuje význam aktivní mediace zajištěné vedle rodičů i dalšími subjekty, mezi které patří knihovny. Výhodou škol, kterou uznávají i knihovníci, je jejich možnost zasáhnout všechny děti[129]. Poměrně výrazný, především v České republice[130], je vliv vrstevníků i v mediaci používání internetu, což přispívá k vhodnosti kooperativního učení, které je aplikováno v navržených lekcích (viz kap. 3.2). Subjektem pro poradenství o internetové bezpečnosti mohou být i knihovny, protože již v současnosti je děti uvádějí mezi zdroji pro tyto rady[131], byť ne ve výrazné míře.

Pokud tedy knihovny budou reflektovat přesvědčení rodičů o vhodných přístupech, měly by se zaměřit na aktivní a méně restriktivní mediaci. To umožňuje také nižší omezení přístupu dětí k informacím, spíše na ně bude přeneseno rozhodnutí o způsobu nakládání s informacemi s tím, že si budou uvědomovat jeho důsledky. Toto řešení odpovídá také výzkumu Wolda[132] mezi učiteli a knihovníky v Norsku. Aktivní mediace používání internetu současně vede k snížení poškození dětí na internetu, naopak technická nemá na riziková jednání vliv[133]. Aktivní mediace internetové bezpečnosti a monitoring vedou ke zvýšení rizikového jednání, nicméně se může jednat o strategii učení pro vyrovnávání se s riziky[134]. Proti tomu podle jiného výzkumu[135] vede diskuze dětí s rodiči o problémech zpřístupňování osobních informací na internetu k redukci tohoto jednání dětí.

Wold[136] vidí možnosti knihoven ve srovnání se školami i rodiči jako jedinečné, které by měly být reálně nabízené a podpořené, protože staví na vyšší volnosti přístupu k informacím a také nabídce důvěryhodného místa, na kterém je možné žádat poradenství v tématech, která jsou ve formálnějších prostředích, jako je škola, nepředstavitelné. Podle jeho výzkumu sami knihovníci vidí internetové služby v knihovně jako pokračování jejich tradiční role zpřístupňování informací[137]. Tyto služby zahrnují (především u dospívajících) komunikaci přes internet,

128 LIVINGSTONE 2011.

129 WOLD 2010, s. 71.

130 LIVINGSTONE 2011, s. 124.

131 LIVINGSTONE 2011, s. 127.

132 WOLD 2010.

133 DUERAGER 2012.

134 DUERAGER 2012.

135 ÁLVAREZ 2013.

136 WOLD 2010.

137 WOLD 2010, s. 67.

a nejen vyhledávání informací, podpora těchto činností zlepšuje i vztah dospívajících ke knihovně[138].

Pro zjednodušení s lepší možností prezentace vazeb jednotlivých opatření jsou dále popsány možnosti knihoven v mediaci pro zvýšení bezpečnosti digitálních stop rozdělené do tří kategorií: právní možnosti, technické možnosti a možnosti chování uživatele internetu. Vzdělání, které je klíčovou složkou aktivní mediační strategie, podporuje efektivitu všech jmenovaných oblastí a současně představuje jádro této práce. Při zavedení libovolných opatření nikdy není možné garantovat stoprocentní jistotu bezpečí, protože vždy se může najít cesta kolem opatření. Každé ale staví bariéru, která může být pro konkrétní útok nepřekonatelná nebo odrazující, protože cíl není tak zajímavý, aby útočník vynaložil potřebnou energii.

1.3.1 Právní předpisy

Již stát nastavuje první, minimální úroveň informační bezpečnosti pomocí právních aktů. Zákon musí dodržovat každý, v opačném případě může být potrestán stanovenou sankcí. V případě informační bezpečnosti lze využít jako prevenci nebo řešení dopadu útoku řadu různých předpisů. Vždy záleží na kontextu, nebude zde proto uveden vyčerpávající seznam všech předpisů, které by mohly být aplikovány. Jmenovány budou pouze ty, které jsou nejčastěji využitelné v souvislosti s útoky popsanými v kap. 1.2.3. Všechny dále uvedené předpisy jsou využity ve znění platném ke dni 1. 2. 2018.

V první řadě s ohledem na právní sílu je nutné uvést Listinu základních práv a svobod. Pro oblast informační bezpečnosti se jedná především o čl. 10, kde je zaručena ochrana osobnosti člověka na úrovni pověsti, důstojnosti, jména a cti, ochrana před neoprávněným zásahem do soukromí a „*před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*“[139]. Listina akcentuje údaje o osobě, což je výrazně širší definice než osobní údaj dle zákona č. 101/2000 Sb., o ochraně osobních údajů. Garantována je také ochrana tajemství listovního a jiných písemností a záznamů uchovávaných v soukromí nebo zasílaných poštou, podávaných telefonem, telegrafem a podobným zařízením, tedy i internetem. V těchto směrech jsou sankce stanoveny zákonem č. 40/2009 Sb., trestní zákoník (§ 182 a § 183), kdy tajemství představuje obsah komunikace a dokumentů, ale ne metadatové údaje, přestože i ony mohou prozradit podstatné informace. Bouřlivé reakce nedávno vyvolalo například zveřejnění lokalizačních

138 WOLD 2010, s. 68.

139 Usnesení č. 2/1993 Sb.

anonymizovaných údajů firmou Strava[140]. Naopak čl. 17, odst. 4 Listiny dává právo svobodně vyhledávat a šířit informace, což ale lze omezit zákonem pro ochranu druhých.

