Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Informační věda

Dizertační práce

PhDr. Pavla Kovářová

Zneužití digitálních stop uživatelů ICT: vzdělávání v knihovnách jako prevence narušení soukromí

Misuse of ICT users digital footprint: library education as a prevention of privacy invasion

Praha 2015

Vedoucí práce: Ing. Martin Souček, Ph.D.

Poděkování:

Na tomto místě bych ráda poděkovala své rodině za podporu a trpělivost během mé tvorby této práce. Za odbornou i lidskou podporu také děkuji svému školiteli Martinu Součkovi a neformálnímu konzultantu Andymu Lassovi. Velké díky patří také všem, kteří mi dávali nové podněty pro obsah práce, především účastníkům výzkumů a kolegům.

Prohlášení:

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

V Praze, dne 27. ledna 2015

……..

Pavla Kovářová

Klíčová slova (česky)

děti, digitální stopy, informační bezpečnost, informační gramotnost, knihovny, metodika, vzdělávání

Klíčová slova (anglicky):

children, digital footprint, education, information literacy, information safety, libraries, methodology

Abstrakt (česky)

Digitální stopy, ve smyslu digitálních informací vypovídajících o konkrétním člověku, patří k základům informační společnosti. Člověku, kterého se týkají, mohou pomoci (např. doklad profesní kvality), ale také ublížit (např. dokumenty nevhodného chování, informace zneužité při informačním útoku). Správa digitálních stop se tak stává důležitou pro stále více lidí. Knihovny mohou lekcemi informační gramotnosti podpořit znalost postupů efektivní správy digitálních stop, která je předpokladem pro jejich aplikaci. Dizertační práce představuje problematiku na teoretické, ale především výzkumné úrovni. Pro správné nastavení lekcí jsou zmapovány aktivity českých knihoven ve vzdělávání. Dotazníky prokázaly, že téma práce navazuje na současné aktivity i zájem knihoven. Následně byly testovány znalosti knihovníků a studentů informačních studií a knihovnictví o digitálních stopách. Byly prokázány, nicméně jen na základní, omezené úrovni, jsou ale dostatečné pro čtyři lekce navržené v dizertační práci pro děti na základní škole. Jedna z lekcí je dále ověřena v akčním výzkumu, jehož součástí je také širší pohled zástupců klíčových skupin osob ve vztahu k lekcím. Akční výzkum prokázal efektivitu lekce i pozitivní postoj všech zkoumaných osob na lekce o digitálních stopách v knihovnách pro zvýšení bezpečnosti dětí, ale návazně i dalších skupin veřejnosti.

Abstract (in English):

Digital footprints, within the meaning of digital information informing about a particular person, belongs to the basic of the information society. They can help (e.g. as a proof of professional quality), but also hurt (e.g. documents of inappropriate behaviour, information misused in information attack) a man whom they relate. Managing digital footprints is becoming important for increasing amount of people. Libraries can promote knowledge of procedures for the effective management of digital footprints by information literacy lessons, which is a prerequisite for their application. PhD thesis describes the theoretical, but especially the research level. Activities of Czech libraries in education are mapped for the correct setting of lessons. Questionnaires showed that the topic continues with the current activities and interest in libraries. Knowledge of librarians and library and information studies students about digital footprints was subsequently tested. Knowledge has been proven, however only to a basic, limited level, but they are enough for four lessons designed for children in elementary school in the dissertation. One of the lessons is further verified in action research, which is a part of a broader view of stakeholders in relation to lessons. Action research has demonstrated the effectiveness of the lesson and positive attitude of all surveyed people for lessons on digital footprints in libraries to increase the safety of children, but subsequently the other groups of the public.

