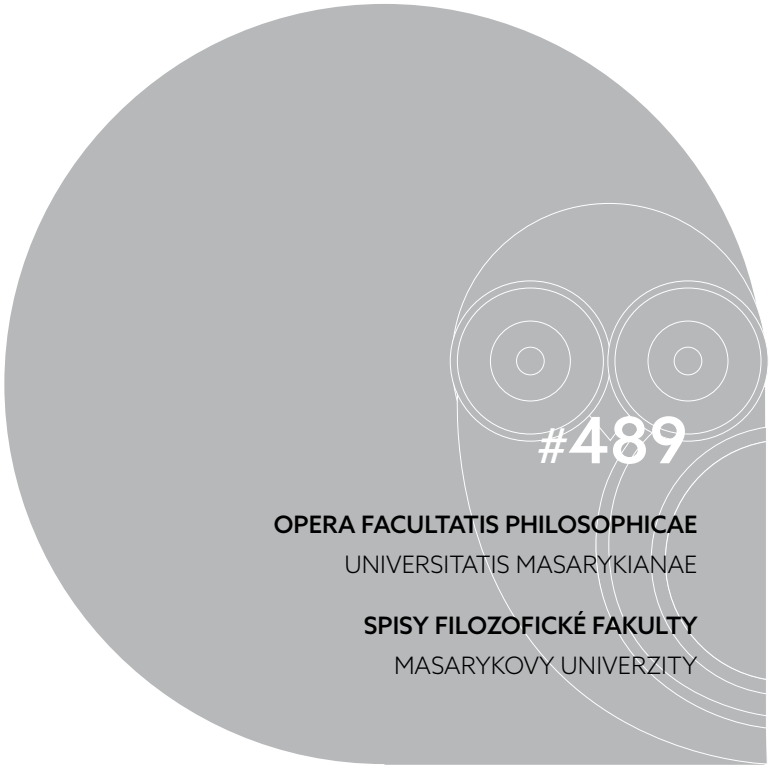
Informační bezpečnost žáků základních škol

Lekce v knihovnách

Pavla Kovářová

FILOZOFICKÁ FAKULTA
MASARYKOVA UNIVERZITA
#489



OPERA FACULTATIS PHILOSOPHICAE
UNIVERSITATIS MASARYKIANAE

SPISY FILOZOFICKÉ FAKULTY
MASARYKOVY UNIVERZITY

MUNI
PRESS

Informační bezpečnost žáků základních škol

Lekce v knihovnách

Pavla Kovářová

FILOZOFICKÁ FAKULTA
MASARYKOVA UNIVERZITA

#489

BRNO 2019

Recenzovali: PhDr. Hana Landová, Ph.D. (Univerzita Karlova)
prof. PhDr. Helena Grecmanová, Ph.D. (Univerzita Palackého v Olomouci)
doc. Mgr. Jiří Zounek, Ph.D. (Masarykova univerzita)

ISBN 978-80-210-9270-9
ISBN 978-80-210-9271-6 (online : pdf)
ISSN 1211-3034
https://doi.org/10.5817/CZ.MUNI.M210-9271-2019

Obsah

PŘEDMLUVA

O současné společnosti se stále více hovoří jako o společnosti informační. Informace a informační technologie proměňují řadu dříve obvyklých a přijímaných přístupů a pravidel v oblasti formy a obsahu vzdělávání, ale také v zajištění informační bezpečnosti. Mění se také role knihoven, jejichž základním posláním je zpřístupňování informací uživatelům, kdy tyto informace jsou stále častěji zprostředkovány právě informačními technologiemi. Téma informační bezpečnosti se silně dotýká všech uživatelů internetu a informačních technologií, mezi nimi jsou však vyzdvihovány možné dopady a rizika pro děti. Ty prochází povinným vzděláváním, které je má připravit na profesní i soukromý život. Cílem této publikace je nabídnout daty podloženou analýzu a současně návrh pro vzdělávání žáků základních škol v informační bezpečnosti. Primárně monografie směřuje do knihoven, ale její výsledky lze jistě uplatnit i v dalších institucích, jak institucích neformálního vzdělávání, tak ve školách.