Trestní zákoník zahrnuje v současnosti 421 paragrafů, z nichž mnoho může být využito při specifických formách zneužití digitálních stop. Jako příklady lze uvést: § 228 Poškození cizí věci (byl použit při prolomení přístupu k uživatelskému účtu v počítačové hře a jeho zneužití[141]) nebo § 354 Nebezpečné pronásledování (viz kap. 1.2.3). Trestní zákoník upravuje také činy proti majetku při zneužití počítačového systému (§§ 230–232). Trestný je neoprávněný přístup k datům, přihlašovací údaje jsou samy o sobě chráněny jak na úrovni získání, tak i přechovávání, pokud je prokázán úmysl je využít. Poslední jmenovaný paragraf se zaměřuje na poškození dat nebo zásah do vybavení počítače, které je trestné i z nedbalosti, pokud k němu dojde při výkonu funkce, povolání, postavení apod. Zásah i z nedbalosti v zastávané pozici je také v případě neoprávněného nakládání s osobními údaji (§ 180).

Zákon č. 101/2000 Sb. stanovuje ochranu při jakémkoli nakládání s osobními údaji mimo vymezené výjimky, např. zpracování pro osobní potřebu fyzické osoby. Základní charakteristikou osobních údajů je dle § 4, písm. a) jejich schopnost identifikace konkrétní fyzické osoby (jednou informací nebo jejich souborem). Osobním údajem tedy může být i fotografie nebo video, kde je rozeznatelný konkrétní člověk. Citlivé údaje jsou zvláštní typ osobních údajů kvůli vyšší možnosti zneužití, jedná se o informace s potenciálem diskriminace (např. národnost nebo odsouzení za trestný čin) a biometrické údaje, které umožňují přímou identifikaci jedinečnou charakteristikou (např. otisk prstu). Pokud chce kdokoli shromažďovat nebo zpracovávat osobní údaje, musí k tomu mít zákonný důvod nebo poučený souhlas subjektu údajů (zákon definuje, o čem je nutné ho poučit) a zajistit technická a organizační bezpečnostní opatření. Ochrana osobních údajů v nejbližších měsících zaznamená výrazné změny s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, známého též pod zkratkou GDPR. To mimo jiné posiluje ochranu osobních údajů dětí a také ochranu osobních údajů v digitálním prostředí. Pro knihovny byla vytvořena příručka pro snazší přechod na novou úpravu[142].

Zákon č. 480/2004 Sb., o některých službách informační společnosti zahrnuje odpovědnost za obsah služeb informační společnosti, které jsou poskytovány

140 Viz např. MINELLE, Bethany. US military to review security amid Strava fitness app fears. *SkyNews* [online]. 29 January 2018 [cit. 2018-02-07]. Dostupné z: https://news.sky.com/story/us-military-to-review-security-amid-strava-fitness-app-fears-11228045.

141 LochyProduction 2013.

142 DANIELISOVÁ 2018.

na žádost, přičemž žádost i služba sama jsou řešeny elektronicky a slouží zejména pro vyhledávání a zpřístupňování informací. Poskytovatel je odpovědný za obsah, pokud se dozvěděl o jeho protiprávnosti. Tento zákon tedy například umožňuje, aby člověk vyžadoval od provozovatele služby smazání informací, které jsou pomluvou (protizákonné dle § 184 trestního zákoníku), kterou o něm někdo jiný napsal na veřejně dostupnou webovou stránku.

Z hlediska protiprávního obsahu je pro koncepci klíčový zákon č. 121/2000 Sb., autorský zákon (a návazně § 270 trestního zákoníku, který ale přináší blanketní úpravu vázanou na autorský zákon) a jeho porušování především při nelegálním stahování a sdílení autorských děl a obcházení technologických ochran. Autorský zákon vymezuje autorské dílo jako *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam*“[143], autorským dílem není myšlenka, například parafráze tedy není zákonem upravena, ale mělo by se s ní nakládat podle etických pravidel. Autorský zákon specifikuje omezení autorských práv, především v rámci zákonných licencí (citace, užití pro osobní potřebu atd.). Pro řešenou problematiku je ale stěžejní uvědomění si naopak jednání, které je možné autorským zákonem sankcionovat.

Nakládání s elektronickými autorskými díly je ovlivněno určitou nezávislostí na nosiči, kdy jsou umožněny jiné způsoby užití díla spojeného s nosičem (např. možnost půjčování) a bez něj (pro nehmotná díla je jediným možným užitím sdělování veřejnosti). Tento rozdíl například vede k tomu, že není možné půjčování e-knihy bez zaplacení odměny vlastníkovi majetkových autorských práv (pokud e-kniha nebyla zakoupena jako součást čtečky e-knih). Pro všechna elektronická díla je proto nutné důkladné seznámení se s licenčními podmínkami, které specifikují, jaké nakládání s dílem je možné.