OBSAH

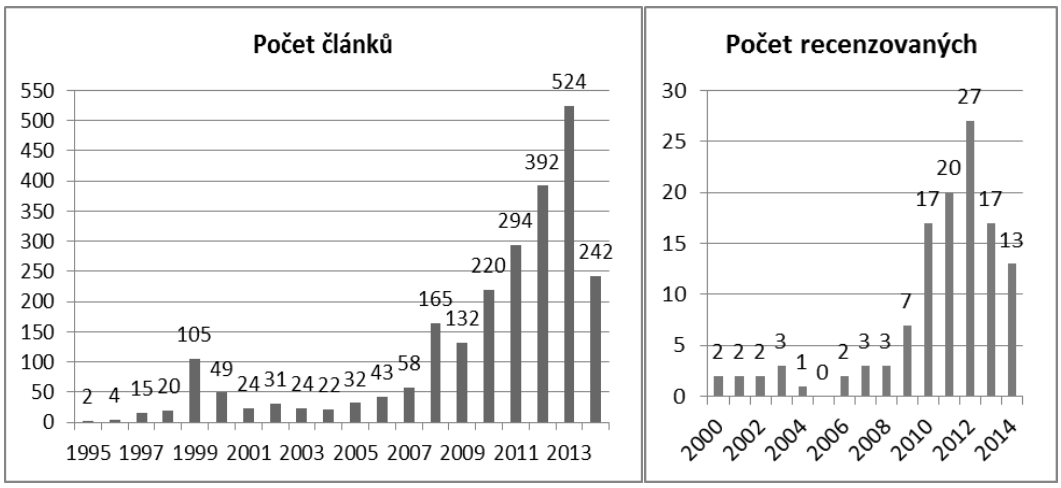
Seznam zkratek

AAP	American Academy of Pediatrics
ACRL	Association of College & Research Libraries
AKM	Archivy, knihovny, muzea (konference)
AKVŠ	Asociace knihoven vysokých škol
ANOVA	Analysis of variance
APEK	Asociace pro elektronickou komerci
A/S/L	Age, sex, location
CILIP	Chartered Institute of Library and Information Professionals
ČIS	Česká informační společnost, o. s.
DS	Digitální stopy
ES	Evropská společenství
EU	Evropská unie
E-U-R	Evokace – uvědomění – reflexe
FIT	Fluency with Information Technology
HR	Řízení lidských zdrojů
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Informační a komunikační technologie
IFLA	International Federation of Library Associations
INEBE	Informační nebezpečí (projekt)
IP	Internet Protocol
ISK	Informační studia a knihovnictví
ISTE	International Society for Technology in Education
IT	Informační technologie
IVIG	Odborná komise pro informační vzdělávání a informační gramotnost
IVU SDRUK	Informační vzdělávání uživatelů Sdružení knihoven
JAP	Java-Anonymize-Project
K12	Kindergarten - 12 grade
KJM	Knihovna Jiřího Mahena
MKP	Městská knihovna v Praze
MOOC	Massive Open Online Course
MS	Microsoft
MZK	Moravská zemská knihovna
NCBI	Národní centrum bezpečnějšího internetu
NETS	National Educational Technology Standards
NIPOS	Národní informační a poradenské středisko pro kulturu
NK	Národní knihovna
OMG	Oh my God
OS	operační systém
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PRVOK	Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci
SKIP	Svaz knihovníků a informačních pracovníků České republiky
SPSS	Statistical Package for the Social Sciences
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TOR	The Onion Router

1 Úvod práce

Téma digitálních stop je diskutováno veřejností jako jeden ze základních problémů při využívání internetu[1]. Vyskytuje se i v odborných publikacích, i když ne vždy pod tímto termínem. Vhodná práce uživatelů s digitálními stopami je řazena do kompetencí nezbytných pro digitální občanství[2]. Proto roste společenská poptávka po vzdělávání v dané problematice. Knihovny patří mezi instituce, které naplňují předpoklady k zajištění řešení tohoto problému, tedy vzdělávání uživatelů o digitálních stopách a informační bezpečnosti vůbec. Tématem této práce je tedy právě možnost zajištění vzdělávání o bezpečnosti digitálních stop knihovnami.

Pojem digitální stopy je používán často na úrovni subjektivního pocitu veřejnosti. Objevuje se ale také stále častěji i ve vědeckých článcích. Růst zájmu o toto téma ilustruje množství publikací v databázi ProQuest v grafu 1.



Graf 1 Počet publikací o digitálních stopách v databázi ProQuest[3]

Digitální stopy ve významu dostupných a zpracovatelných informací spojitelných s konkrétním uživatelem informačních technologií[4] lze vztáhnout k informační vědě různými způsoby. V tradičním přístupu[5] se jedná o data

[1] TAMBAUM 2010
[2] GALLAGHER 2011
[3] Vzhledem k digitalizaci stop v různých oborech, např. archeologii nebo geografii se jedná o výsledky ke dni 24. 7. 2014 (nižší hodnota v posledním roce je dána jen polovinou pro hodnocení) pro vyhledávací dotaz: "digital footprint*" AND internet
[4] Jedná se o zjednodušené vymezení, podrobněji je rozvedeno v kap. 2 Digitální stopy
[5] CEJPEK 2005, s. 14

cirkulující v technických zařízeních, která představují jeden ze základních významů informace v informační vědě. Ta prochází stálou formulací vlastního předmětu, především kvůli nejasnosti dané šíří pojmu informace, proto tento přístup lze považovat za překonaný. V jiných pojetích[6] se mj. objevuje v jádru informační vědy zkoumání informace ve smyslu komunikace. Protože současná komunikace, především ta zprostředkovaná informačními zdroji, je stále více spojena s informačními technologiemi, roste v této oblasti význam spojení informační vědy s počítačovou vědou (v angličtině preferované označení Computer Science, do češtiny obvykle překládané jako informatika), která není součástí informační vědy, ale část jejich předmětu se překrývá. Právě do tohoto překrytí spadá i problematika digitálních stop, které představují digitální informace vznikající právě při komunikaci, ať už mezi uživateli nebo i mezi technickými zařízeními. Oblast soukromí, která je reprezentována především 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*[7].

Problematika digitálních stop v pojetí této práce je omezena na možnosti zvýšení bezpečnosti subjektů s nimi spojených pomocí vzdělávání v knihovnách. Téma digitálních stop je možné zařadit mezi oblasti pokryté knihovnami v rámci informačního vzdělávání. To spadá do zájmu informační vědy jako vzdělávání pro efektivnější práci s informacemi a pro to určenými technologiemi, představuje tradiční službu knihoven, pro obor informační věda klíčového typu institucí. Informační vzdělávání je sice úzce spojeno s pedagogikou, ale nezabývá se jen formou vzdělávání, ale i obsahem (práce uživatele s informacemi), což jej začleňuje do oblasti informační vědy. Naopak přínos vědeckého přístupu do informačního vzdělávání je významný pro hodnocení jeho efektivity[8], a to jak na úrovni jednotlivých aktivit, tak i v oblasti přístupů a řešených témat. Ta se v současné společnosti s informačními technologiemi rychle mění a je nutné se těmto změnám přizpůsobovat, aby informační vzdělávání bylo přínosné pro vzdělávané[9].

[6] LORENZ 2012
[7] SEIDELIN a HAMILTON 2005
[8] 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
[9] Změnám v informační gramotnosti vlivem ICT se věnuje např. KOVÁŘOVÁ 2013

Vymezení oborových vztahů, které znázorňuje obr. 1, ukazuje, že téma této práce spadá do oblasti informační vědy, ale také zasahuje do dalších oborů. Informační věda díky své transdisciplinaritě umožňuje zohlednit nejen směry zájmů konkrétního oboru, ale především umožňuje jejich provázání v souvislostech. Pro posun tématu blíže k informační vědě je problematika řešena s důrazem na uživatelské a společenské aspekty a jejich vazbu na další pohledy, jako je technický, pedagogický, psychologický nebo právní, pro vymezení pojetí je klíčová také souvislost s prostředím knihoven.