Pro dosažení tohoto cíle je monografie rozdělena do tří základních částí. První část přináší teoretické představení problematiky informační bezpečnosti. Zaměřuje se na rizika, hrozby a možná bezpečností opatření, která by měl lektor znát nejen pro realizaci dále řešených lekcí. První část tedy může být přínosná nejen pro lektory, ale i odbornou a širokou veřejnost pro získání přehledu o problematice informační bezpečnosti, bezpečnostních opatřeních, která by měl využívat běžný uživatel informačních technologií, i o důvodech jejich využití.

Druhá část publikace se již soustředí na samotnou koncepci vzdělávání žáků základních škol v informační bezpečnosti v knihovnách. Jsou představena východiska, která může knihovna využít pro argumentaci vůči zřizovateli a uživatelům ke zdůvodnění aplikace dané koncepce. Následně jsou popsány jednotlivé lekce do té míry podrobnosti, aby je knihovník mohl využít přímo, případně po přízpů-

sobení specifikům cílové skupiny. Akcentováno je proto nejen to, co bylo nastaveno, ale také proč a co je nutné zachovat pro dosažení stanovených cílů lekce. Tato část publikace je tedy již určena zejména lektorům v knihovnách, případně jiných vzdělávacích institucích, ale také managementu těchto organizací pro zdůvodnění realizace této služby (v anglickém prostředí označováno jako *information literacy advocacy*[1]).

Forma i důvody nastavení lekcí nevycházejí jen z odborné literatury, ale výrazně je ovlivnily také výsledky výzkumů, které byly využity jak pro orientaci v prostředí knihoven a jejich potenciálu lekce realizovat, tak pro ověření koncepce pomocí akčního výzkumu. Přestože v knihovnictví i dalších oblastech se diskutuje potřeba služeb založených na datech (*evidence-based librarianship*), knihovny poskytují své služby převážně na základě vlastního přesvědčení[2]. Tato část publikace tedy slouží jako empirický doklad reálnosti a efektivity navržené koncepce. Sekundárně může být využitelná pro knihovníky jako inspirace pro provádění vlastních výzkumů i jako ukázka jejich přínosu. V tomto ohledu jsou opět primární cílovou skupinou publikace lektoři informačního vzdělávání v knihovnách, ale sekundárně i ostatní zaměstnanci knihoven nebo lektoři neformálního vzdělávání.

Tato publikace navazuje na dizertační práci autorky[3]. S ohledem na výše představený cíl je ale větší část práce přepracována. Některé pasáže jsou rozpracovány podrobněji pro využitelnost v praxi, jiné jsou naopak zkráceny s ohledem na aktuálnost nebo volnější vztah k jádru knihy.

1 KATZ 2007.

2 KOVÁŘOVÁ 2016.

3 KOVÁŘOVÁ 2015.

ÚVOD

Téma informační bezpečnosti je diskutováno veřejností jako jeden ze základních problémů při využívání internetu[4]. Efektivní a bezpečná práce uživatelů s informacemi je řazena do kompetencí nezbytných pro digitální občanství[5]. Roste proto společenská poptávka po vzdělávání v této problematice. Oblast soukromí, která je silně propojena s digitálními stopami, byla zařazena do oblasti zájmu knihoven spolu s dalšími tématy informační bezpečnosti již v roce 2005, jak dokládá obsah dokumentu IFLA s titulem *Libraries, National Security, Freedom of Information News and Social Responsibilities*[6]. Problematika autorských práv a hodnocení informací představuje oblast, které se knihovny věnují dlouhodobě (např. již akvizicí jednotek do fondu). Knihovny tak právem patří mezi instituce, které naplňují předpoklady k zajištění vzdělávání uživatelů v informační bezpečnosti.