Specifická úprava je v autorském zákoně pro počítačové programy (§ 65 a § 66). Většina omezení práv autora v § 66 pokrývá nakládání se softwarem způsoby, které jsou nutné pro jejich korektní využití, ale nebyly by v souladu s jinými částmi zákona (např. vytvoření rozmnoženiny v paměti počítače, tj. instalace). Pro software není možné využít užití pro osobní potřebu, stejně jako další bezúplatné zákonné licence (hlava I, díl 4). Různé typy elektronických děl mohou být spojeny s technickými prostředky ochrany práv, které je zakázáno obcházet (§ 43), stejně jako je zakázáno odstraňovat či měnit elektronickou informaci o správě práv k dílu či podporovat šíření takto upraveného díla (§ 44).

Vedle autorských práv upravuje autorský zákon i práva související, což jsou především práva výkonných umělců. Z tohoto důvodu je proto často porušením

143 Zákon č. 121/2000 Sb., § 2.

zákona, pokud například je bez souhlasu umělce vytvořena nahrávka koncertu a následně je umístěna na internet, a to přesto, že to udělá autor této nahrávky.

Bylo by možné pokračovat jmenováním dalších zákonů, které jsou využitelné při konkrétních internetových útocích, to ale není předmětem této práce. Důležité je uvědomit si, že i když zákonná úprava existuje, její role je na jednu stranu preventivní a na druhou stranu represivní. Jako prevence slouží tak, že lidé, kteří vědí, že by jednali protiprávně, si často čin rozmyslí, protože výsledek je pro ně méně zajímavý než obava z možné sankce. To ale předpokládá, že o dané právní úpravě ví, tato prevence tedy nefunguje bez osvěty. Není nutná znalost konkrétní právní úpravy, je ale potřebné povědomí o možnosti zákonného postihu. Současně ne pro každého je obava z postihu dostatečná, aby jej odradila.

Pokud prevence nebyla účinná, lze předpisy využít při represi. I zde se objevují významné problémy. Prvním je působnost práva, která je ohraničena státními hranicemi a občanstvím (teritorialita[144]). Tu je na internetu snadné obejít, např. využitím elektronických služeb, jejichž poskytovatelé nemají pobočku v ČR, příp. skrytím datových přenosů přes různé státy, kdy není výjimečný problém při předávání informací. V mezinárodním prostředí sice existují snahy o harmonizaci práva, především v rámci Evropské unie, problémy se ale objevují při jednání o dotčení suverenity států. Zásadní vliv má také složitost vzniku právních aktů, které mohou být problémem z hlediska rychlosti vývoje informačních technologií. Problém může nastat také v případě, že poškozený potřebuje podporu, ale neví, na koho se obrátit, příp. mu daná instituce nemůže pomoci kvůli omezeným pravomocím (Policie ČR[145], Úřad pro ochranu osobních údajů[146] atd.). Poškozený také nemusí vědět, že existuje možnost právní obrany, nebo se může obávat vložení velkého úsilí a finančních prostředků do soudního řešení bez jistoty, že výsledek bude v jeho zájmu. Posledním, ale významným nedostatkem je aplikace až po útoku, jelikož některé mohou způsobit nevratné následky, např. znásilnění nebo sebevraždu (viz kap. 1.2.3).

Vzhledem k jmenovaným výhodám i nevýhodám předpisů pro řešení internetových útoků je patrné, že usilovat o vhodně nastavené právní akty má smysl, ale současně by měla být jejich omezení zohledněna zavedením dalších typů bezpečnostních opatření.

144 Podrobněji např. NOVOTNÝ 1997; SMEJKAL 2001; MATĚJKA 2002.

145 Působnost dle zákona č. 273/2008 Sb.

146 Působnost dle zákona č. 101/2000 Sb.

1.3.2 Technické zabezpečení

Technické zabezpečení je v kontextu této publikace zaměřeno na koncové stanice[147]. Právě na technickou stránku se dříve informační bezpečnost omezovala[148], s rozšiřováním sociálních hrozeb (např. kyberšikana) jsou technická řešení vnímána jen jako část bezpečnostních opatření. Jejich výhodou je často automatizovaná prevence či řešení útoků, které pro běžného uživatele mohou být transparentní. Technická bezpečnostní opatření je možné rozdělit do čtyř základních kategorií: specializované bezpečnostní aplikace, operační systém, internetový prohlížeč a ostatní aplikace.

U operačního systému záleží na jeho charakteristikách, vývoji a bezpečnostní politice. V tradičním prostředí (stolní počítače a notebooky) silně převažují systémy Windows, nejčastěji ve verzi 7 (postupně nahrazována verzí 10)[149], v mobilním prostředí Android (68,63 %) a iOS (29,52 %)[150]. Tato tři prostředí se liší již svojí podstatou a vyžadují odlišná řešení. Přesto je možné vymezit alespoň základní bezpečnostní pravidla, která jsou společná.