Obr. 1 Digitální stopy uživatelů a související vědní obory

Hlavním cílem práce je vytvoření osvědčené metodiky pro vzdělávání v knihovnách o bezpečnosti digitálních stop, která by byla uplatnitelná v současných podmínkách. Vzhledem k šířce tématu a nutnému odlišnému oslovování různých cílových skupin došlo k zaměření na děti. Omezení lze považovat za logické vzhledem k zranitelnosti dětí 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 také v současnosti nabízejí své lekce do škol, čímž mají zajištěnu návštěvnost, školy zase vzdělávání

ve sjednaném tématu, kdy je pokryta jak oblast informační gramotnosti[10], tak i tématu odpovídajícího vzdělávacím cílům pro danou třídu. Tak je možné plošné oslovení a následně vzdělání velké části cílové skupiny stanovené pro tuto práci, které je výrazně reálnější než oslovování osob v produktivním věku pro lekce, se kterými knihovny stále mají problém[11].

Aby bylo možné určit, co je reálné, a podle toho metodiku postavit, bylo nutné popsat současné prostředí knihoven ve vzdělávání a bezpečnosti digitálních stop. Jedná se tedy o první a nezbytný dílčí cíl práce, bez kterého není možné navrhnout metodiku tak, aby odpovídala možnostem současných knihoven. Pro oblast vzdělávání v knihovnách bylo nejdříve nutné zjistit, zda se knihovny věnují alespoň širším tematickým oblastem, do kterých by bylo možné digitální stopy začlenit. V opačném případě by bylo nutné pro vzdělávání nejdříve připravit předpoklady v širších tematických oblastech, aby bylo možné dospět k digitálním stopám. Dále bylo nutné ověřit zájem knihovníků pokrýt toto téma, tedy využít navrhované metodiky ve vlastní praxi, s čímž souvisí uvědomění si významu tématu pro cílovou skupinu, a také znalosti lektorů v knihovnách o digitálních stopách. Aby bylo možné metodiku aplikovat, musí se knihovník orientovat v problematice. Úroveň znalostí v zásadě vymezuje hranici lekcí o digitálních stopách, protože pro specifičtější cílové skupiny, které využívají internet pro více či sofistikovanější činnosti, jsou nutné hlubší znalosti lektora. I to byl jeden z důvodů omezení tématu dizertační práce na děti, které ne nutné naučit základní znalosti, dovednosti a postoje v problematice digitálních stop, na které je později možné navázat jak na úrovni rozvoje jedince, tak i v oblasti koncepčního přístupu ke vzdělávání v knihovně.

Po stanovení možností knihoven v řešené problematice bylo možné přistoupit k hlavnímu cíli práce s respektováním předchozích zjištění. Výstupem je metodika vzdělávání v knihovnách o bezpečnosti digitálních stop složená ze čtyř lekcí pro 3. – 9. třídu. Testování metodiky bylo možné jedině její realizací spojenou s důvěryhodným hodnocením pomocí výzkumů. K tomu bylo využito akčního výzkumu pojetí lekcí prostřednictvím jedné vybrané lekce. Akční výzkum byl složený ze tří dílčích šetření, aby výsledky bylo možné potvrdit triangulací dat.

[10] Vymezení pojmů informační gramotnost a vzdělávání a jejich vztahu se věnuje kap. 4.2
[11] ŠTEFEK 2012

Postoj zainteresovaných osob s ohledem na lekci i obecné, širší vymezení, slouží k potvrzení reálnosti aplikace vzdělávání v knihovnách o bezpečnosti digitálních stop především díky ověřenému zájmu, přínosům a odstranitelnosti bariér. Tak je dosaženo stanoveného cíle práce s potvrzením reálnosti aplikace osvědčené metodiky nejen na úrovni nabídky knihovnami, ale také poptávkou u zástupců zainteresovaných osob.

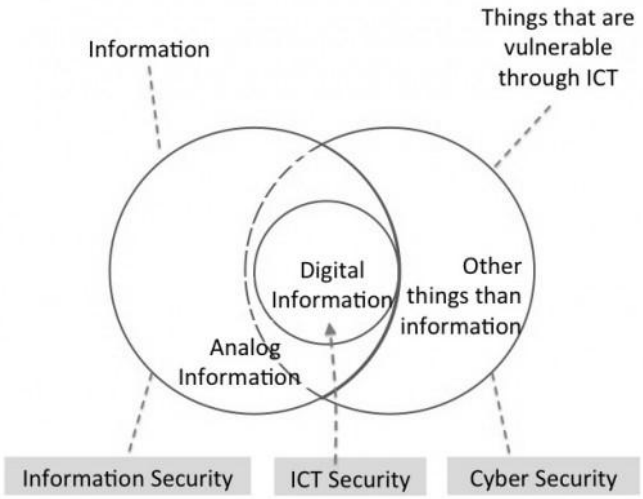
I. Teoretická východiska

2 Digitální stopy

Vzhledem k omezené úrovni dostupných informací i k aktuálnímu stavu řešené problematiky digitálních stop v knihovnách, je nutné rozšířit pozornost na širší oblast informační bezpečnosti. Daný kontext a širší termín je vhodné vymezit před samotným definováním tématu digitálních stop pro potřeby této práce.

Označení *informační bezpečnost*, podobně jako digitální stopy, se objevuje v laickém vyjadřování spíše s pocitovým vymezením. I v odborných publikacích nepanuje shoda na obsahu termínu, k čemuž v českém prostředí přispívá jazykové omezení pro přenos ze zahraničních prací. Z historického pohledu se pojem vázal na technické zabezpečení informačních systémů, čímž problematika jasně 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 systému[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 práci. 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 najít doklad, že problematika informačního zabezpečení má jasnější vztah k informační než počítačové vědě, jelikož není omezena na spojení s ICT, jak dokládá obr. 2.

[12] POŽÁR 2005, s. 54-55



Obr. 2 Informační bezpečnost ve vztahu k ICT[13]

Informační bezpečnost (pro účely dále používáno především ve smyslu bezpečí s vědomím souvisejících prvků zabezpečení, obecně zahrnující oba tyto významy) je možné chápat jako ochranu před ohrožením způsobeným informacemi a s nimi spojenými technologiemi. S rozvojem využití ICT ve všech oblastech života, ať už pracovního nebo osobního od velmi malých dětí (Chang[14] uvádí vystavení dětí internetu od dvou let) po seniory, se zvyšuje význam právě oblasti digitálních informací. Ve chvíli, kdy jsou tyto informace zaznamenány, je lze do jisté míry označovat jako digitální stopy.