Problematika informační bezpečnosti je ve zde řešeném pojetí omezena na možnosti zvýšení bezpečnosti uživatelů, zejména dětských, pomocí vzdělávání v knihovnách. Téma je již nyní pokryté knihovnami v rámci informačního vzdělávání (viz kap. 2.1.4), které představuje tradiční službu knihoven. Informační vzdělávání je sice úzce spjato s didaktikou, ale nezabývá se jen formou vzdělávání, nýbrž i obsahem (práce uživatele s informacemi). Naopak aplikace výzkumu do informačního vzdělávání je významná pro hodnocení jeho efektivity[7], a to jak na úrovni jednotlivých aktivit, tak i v oblasti přístupů a řešených témat. Ta se

4 TAMBAUM 2010.

5 GALLAGHER 2011.

6 SEIDELIN a HAMILTON 2005.

7 Význam tohoto spojení ukazuje současný rozvoj tzv. „evidence-based teaching" (někdy také learning, education apod., terminologie zatím není ustálená). Přínosy přístupu pro jednotlivé vzdělávací aktivity prezentuje např. KOVÁŘOVÁ 2014.

v současné společnosti s informačními technologiemi rychle mění a je nutné se těmto změnám přizpůsobovat, aby informační vzdělávání bylo přínosné pro vzdělávané[8].

Aby koncepce vzdělávání odpovídala současným podmínkám a potřebám, bylo nutné zohlednit chování dětí, současnou podobu vzdělávání v knihovnách a vzdělávání v informační bezpečnosti. Průnik všech tří oblastí je v současnosti v odborné literatuře a výzkumech pokryt nedostatečně. Tato publikace usiluje o představení těchto témat a aplikovaného výzkumu pro posílení řešení informační bezpečnosti dětí v českém prostředí. Lekce jsou po úpravách využitelné i pro další cílové skupiny, informační bezpečnost není omezena jen na děti. To již ale není předmětem této publikace, byť může sloužit jako inspirace pro lektora v přípravě lekcí informační bezpečnosti i pro další uživatele.

Hlavním cílem publikace je představení daty podložené koncepce pro vzdělávání v informační bezpečnosti, která by byla uplatnitelná v současných podmínkách knihoven. Děti jsou kvůli svým omezeným životním zkušenostem, pozitivnímu vztahu k technologiím a dalším charakteristikám spojeným s vývojovou psychologií[9] náchylnější k zranitelnosti na internetu. Zahájení vzdělávání je vhodnější v době, kdy se lépe budují postoje v chování, následně získávané znalosti se ve spojení s nimi lépe rozšiřují. Knihovny v současnosti nabízejí své lekce do škol, čímž mají zajištěnu návštěvnost, školy zase vzdělávání v oblasti, která pokrývá mimo jiné i informační gramotnost[10]. Je tak umožněno plošné oslovení plošné oslovení a následně vzdělání velké části cílové skupiny – žáků základních škol, které je výrazně reálnější než oslovování osob v produktivním věku pro lekce, se kterými knihovny stále mají problém[11].

8 Změnám v informační gramotnosti vlivem IT se věnuje např. KOVÁŘOVÁ 2013.

9 Viz kap. 1.2.1, podrobněji viz KOVÁŘOVÁ 2011.

10 Vymezení pojmů informační gramotnost a vzdělávání a jejich vztahu se věnuje kap. 2.1.1.

11 ŠTEFEK 2012.

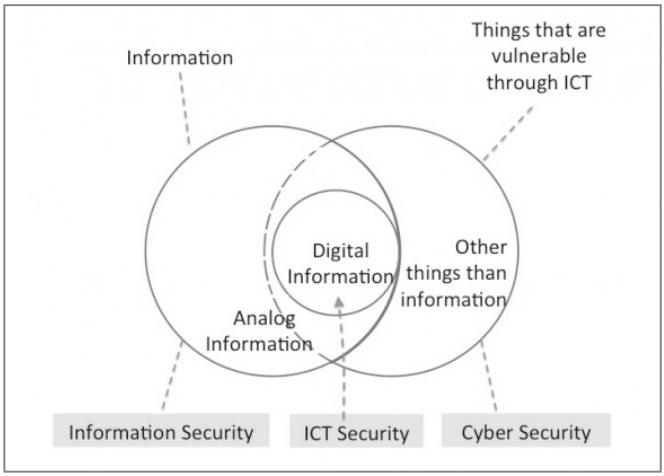
1 INFORMAČNÍ BEZPEČNOST A DIGITÁLNÍ STOPY