V první řadě je nezbytností pro každý software od operačního systému po bezpečnostní aplikaci pravidelná, ideálně automatická aktualizace co nejdříve po jejím vydání. Tímto postupem jsou ošetřeny zjištěné slabiny v informačních systémech. Aktualizace brání zneužití přes známou a popsanou zranitelnost, na kterou existuje řešení.

Dalším krokem je vhodné využití autorizace (stanovení oprávnění). V prostředí Windows se jedná především o uživatelské účty. Jeden účet by měl odpovídat jednomu uživateli s tím, že nastavená oprávnění by měla reflektovat jeho znalosti a potřeby (sdílení přístupových údajů je bezpečnostním rizikem a omezuje řešení při bezpečnostním incidentu). Uživatelské účty jsou použitelné i v prostředí Android od verze 4.2 Jelly Bean[151]. Na jiné úrovni autorizace odpovídá udělení oprávnění aplikaci. Ta jsou přidělována při instalaci v OS Android, v iOS si o ně může aplikace požádat, když je aktuálně potřebuje k výkonu požadované činnosti, např. polohové služby pro zjištění místa na mapě. Autorizace je základním opatřením při ochraně digitálních stop, pokud chce uživatel využívat ukládání dat, a to nejen na úrovni operačního systému, ale i v mnoha dalších softwarech a službách, např. pro nastavení soukromí.

S autorizací úzce souvisí autentizace (prokázání identity), která je podstatná nejen u operačních systémů. Varianty autentizace lze kategorizovat podle toho, čím

147 Využíváno v širším slova smyslu, tj. stolní, přenosný (vč. tabletů) i kapesní (hl. smartphony).

148 Viz např. POTÁČEK 2003–.

149 Operating System Share by Version 2018.

150 Operating System Market Share 2018.

151 Jelly Bean 4.2 [2012].

je totožnost prokazována:[152] znalostí (hesla), vlastnictvím (např. mobilní telefon u SMS s autentizačním kódem) a bytím (tj. biometrické ověření, např. otisk prstu při odemykání telefonu). V případě operačního systému je autentizace využívána pro umožnění práce s počítačem po zapnutí nebo obnovení z režimu spánku, hibernace apod. S ohledem na možnost fyzických útoků je vhodné při každém opuštění počítače vyžadovat heslo a také mít nastavený optimální co nejkratší interval přechodu do režimu spánku při zapomenutí manuálního nastavení.

Autentizace se nejčastěji provádí pomocí hesla. Pro silná textová (tradiční) hesla jsou poměrně známá pravidla, doporučená je kombinace různých typů použitých znaků, dostatečná délka (8–12 znaků) i práce s ním, např. pravidelná změna po určitém období[153]. Mnohá pravidla jsou ale přenositelná i na jiné typy hesel. Především v mobilním prostředí se prosazují grafická hesla, která spočívají v zapamatování si vedení čáry do obrazce, výběru obrázků apod. I při jejich použití by si měl uživatel dát pozor především na tzv. piggybacking[154], tedy jejich neoprávněné zjištění pozorováním při zadávání. Základem funkčnosti autentizace je důsledné odhlašování od všech služeb. Hesla jsou ale využívána i na jiných úrovních, například v bezdrátových sítích je zásadní udržení bezpečnosti hesel, protože cizí připojený počítač v síti může mít přístup k přenášeným datům[155].

Dalším klíčovým softwarem je internetový prohlížeč. Z hlediska bezpečnosti běžného uživatele je vhodné opět zvážit vhodnou kombinaci nastavení pro konkrétního uživatele. V prohlížeči je možné nastavit blokování vyskakovacích oken, blokování instalace doplňků, blokování nebezpečného, klamavého nebo nevhodného obsahu (např. zobrazujícího násilí), pamatování přihlašovacích údajů nebo ochranu soukromí. Možné je smazání různých digitálních stop, např. historie prohlížení, uložená uživatelská jména a hesla apod. Další nabídka záleží na konkrétním produktu.

Jedna z obvyklých možností je nastavení Cookies. Ty primárně ukládají informace o relaci, pokud v ní ale byly zadány osobní informace, mohou se i tyto v Cookies uložit a být přes ni dostupné[156]. Jejich zakázání v podstatě znemožňuje práci s internetovými službami (mnoho jich funguje na personalizované úrovni, která při zákazu Cookies není realizovatelná). V minulosti vznikaly různé iniciativy, především v angloamerickém prostředí (USA, konkrétně Federal Trade Commision[157], a Velká Británie), jejichž cílem bylo zlepšit vztah se zákazníky tím, že

152 NIXON 2010, s. 154.

153 Podrobné vymezení pravidel pro silná hesla a jejich užívání, vč. tipů pro praktické vyvážení použitelnosti a bezpečnosti uvádí BOTT 2004, s. 111-123.