Oblast digitálních stop se začala formovat později než informační bezpečnost, na rozdíl od ní proto ještě silněji vykazuje terminologický nesoulad. Ten vychází ze situace, kdy si každý obor definuje tento termín pro své potřeby. Sledujeme zde společný základ, zároveň i jistou míru odlišnosti. Pro srovnání lze uvést definice z oborů kriminalistiky (a dalších typů vyšetřování), marketingu a počítačové vědy.

Kriminalistika používá pojem digitální stopa ve smyslu *Digital evidence*, rozdíl v potenciálu stopy a výsledné hodnoty důkazu se vzhledem k zaměření na výsledek procesu spíše nerozlišuje[15]. Často je užívaná poměrně široká definice Scientific Working Group on Digital Evidence (SWGDE): „*Informace s důkazní*

[13] IRGENS 2013
[14] CHANG 2010, s. 501
[15] PORADA 2006, s. 5

hodnotou, která je uložena nebo přenášena v binární podobě.“[16] Tato definice je podle Raka a Porady[17] vhodná tím, že neomezuje využití důkazu při šetření jen na kriminalistiku, ale odpovídá obecnému forenznímu šetření i na komerční bázi, nezávislé audity atd. Stále je ale patrné, že vypovídající hodnota digitální stopy v tomto pojetí je limitována na využití jen pro velmi omezený účel šetření korektnosti jednání.

V oblasti počítačové vědy lze opět najít široké, i když mírně odlišné definice, např. „*informace o uživatelích odvozená ze senzorů*“[18]. Této definici v zásadě není co vytknout, snad jen chybějící důraz na využitelnost. Některé produkty digitální interakce mohou být nezachytitelné nebo nezachycené (např. na krátké elektronické signály) a je tedy sporné, do jaké míry se může jednat o stopy, když pozůstatek po činnosti nevznikne.

V oblasti marketingu se pojem digitální stopa používá ve spojení s různými variantami cíleného marketingu[19], termín ale není nijak explicitně vymezován. Je využíván široce, jedná se o jakoukoli informaci, kterou je možné využít při přizpůsobování reklamy konkrétnímu člověku pro zvýšení její efektivity[20]. Případně je pojem vymezován pro potřeby konkrétní práce, např. „*koncept digitálních stop jako vysoceúrovňová abstrakce pro reprezentaci stop zanechaných za lidmi, když implicitně nebo explicitně interagují s digitálním systémem.*“[21] Problematiky se může jevit využitelnost obsahu digitální stopy, ale také v tom, s jakou osobou je digitální stopa spojena. Může se jednat o informace, které vypovídají o někom jiném než o osobě, z jejíž činnosti vznikly.

Pro oblast informačních studií a knihovnictví byla použita definice digitálních stop Tonyho Fishe: „*záznam vašich interakcí s digitálním světem a jak data, která jsou zanechána za nimi mohou být využity.*“[22]

Zohledněním definic z různých oborů, především poslední uvedené, s přihlédnutím ke vztahu k informační vědě (viz kap. 0), lze formulovat definici pro účely této práce: Digitální stopy jsou informace v digitální podobě s vypovídací

[16] SWGDE and SWGIT Digital & Multimedia Evidence Glossary 2005
[17] PORADA 2006, s. 6
[18] KAPADIA 2007
[19] RAMSEY 2011
[20] Pervasive advertising 2011, s. 139
[21] Pervasive advertising 2011, s. 140
[22] FISH, Tony. Definition of a digital footprint (again). In: EKE 2012

hodnotou o konkrétní osobě, primárně fyzické, ale i právnické, a s reálným potenciálem jejich využití třetí stranou a zpětným vlivem na osobu, o které vypovídají. Vypovídací hodnota znamená jasnou vazbu na konkrétní osobu, která ale může být zprostředkována jeho 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 nutně pojených s digitálními stopami podle Fishe[23], tj. uložení, analýza a vytvoření hodnoty. Zpětná vazba k dané osobě pak vylučuje datové soubory slučující informace o mnoha osobách, které anonymizuje, akcent je kladen na udržení spojení digitální stopy a konkrétní osoby, resp. persony (digitální reprezentace konkrétní osoby). Tato zpětná vazba nemusí být negativní, např. narušení soukromí, ale i pozitivní, např. nabídka reklamy odpovídající zájmům.

Přestože digitální stopy mohou mít jak pozitivní, tak i negativní využití, je pro tuto práci podstatnější způsob, který je uživateli nepříjemný. Lze konstatovat, že v tomto případě by se jednalo 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 něm šířeny dál[24]. Nežádoucí užití digitálních stop je proto možné bezpochyby označovat jako soukromí. 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. Pokud ale dál bude operováno s narušením soukromí lze jej vnímat jako nežádoucí užití digitálních stop bez ohledu na právní úpravu.

Výše uvedený problém, s kým spojit digitální stopu vypovídající o někom jiném, než o jejím tvůrci, vyřešilo Pew Research Center[25] rozdělením digitálních stop na aktivní („*Osobní informace zpřístupněné online záměrným odesláním nebo sdílením informace uživatelem.*“[26]) a pasivní („*Osobní informace zpřístupněné*

[23] FISH 2009, s. 21
[24] volně dle WESTIN 1967
[25] MADDEN 2007
[26] MADDEN 2007, s. 4

online bez jakékoli záměrné intervence od jedince.“[27]). Aktivní stopy mohou mít různou podobu. Na jedné straně se jedná o informace, které o sobě člověk přímo zadává, např. blogy, informace v registračním formuláři, fotografie, e-maily apod. Proti tomu pasivní vytváří technická zařízení při jejich použití, 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 nebude s pojmy aktivní a pasivní digitální stopa příliš operováno, spíše budou členěny na technické[28] a uživatelské[29].