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:

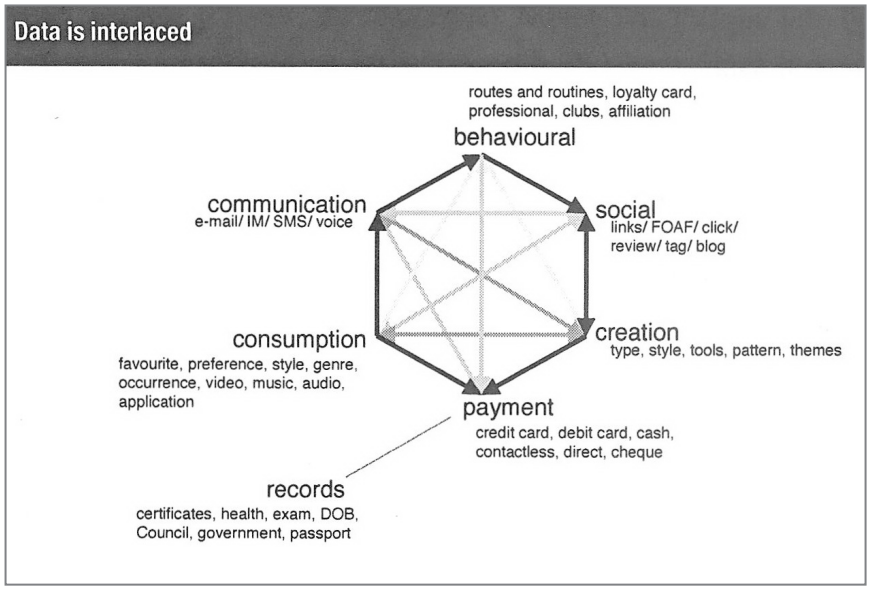
> *„Červená – rodné číslo, číslo pojištění, identifikační čísla (PIN) účtů, rodné jméno matky, informace o zdravotním stavu, trestní rejstřík, podrobné informace o financích, cestovní plány, seznam předchozích zaměstnání, informace o rodině a přátelích vč. jejich telefonních čísel, e-mailových i skutečných 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.

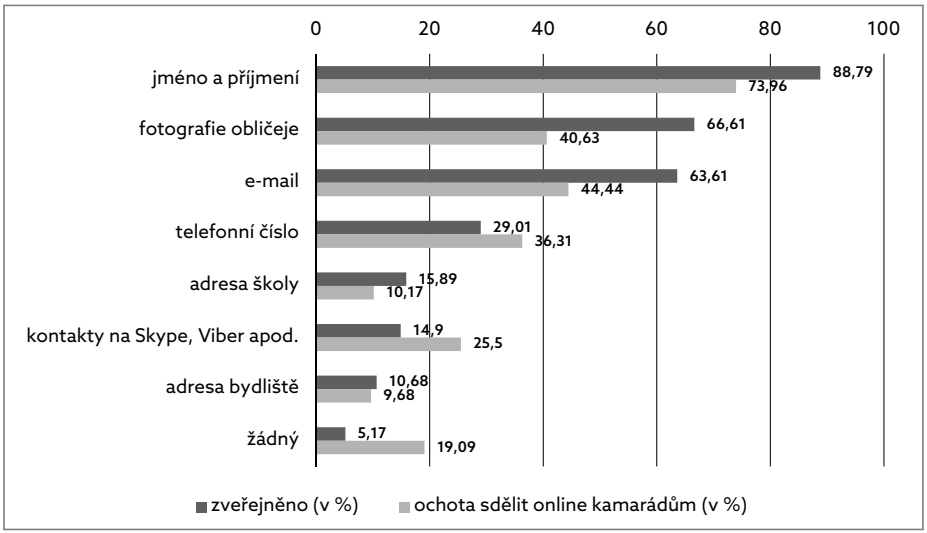
51 JOINER 2005.

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.