154 POŽÁR 2005, s. 119.

155 SALTZMAN 2008, s. E.14.

156 BOTT 2004, s. 42.

157 Federal Trade Commission Decision and Order 2011.

mu umožnily oznámit, že nechce být sledován. Respektování tohoto přání se ale v praxi příliš nepodařilo prosadit.[158] Opačný princip preferuje Evropská unie, kdy naopak uživatel musí vyjádřit souhlas (ne nesouhlas) s uložením Cookies[159], která ale navzdory stanoveným lhůtám ještě nebyla přenesena plnohodnotně do českého prostředí.

V případě využití cizího počítače (např. počítač v knihovně), je možné využít anonymní mód prohlížeče, jehož výhodou je, že po ukončení relace nejsou uloženy v prohlížeči žádné informace o předchozí aktivitě uživatele. To je ale omezeno jen na prohlížeč, např. stažené soubory v počítači zůstávají. Současně se jedná o opatření jen na straně používaného zařízení, při použití anonymního módu nedojde k omezení informací, které o uživateli prohlížeč posílá do prostředí internetu (např. zobrazovaným webovým stránkám). Pokud by uživatel chtěl omezit i tyto informace, musel by použít specializované nástroje, jako jsou anonymizéry, proxy servery nebo služby využívající Onion Routing[160], které jsou ale již nad rámec zaměření této publikace. Všechny výše jmenované nástroje se zaměřují jen na pasivní digitální stopy, je nutné doplnit je vhodným nakládáním s informacemi, které uživatel na internetu vědomě zveřejňuje.

Existují také specializované bezpečnostní aplikace využitelné běžnými uživateli, především různé typy antimalware (antivir, antispyware, antirootkit), firewall, antispam, filtr obsahu, antiphishingový nástroj nebo anonymizér. Antiviry by měly být schopny detekovat a odstranit různé typy škodlivého softwaru. Firewall oddělující chráněnou a nechráněnou část sítě může pomoci při zjištění odesílaných informací, nebo naopak při jejich přijímání, pokud jsou vyhodnoceny jako nevhodné. Pomáhá také zjištění skenování portů a řešení otevřenosti nevhodných. Antispam slouží k automatickému vyhodnocování přijímaných e-mailů jako nežádoucích (dle nastavených pravidel), podobně jako filtry internetového obsahu. Poměrně málo rozšířené jsou antiphishingové nástroje, jejichž cílem je varovat před podvrženou webovou stránkou. Lze se s nimi setkat např. při vyhledávání na Google, kdy vyhledávač varuje při pokusu otevřít webovou stránku, která je dle něj podvodná.

Podobně jako je apelováno na bezpečnou skartaci dokumentů[161], je nutné uvažovat i nad elektronickým košem. Umístění souborů do něj totiž neznamená smazání, což nemusí být méně počítačově gramotnému uživateli zřejmé. I po příkazu *odstranit z* koše je možné za určitých okolností obnovit data pomocí specializovaného softwaru[162], v případě klíčových informací je proto vhodné (i několikanásobné)

158 Overview [b.r.].

159 Směrnice Evropského parlamentu a Rady 2009/136/ES.

160 HUSSAIN 2012.

161 MITNICK 2003, s. 164–166.

162 Např. File Scavenger, Disk Checker, Recuva, GetDataBack, Pandora Recovery a mnohé další.

přepsání[163] nebo zformátování nosiče, na kterém byly uloženy, např. flash disku nebo harddisku prodávaného počítače.

Při správě počítače je možné využít nástroje, které usnadní odstranění digitálních stop bez jednotlivých manuálních příkazů. Obvykle se jedná o odstranění dočasných souborů, historie prohlížení a stahování, vyplněných formulářů, hesel a Cookies. K tomu lze využít produkty jako Ccleaner, Advanced Cleaner, Eusing Cleaner nebo BleachBit. Vzhledem k tomu, kolik problematických digitálních stop vzniká na sociálních sítích[164], je přínosný nástroj specializovaný právě na jejich odstranění. Příkladem je Web 2.0 Suicidal Machine, který ale tuto funkci plní jen pro Facebook, MySpace, Twitter a LinkedIn[165]. Pro splnění své funkce nezbytně vyžaduje zadání přístupových údajů do služeb pro úpravu v nich uložených digitálních stop, proto je vhodné před využitím ověřit, že heslo nebude diskreditováno s ohledem na využití v jiných prostředích.

Jak bylo řečeno, jmenované technické možnosti obvykle neřeší nevhodné chování uživatele a aktivní tvorbu digitálních stop. Přesto je možné využít několik technických pomůcek pro jejich nalezení a odstranění. Pokud digitální stopa vznikne, pro automatizaci a zjednodušení základního vyhledávání informací o vlastní osobě (viz kap. 1.3.3) lze použít tzv. alertů, které v pravidelných intervalech zadávají dotaz a nové výsledky zpřístupní uživateli, např. automaticky zasílaným e-mailem. Takto lze využít Me on the web, který je součástí Google Dashboard, nebo alternativy pro Yahoo! a Bing. Tyto nástroje lze samozřejmě zneužít při získávání digitálních stop jinou osobou, podobně je pro egosurfing možné využít postupy popsané u získávání digitálních stop (viz subkapitoly 1.2). Jinou kategorii zjištění existující digitální stopy zastupuje možnost stažení přehledu zpracovávaných dat z Facebooku (od roku 2010). Zásluhu o vznik této možnosti má iniciativa Europe vs. Facebook, jejíž zakladatel s využitím Směrnice Evropského parlamentu a Rady 95/46/ES prosadil, že mu navzdory neochotě byl Facebook nucen sdělit, jaké informace o něm shromažďuje[166]. Přesto existují dohady, že rozsáhlý seznam informací[167] neobsahuje všechny, které Facebook zpracovává[168].