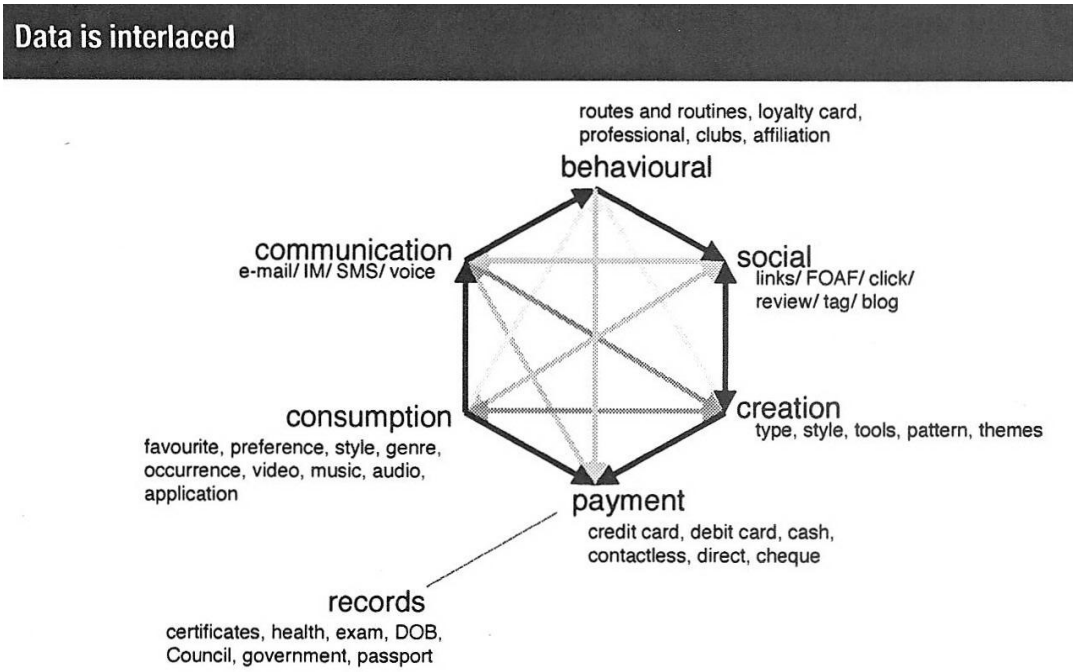
Jiné dělení, podstatné pro tuto práci, je podle zneužitelnosti informací obsažených v digitálních stopách. Jedno z takových vymezení uvádí Král:

> „*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.*“[30]

Problémem tohoto členění je jeho přílišné omezení na fyzickou osobu, přestože informace stejného typu a stejných možností využití mohou být spojeny s personou (např. heslo k elektronické službě), které slouží k prokázání totožnosti podobně jako informace ve fyzickém prostředí. Na příkladu e-mailové adresy, která se nachází s určitým rozdílem v prvních dvou kategoriích, je zřejmé, že informace může být zneužitelná na různých úrovních v závislosti na okolnostech. Na druhou stranu upozorňuje na možnost spojování nevýznamných a významnějších

[27] MADDEN 2007, s. 3
[28] Ve smyslu pasivních, termíny zavedené Fishem (FISH 2009, s. 22) *click data* a *digital trace* nebudou z důvodu problematického překladu využity, stejně jako pojem *content* pro následující typ digitálních stop.
[29] Resp. založené na chování uživatele, ať už se týkají jeho samotného nebo někoho jiného.
[30] KRÁL 2006, s. 100

informací, které společně vedou k vyšší možnosti užití digitální stopy (viz obr. 3). Bylo prokázáno[31], že toto spojení digitálních stop může vést k identifikaci jedince i po anonymizaci datových souborů (odstranění tradičně chráněných informací jako jméno, datum narození apod.).



Obr. 3 Typologie digitálních stop se zdůrazněním spojení[32]

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[33]. Podstatné je neopomenout, že se může jednat o hodnotu informace, ale i metadata (např. místo pořízení fotky) nebo odvozenou hodnotu (např. lokalita počítače pro přístup k internetu zjištěná pomocí IP adresy).

Digitální stopy jsou často zneužívány při internetových útocích z jejich podstaty nebo pro podpoření efektivity, svou roli při tom hraje zkvalitňování technického zabezpečení[34] a omezená informační gramotnost uživatelů. Stále

[31] OHM 2009
[32] FISH 2009, s. 79
[33] GRAYSON 2011, s. 24
[34] Institute of Management & Administration. Six Security Threats That Will Make Headlines in ’05. In: THOMPSON 2013, s. 222

silněji se projevuje již dlouho zdůrazňovaný fakt, že nejslabším článkem zabezpečení je člověk[35]. Mnoho stop vytváří člověk explicitně, jiné vznikají při běžném používání elektronických zařízení nebo činností třetí strany, často s omezeným vědomím uživatele o jejich existenci i možnostech využití i zneužití. V další části práce jsou proto vymezeny možné typy získání digitální stopy a následně různá využití, ať už z hlediska zákona korektní nebo ne.