Tento přehled různých směrů, ve kterých je možné aplikovat technická řešení pro zvýšení bezpečnosti uživatele, ukazuje, že možností je mnoho. Problémem u všech zůstává, že je možné je obejít, a pokud ne v daném okamžiku, tak při zvýšení výkonu počítače (např. problém délky hesla) nebo zjištění nečekaného

163 Např. pomocí softwarů FileShredder, Secure Eraser, Active@ KillDisk, FCleaner, O&O SafeErase a další.

164 MOORE 2012.

165 Web 2.0 suicide machine [b.r.].

166 SOLON 2012.

167 Viz Přístup k osobním údajům na Facebooku c2014.

168 Get your Data! [b.r.].

problému (např. tzv. *Zero day attack*). Obejít je se ale může pokusit také uživatel, kterého mají chránit, např. dostupné jsou návody na překonání blokování Facebooku ve škole[169]. I technická prevence, podobně jako právní, je tedy nutně spojena s osvětou, aby mohla být efektivní. Podle Herrington[170] je také osvěta přínosnější než přísná restrikce pomocí bezpečnostních nástrojů, které omezují svobodný přístup k informacím, včetně těch hodnotných.

1.3.3 Prevence chováním

Předchozí dvě kapitoly ukazují, že oba popsané typy bezpečnostních opatření mohou přinést výraznou pomoc v oblasti digitálních stop, ale současně mají svá omezení. Vzhledem k trendům vývoje internetu význam chování uživatele roste. Ukázkou je např. princip Webu 2.0, který staví na příspěvcích běžných uživatelů, tj. vytváření aktivních digitálních stop. Jiným souvisejícím trendem je rozšiřování personalizace služeb (viz kap. 1.2.2). Proto je vhodné uvažovat nad bezpečností na úrovni uživatele.

Odpovědné chování je klíčovým aspektem informační bezpečnosti, zejména při zaměření na informační soukromí a digitální stopy. Pokud si uživatel chce ponechat právo rozhodovat o svém informačním soukromí, měl by tomu přizpůsobit své chování při práci s IT. V případě zaměření na bezpečné informační chování jsou opatření méně závislá na konkrétním zařízení (např. využití počítače u kamaráda nebo v knihovně). Bezpečnost závisí především na znalostech, dovednostech, postojích a zkušenostech konkrétního uživatele. Technická řešení často slouží jako bariéra, kterou musí uživatel potvrdit svým jednáním, např. webový prohlížeč může zobrazit varování pro uživatele, že SSL/TLS certifikát je nedůvěryhodný, je ale na rozhodnutí uživatele, jak na toto varování bude reagovat. To vše podporuje význam bezpečného chování v elektronickém prostředí.

Základním krokem při odpovědném chování při práci s informacemi je důsledné zvažování důvěryhodnosti. To by mělo probíhat na úrovni zprostředkovatelů informací, jejich zdrojů i informací samotných. Jednotlivé postupy popsané v kap. 1.1.2 lze uplatnit pro hodnocení různých forem informací (text, video apod.). Například při hodnocení komunikace na sociální síti, která je zprostředkovatelem informací, lze zvažovat, jaké umožňuje nastavení soukromí a zabezpečení (např. jaké zabezpečení služba využívá pro ochranu proti narušení informačního systému). Uživatel služby, se kterým komunikujeme, je informační zdroj, u kterého zvažujeme, nakolik je známý a důvěryhodný. Následně je zhodnocena samotná

169 XNOTION 2010.

170 HERRINGTON 2010, s. 10.

informace, kterou sdílí. Při tom je možné využít podobné postupy, jako při hodnocení kvality argumentů.

Vzhledem k náročnosti postupu je evidentní, že mnohem více subjektů dokáže využít informaci o člověku zveřejněnou na sociální síti než například verzi jeho webového prohlížeče (viz kap. 1.2.3). Právě úroveň využití, resp. zneužití, by měla odpovídat tomu, jak je uživatel opatrný při sdílení konkrétní informace v elektronickém prostředí (nejen zveřejněním). Obecně lze konstatovat, že bezpečné chování stojí na zvažování možných pozitivních a negativních důsledků chování s tím, že výsledné jednání odpovídá převažující hodnotě. Pokud by totiž vytvoření stejné digitální stopy mělo mít za následek jen nevýznamný přínos pro uživatele, měl by od něj upustit. Naopak pokud je pro něj klíčový, měl by vědomě rozhodnout, že je ochotný přistoupit na riziko pro něj nepříjemného využití digitální stopy. Toto rozhodování staví na podobných principech jako risk management[171]. Často se uplatňují podobná bezpečnostní doporučení jako ve fyzickém prostředí, např. děti by se neměly bavit s cizími lidmi nebo si od nich brát sladkosti (lákavé výhody, např. ve stahovaném souboru nebo službě po registraci či jiném úkonu), protože v tom může být skrytý negativní zájem útočníka.

Pro konkrétnější vymezení vhodného chování je nutné uvažovat jak úroveň prevence vzniku digitální stopy, tak nakládání s již existující. První ze jmenovaných přístupů je podstatný proto, že již digitální stopa se může dostat mimo řízení uživatelem, o kterém vypovídá, například může být uložena na různých místech, o kterých neví[172]. Může se také objevovat opakovaně i po dlouhé době. I firmy specializované na odstranění digitálních stop garantují jen omezené vyřešení (např. firma ReputationDefender stanovuje tuto hodnotu na 80–90 %[173]). Na druhou stranu i při nejlepším chování může nastat problém tím, že informaci o subjektu údajů vytvoří někdo jiný. Je ale možné omezit potenciál využití digitální stopy tím, že je řešena alespoň ta, která je dobře dostupná a subjekt údajů o ní ví.

Prvním krokem by mělo být omezování sdělování kontaktních údajů. Ty patří mezi nejsnáze využitelné informace, mohou sloužit také pro propojování informací z různých zdrojů (viz kap. 1.2), protože bývají jedinečné. Takovou informací je např. e-mailová adresa, ale i fyzická adresa, nejen bydliště, ale také školy či zaměstnání. Vzhledem k rozšíření sociálních sítí, kdy pro identifikaci stačí jméno, příp. přezdívka, je i tento údaj samotný možné považovat za kontaktní. Přezdívka je také problematickou informací, protože si ji často člověk přenáší do různých služeb, proto opět dobře slouží k propojování různých informačních zdrojů. Vzhledem k možnosti kompromitace služby (nejen nechtěné využití po oprávněném

171 POŽÁR 2005, s. 42–43.

172 GRAYSON 2011, s. 8.

173 MARTÍNEZ-CABRERA 2010.

přístupu) je vhodné sdělovat co nejméně osobních informací, a to i v registračních formulářích.

Zvažovány by měly být samotné informace, ale také důvěryhodnost prostředí či subjektu, kterému jsou zpřístupňovány. Zejména v oblasti e-komerce je zásadní hodnocení důvěryhodnosti obchodního partnera, který může být podvržený, kdy usiluje o získání financí nebo informací od oběti. Nedůvěryhodný obchodní partner může poskytnout osobní informace třetí straně či s nimi sám nezachází eticky. Na úrovni e-shopů lze pro hodnocení důvěryhodnosti využít různých typů certifikátů, v českém prostředí především APEK[174]. V případě obchodní transakce typu Consumer-to-Consumer, např. v elektronické aukci, lze využít nastavených reputačních mechanismů prodejců a nakupujících[175].

Dalším typem bezpečného chování je budování pozitivní digitální stopy[176]. Není reálné nemít digitální stopu, spíše je otázkou, co vypovídá o člověku. Proto je dobré přemýšlet nad obsahem informace, než se z ní stane digitální stopa, ale také nad možným vlivem na člověka při jejím využití různými subjekty. Např. fotografie z oslavy může mít vliv ze strany přátel (pozitivní ukázka společenského charakteru a zábavy), tak i ze strany zaměstnavatele (pokud úroveň zábavy převyšuje úroveň, kterou považuje za vhodnou) nebo útočníka (možnost vydírání obsahem fotky nebo při fotomontáži).

Pro ochranu proti útokům, které začleňují sociální inženýrství (viz kap. 1.2.1), je vhodné ověřování oprávněnosti jakéhokoli požadavku na poskytnutí informace nebo vykonání činnosti (např. instalace softwaru), nejlépe ne elektronicky, aby nedošlo k využití podvrženého informačního zdroje. S tím také souvisí to, že by neměly být využívány odkazy ve zprávách, ale ověření přes oficiální kanály. Dále je vhodné navrhovat alternativní řešení, všímat si podrobností a usilovat o vedení rozhovoru tak, aby mohly být identifikovány nepřesnosti při komunikaci v oblasti, na kterou se sociotechnik nemohl dopředu připravit[177]. Protože sociální inženýrství často využívá nátlak přes emoce, je vhodné si toto uvědomovat a zpozornět v situacích, kdy by právě emoce mohly vést k rizikovému jednání.

Chování je vázáno také na vhodnou práci s bezpečnostními technickými opatřeními. Jejich funkce je informační, varovná, může se ale stát, že se jedná o falešně pozitivní oznámení, proto je rozhodnutí ponecháno uživateli. Navzdory nepohodlnosti je pro zvýšení bezpečnosti vhodné číst certifikáty, licenční podmínky, varování, potvrzení apod. Nicméně především licenční podmínky vzhledem k jejich délce slouží spíše pro právní ochranu poskytovatele služby než pro ochranu uživatele.