2.1 Vznik a získání digitální stopy

Jak vyplývá z předchozí kapitoly, digitální stopy vznikají buď přímým zveřejněním informace (především aktivní stopy), nebo vlivem činnosti technického zařízení (pasivní stopy). Druhému uvedenému typu bude s ohledem na zaměření práce věnována omezená pozornost. Je vhodné o nich vědět, ale řízení jejich vzniku je omezené. Pokud se uživatel nechce vzdát používání technických zařízení, jsou možnosti popsány v kap. 3.2. Technické zabezpečení. Většina informací je poskytována prohlížečem, který při běžném nastavení zpřístupňuje webovému serveru (bez ohledu na Cookies) informace:

- „*Druh a verzi webového prohlížeče.*
- *IP adresu.*
- *Poslední stránku, kterou jste měli otevřenou, pokud jste pro přechod na aktuální stránku použili odkaz umístěný na předchozí stránce (...).*
- *Identifikaci vašeho poskytovatele internetových služeb.*
- *Verzi operačního systému.*
- *Typ používané jednotky CPU.*
- *Použité rozlišení obrazovky a barevnou hloubku (tuto položku odesílá pouze Internet Explorer).*“[36]

Jak vyplývá z posledního bodu, poskytované informace se mírně liší v různých prohlížečích. Další informace pak 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

[35] MITNICK 2003
[36] BOTT 2004, s. 436-437

zkvalitňování produktu, řešení problémů apod.). Tyto postupy a informace by měly být popsány v licenčních podmínkách daného produktu, kde se ale objevuje problém s tím, že podle statistických zjištění je většina uživatelů nečte[37]. To je problém především samotného uživatele, ale do určité míry i autora produktu, protože lze pochybovat, že byl opravdu udělen informovaný souhlas se zpracováním těchto informací[38]. Svou roli zde hraje i dynamika dokumentů, opakovaně vznikají nové verze, se kterými by se měl uživatel seznámit a i v případě, že to učiní, může být problém opustit ihned zavedenou službu, když uživateli přestanou vyhovovat nově nastavené podmínky v oblasti soukromí, jak ukázal pokus Facebooku se službou Beacon[39]. Přitom součástí podmínek nemusí být jen využití digitálních stop provozovatelem produktu, ale může být zahrnuta i možnost jejich poskytnutí třetím stranám pro různá využití. Podle Bechnann je rozhodnutí o přijetí podmínek užití především u sociálních médií (vč. social-pluginů, např. *Like* nebo *Tweet* na stránkách třetích stran) podmíněno ne jejich obsahem, ale předchozím přijetím přáteli, kterým daný člověk důvěřuje[40]. To vede k druhému jmenovanému typu digitálních stop.

Informace zpřístupněné online záměrným jednáním člověka výrazně více závisí na jeho vlastním rozhodnutí, proto by si měl být vědom důsledků, ke kterým toto zpřístupnění může vést. Proto je vhodné znát nejen bezpečnostní opatření, která především v bezpečném chování jsou spojena s posouzením řešené konkrétní informace, ale také jak je tato informace získána pro využití a co se s ní může stát vzhledem ke zpětnému ovlivnění uživatele, např. pocitem narušením soukromí.

Digitální stopy člověk zpřístupňuje dvěma základními způsoby, oba budou dále v textu brány v úvahu:

a) Zveřejněním je informace uložena tak, že je dostupná každému, kdo má odpovídající autorizaci (v případě veřejné informace nen nutná) a je možné ji vyhledat a získat. Tyto postupy jsou často legální, pokud nedojde k narušení informačního systému, např. prolomení hesla (viz kap. 3.1 Právní předpisy) nebo procházení dat uložených na zakoupeném použitém nosiči.

[37] BECHMANN 2014, s. 22
[38] Toto je nutný předpoklad pro legální zpracování osobních údajů podle práva Evropské unie dle Směrnice Evropského parlamentu a Rady 95/46/ES
[39] FISH 2009, s. 109
[40] BECHMANN 2014, s. 35

b) V přímé komunikaci může být zpřístupněná informace obsažena v obsahu sdělení (např. text e-mailu) nebo v metadatech[41] (např. e-mailové adresy dalších příjemců sdělení v hlavičce odeslaného e-mailu), odesílání těchto zpráv může být i automatické (např. již uvedené informace odesílané s udělením souhlasu v licenčních podmínkách bez opakované iniciace uživatele, časté v programech zdarma, jako freeware nebo shareware).

S rozvojem Webu 2.0 se výrazně zvýšila možnost uživatele publikovat libovolné informace snadno na internetu a sdílet je tak s ostatními. Může se jednat o komentáře v diskuzních fórech, fotoalba, vlastní videonahrávky, deníčky (blogy), ale také přímo informace o sobě (v různých službách pro seznámení) nebo jen komunikaci (s přáteli nebo lidmi se společnými zájmy). Všechny tyto informace je pak možné vyhledat, pokud je ponechána často přednastavená možnost veřejného přístupu, příp. s omezením autorizací.

Možnosti kontaktu se známými lidmi i těmi se společnými zájmy se v současnosti nejvíce projevují na sociálních sítích. Ty umožňují využít alternativ většiny typů komunikačních služeb, např. sdílení příspěvků či komentářů k nim, Instant Messaging, textové zprávy s možností přiložení souboru (funkce shodná s e-mailem) apod. Kromě sloučení typů komunikace slučují i profily, na které jsou vázané, přičemž klíčové je vyjádření vztahu mezi osobami (společná skupina, přátelé, příp. ještě rozčlenění do skupin a další). Z toho je patrné, že se jedná o informace, které o uživateli mohou sdělit mnoho poznatků využitelných různými subjekty. Jelikož se jedná o silně centralizovaný zdroj mnoha digitálních stop na vysoké úrovni zneužitelnosti dané typy i jasným spojením informací. Proto je zde ještě podstatnější důsledná autorizace informací i zvažování, zda je vůbec zpřístupnit, mohou být autorem služby zpřístupněny třetí straně, např. pro účely reklamy[42]. Především dospívající zde ale zveřejňují mnoho informací se silnou úrovní přímého zneužití, 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[43]).

[41] Přestože tyto typy údajů jsou jen omezeně chráněny zákonem (viz kap. 3.1), jejich hodnota může být vysoká, jak zdůrazňuje FISH 2009, s. 19, 44, 177

[42] Např. Facebook získává přibližně 2 bilióny dolarů ročně poskytováním informací o zájmech uživatelů pro účely reklamy. (VOGELSTEIN 2010)

[43] Tyto a související psychologické charakteristiky dospívání vedoucí k zveřejňování problematických informací podrobněji popisuje např. ŠIMÍČKOVÁ-ČÍŽKOVÁ 2003

Podrobnější údaje z výzkumů, jaké informace a v jaké míře děti a dospívající zpřístupňují na sociálních sítích jsou popsány v kap. 6.1.

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 některé informace na sociálních sítích, pokud veřejné. Problém se může objevit při velkém množství výsledků, ze kterých je těžké získat žádoucí informace, příp. v určení, zda patří ke sledované osobě, ne např. jmenovci. Pro toto ověření se využívá shody zjištění v různých zdrojích, vypovídající hodnotu má vzhled osoby, přezdívky, e-mailové adresy a další kontaktní údaje. Možností pro získání již smazaných informací, tj. i digitálních stop, jsou různé webové archivy, např. WayBackMachine.

Při vyhledání je možné použít různých nástrojů pro ověření dostupných informací člověkem, kterého se týkají, aby zjistil, kde je vhodné učinit bezpečnostní opatření (viz egosurfing v kap. 3.3). Pro tento účel lze vedle softwarů využít i speciální vyhledávače, tzv. People search engines[44], které se rozvíjí 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 osob, proto i výsledky jsou spíše faktografické než jen seznam zdrojů.

Všechny tyto informace jsou zveřejňovány s představou hodnoty, kterou poté uživatel získá, např. snadnost vyhledání a kontakt s přáteli nebo uznání vlastních kvalit. To ale někdy překročí úroveň vedoucí ke druhé kategorii, kdy jsou informace zpřístupněny v komunikaci, kdy přechodem je udělení autorizace k přístupu k informacím. Příkladem takového postupu, kdy je výhoda poměrně riziková, může být přijímání žádostí o přátelství z falešných profilů druhého pohlaví. Podle serveru Technet.cz[45] ji přijalo 60 % českých dospívajících mužů (15-20 let) a 42 % žen. Jiný průzkum v Los Angeles[46], blíže ke komunikaci mezi dvěma subjekty, ukázal hodnotu autentizačních údajů ve srovnání s výhodou v podobě poukazu na kávu za 3 dolary, kdy za tuto cenu sdělilo své heslo 66 % dotázaných a dalších 19 % jeho formát. Tyto výsledky ukazují, jak jsou lidé náchylní k požadavkům na poskytnutí i citlivých informací.

[44] např. Pipl, Spock nebo Spokeo
[45] KASÍK 2009
[46] LEYDEN 2005

Při komunikaci na úrovni kontaktu mezi jasně vymezeným okruhem příjemců (typicky dva komunikující, ale jsou možná i širší schémata, pro zjednodušení bude dále operováno jen se sděleními mezi dvěma lidmi) mohou být zjišťovány poměrně snadno různé informace. Jak bylo popsáno při vymezení digitálních stop (kap. 2), může být zjišťována jakákoli informace, rozdíl je ale ve snadnosti jejich zneužití, které někdy může být až při spojení s dalšími zjištěnými údaji. Proto někdy vznikají cykly zjišťování informací, kdy dříve zjištěné digitální stopy jsou uplatněny pro zvýšení úspěchu dalšího kroku, především již na úrovni interakce s člověkem, kterého se týkají. Důležité je, že citlivější informace na různých úrovních takto mohou být získány složitějšími postupy, kdy každý cyklus představuje pro člověka možnost zastavení dalšího postupu.

Tyto cykly, obvykle začínající u rešerše volně dostupných informací, jsou typické 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.*“[47] Jeho úspěch stojí na přesvědčivých, ale falešných žádostech, které odpovídají častým skutečným situacím. Člověk poskytující informaci obvykle nepředpokládá, že by právě daná komunikace měla být problém. Jedná se tedy spíše o psychologický útok, kdy informační technologie jsou jen vhodným prostředkem, ne nezbytně musí být využito technických možností, které nabízí (např. úprava hlavičky e-mailu může zvýšit jeho důvěryhodnost, protože budí zdání, že přichází od osoby oprávněné žádat danou informaci). Thomson[48] uvádí, že právě knihovny mohou být jednoduchým zdrojem informací o třetích stranách při sociálním inženýrství, přičemž 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, politik v organizaci 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

[47] THOMPSON 2013, s. 222
[48] THOMPSON 2013, s. 223-224

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).

Protože děti a dospívající mají omezenou životní zkušenost, mohou být náchylnější k sociálnímu inženýrství, zejména pokud využije dalších psychických charakteristik typických pro tato vývojová období. Děti, především citově deprivované, mohou být ovlivnitelné pro získání uznání a náklonosti, 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.

Vzhledem k jeho efektivitě se používá také jako podpůrný prostředek pro získání důvěry při různých typech útoků, např. při šíření škodlivých kódů (snaha přesvědčit k vlastní infikaci) nebo phishingu (poskytnutí údajů do podvrženého formuláře), které jsou popsány v kap. 2.2.2. Pro omezení vlivu sociálního inženýrství je zásadní dodržování pravidel bezpečného chování (viz kap. 3.3).

2.2 Užití digitální stopy

Digitální stopy jsou rizikem, jsou tedy nositelem potenciálu využití, které nemusí být příjemné. Může představovat legální, až zákonem dané postupy, např. vyšetřování internetového trestného činu. Jindy se může jednat skutečně o informační incident, který je na hraně právních, paraprávních nebo etických norem a někdy až za ní. Pro pochopení důvodů, proč je vhodné s digitální stopou zacházet uvážlivě, proto výrazně přispěje znalost možných důsledků jejich využití proti osobě, které se týkají (na obecné úrovni doplněné kazuistikami)[49].

[49] CHANG 2010, s. 526

2.2.1 Možnosti legálního využití

Digitální stopy na úrovni legálně dostupných informací, tj. především zveřejněných či poskytnutých se souhlasem člověka, kterého se týkají, mohou nabídnout vysokou hodnotu mnoha oblastem, kdy pozitivní je přínos pro toho, kdo je zpracovává, ale často i pro další osoby, ne vždy ty, které se informace týká.