174 Certifikáty a ocenění e-shopů c2014.

175 Např. Aukro nápověda [b.r.].

176 GRAYSON 2011.

177 MITNICK 2003.

Je nutné poznamenat, že chování při nastavení softwaru a internetových služeb závisí i na úrovni porozumění, což je podle O'Neilla[178] důvod problému, že třetina uživatelů sociálních sítí neví, jak zde změnit nastavení soukromí. Na úrovni dospělých uživatelů se ukazuje, že od roku 2009 se zvyšuje aktivní úprava dostupnosti sledovaných digitálních stop (nejméně omezený přístup je u osob ve věku 18–29 let a nad 65 let, současně ale polovina z nich měla problémy při řízení nastavení soukromí)[179]. Po nastavení soukromí je nutné věnovat se udělování autorizace, typicky přidávání kontaktů (např. přátel na sociální síti Facebook).

Pro řešení rizikové situace v podobě nežádoucí digitální stopy je nutné nejdříve se o ní dozvědět, protože, jak již bylo opakovaně uvedeno, ne všechny digitální stopy o sobě člověk vytváří sám. Při zjišťování existence digitálních stop je nejsnazším postupem jejich vyhledání. Tento postup je označován jako egosurfing[180] a především v USA se jedná o často zmiňované bezpečnostní opatření[181]. Egosurfing by měl být prováděn pravidelně, a to ve vyhledávačích i v sociálních médiích. V případě zde existující nežádoucí stopy vytvořené někým jiným je na sociální síti jednodušší řešení, protože je možné požádat známého o odstranění daných informací. Pokud digitální stopu vytvořila třetí strana, ke které subjekt údajů nemá užší vztah, např. organizátor soutěže, které se zúčastnil, nebo firma, od které si něco koupil, je možné i ji požádat o smazání. Pokud není možné kontaktovat přímo osobu zodpovědnou za zveřejnění, např. v příspěvku v diskuzním fóru, lze využít oprávnění správce služby odstranit tuto informaci. V obou případech by mělo být požadavku vyhověno podle evropské a české legislativy (viz kap. 1.3.1). Z rozsudku Soudního dvora (velkého senátu) Evropské unie[182], vyplývá, že o smazání je možné požádat také internetový vyhledávač, který dané informace neobsahuje přímo, ale zobrazuje ve vyhledávání a umožňuje k nim přístup. Pak ale není smazána samotná digitální stopa, ale jen její záznam ve vyhledávači – stránka tedy není tímto nástrojem vyhledaná, ale informace je dál na této stránce dostupná. V případě, že digitální stopa vznikla působením subjektu, který má tuto činnost danou ze zákona, je nutné se s digitální stopou smířit a být si nadále vědom, že daná informace je veřejně dostupná (např. nevyužívat ji jako heslo).

Informační bezpečnost je vhodné podpořit všemi možnostmi, které se nabízejí. Měla by být propojena technická a právní opatření s vhodným informačním chováním. Každé bezpečnostní opatření je možné překonat, ale čím více bude bariér

178 O'NEILL 2012.

179 MADDEN 2012.

180 Egosurf © 2014.

181 Egosurfing někdy využito 47 % dospělých Američanů, z nich 25 % opakovaně. Viz MADDEN 2007, s. 7.

182 Rozsudek Soudního dvora (velkého senátu) ze 13. května 2014, spis. zn. C-131/12.

při útoku, tím je vyšší je pravděpodobnost, že některá útok zastaví nebo alespoň omezí.

Zásadním prvkem spojeným s každým z těchto přístupů k zvýšení bezpečnosti je vzdělání. Osvěta v informační bezpečnosti by měla zahrnovat nejen možná bezpečnostní opatření, ale i důvody jejich využití. Vedle řízeného vzdělávání by uživatelé měli znát kontaktní místa, která jim mohou pomoci s řešením konkrétních problémů. Jedním z těchto míst může být knihovna, jak ukazuje následující kapitola. Knihovník ale nemusí být nutně ten, kdo zná všechny odpovědi. Stačí, když bude důvěryhodným subjektem, který je schopný dohledat potřebné informace k tématu, příp. kontaktovat instituci, která se na dané téma specializuje. Vždy je nezbytné, aby knihovník byl pozorný posluchač a umožnil sdělení všech aspektů útoku, které mohou hrát roli při pochopení i řešení situace. Pokud je událost nepříjemná, není vhodné podporovat pocit sekundární viktimizace[183] projevy negativních emocí (např. *To je strašné!*), ale spíše usilovat o přesvědčení, že problém je řešitelný a měl by se řešit, ne přetrpět. K tomu jsou nutné důkazy a jednání s oprávněnými osobami, což jsou v případě dětí vždy rodiče. To může být pro dítě náročné, častá je obava ze zákazu dalšího použití internetu[184]. V případě překročení zákona při útoku může pomoci Policie. Pro podporu z psychologického hlediska i hledání řešení, ať už pro dítě nebo knihovníka či rodiče, mohou pomoci horké linky, kde působí pracovníci školení pro tyto případy.

183 Druhotné poškození řešením incidentu – VÁGNEROVÁ 1999, s. 393.

184 JUVONEN 2008.