Cílený marketing je přizpůsoben zájmům člověka, čímž se zvyšuje pravděpodobnost poskytnutí žádoucí informace v oblasti zájmu. To je pozitivní jak pro subjekt údajů (protože se omezí množství reklamy, které je vystaven, na tu s možností jej úspěšně oslovit) i pro prodejce, kdy se prokazatelně zvyšuje pravděpodobnost zakoupení daného produktu a je omezeno vkládání prostředků do reklamy k subjektům, kde je minimální pravděpodobnost jejich získání mezi zákazníky[50]. To odpovídá tradičnímu Face-to-Face prodeji, kdy dobrý prodavač odhaduje na základě pozorování a zkušenosti charakteristiky možného kupujícího, příp. se na něco doptá a na základě toho mu nabídne produkt, který bude odpovídat jeho zájmům a s větší pravděpodobností si jej zakoupí[51]. Kromě prokazatelného zájmu o inzerovanou oblast se zde dlouhodobě prosazuje využití podobných postupů, které jsou popsány u sociálního inženýrství v kap. 2.1[52].

Cílený marketing se vyvíjí desítky let, v současnosti je trendem behaviorální marketing[53] založený na analýze chování, kterou mohou být predikovány budoucí aktivity člověka. Využito je množství typů informací. Jednoduché osobní informace tvoří profil, kde formou odpovídajících si klíčových slov je nabízena reklama. Demografické, příp. geodemografické údaje slouží pro upřesnění zájmů (např. existují preference podle etnika[54], nebo že člověk žijící u Středozemního moře potřebuje jiné produkty než obyvatel Islandu). Pokročilá predikce staví na psychografických charakteristikách (nejčastěji dle marketingové segmentace PRIZM do 66 typů) a aktuálně vykovávaných činností (od vyhledávacích dotazů, přes geografickou polohu po fyzickou aktivitu, např. zatloukání hřebíků)[55].

[50] WEAVER 2007, s. 326
[51] Pervasive advertising 2011, s. 83-85
[52] MCLUHAN 2008, s. 20
[53] Part IV: Marketing & Promotion 2006; SULLIVAN, 2011
[54] FISH 2009, s. 33
[55] Pervasive advertising 2011, s. 87-90

Cílený marketing k dětem je často diskutován kvůli etice. Děti mohou být předmětem analýz stejně jako jiní lidé, ale někdy jsou úmyslně využívány prostředí a zájmy, které jsou relevantní primárně pro děti, např. internetové hry, se sociálními prvky pro virální šíření. Informace z profilu dítěte slouží jako zdroj pro cílenou reklamu, často přizpůsobovanou nově zjištěným informacím. Ve hře může být také 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 *game-vertising*[56]. Jinou variantou ceny za produkt je stažení žádaného softwaru (např. hry), která vedle poskytování zábavy slouží jako prostředník pro informace mezi telefonem dítěte a prodejcem inzerovaného zboží (na jednu stranu shromažďované údaje o dítěti, na druhou upozornění na akční cenu určitého zboží)[57].

Jako zdroj informací pro marketing i další využití jsou v současnosti nejvíce využívány vyhledávače (záznamy vyhledávacích dotazů, např. pro včasné detekování počátku chřipkové epidemie[58]) a sociální sítě (např. pro predikci vývoje společenské situace v politicky nestabilních oblastech[59] nebo nezaměstnanosti[60]). Jedná se v zásadě o monitoring společnosti pro předvídání nežádoucích jevů a možnost včasného zásahu. Pro tento účel je monitoring využívající digitálních stop použit i na úrovni jednotlivců. Monitoringem dětí a seniorů je podporována snaha o jejich bezpečí. Senioři jsou monitorováni především pro kontrolu jejich zdravotního stavu (tzv. telemonitoring)[61], kdy informace ze senzoru mohou být zasílány rodinnému příslušníku nebo zdravotnímu pracovníku, v tomto případě by mělo být rozhodnutí o využití telemonitoringu na seniorovi, protože jej může pociťovat jako narušení soukromí. V případě dětí se spíše jedná o monitoring místa pohybu, ale také různých činností online (viz mediační strategie v kap. 3). Často je používáno mobilní zařízení, které v současnosti obvykle obsahuje všechny potřebné senzory. Při tomto využití se někdy děti úmyslně rozhodnou *zapomínat* mobilní telefon doma, aby si uchránily své soukromí před rodiči[62] (viz kap. 3.2).

[56] CHESTER 2008
[57] CHESTER 2008
[58] GINSBERG 2008
[59] SUJA 2011
[60] NIKOS 2009
[61] VÁLEK 2009
[62] FISH 2009, s. 64

Podobně je tomu u monitoringu zaměstnanců, který sice neslouží tolik pro jejich ochranu, jako spíše pro ochranu zaměstnavatele. Sledována je tak pracovní činnost, především v pracovní době na služebním počítači, telefonu a dalších zařízeních, které mají možnost vytvářet digitální stopy. Bývají použity kamerové systémy, aby byly vyváženy zájmy zaměstnavatele i zaměstnance, především s přihlédnutím k zákonným pravidlům (např. Úřad pro ochranu osobních údajů vydal směrnici k požití kamer pro monitoring zaměstnanců[63]). Mezi těmito subjekty se vyskytují problematické způsoby monitoringu, např. čtení e-mailů[64] v pracovní schránce, ale také v osobní poště otevřené v pracovní době na pracovním počítači. Jedná se o velmi složitou oblast, kde je řešeno stanovení vhodných hranic v každé metodě monitoringu. Jejich hlubší rozbor je nad rámec této práce vzhledem k jejímu cíli. Pro předcházení problémů monitorují podobnými způsoby školy chování svých žáků, kvůli častému publikování informací na sociálních sítích jsou využívány především nástroje zaměřené na monitoring této služby[65].

Ve vztahu zaměstnavatel – zaměstnanec není monitoring jediným využitím digitálních stop. Dle výzkumů slouží často při rozhodování o přijmutí zaměstnance, s čímž je často operováno v americkém prostředí při vzdělávání k digitálnímu občanství[66] (viz kap. 4.3). Vlivem impulzivnosti a experimentování s různými věcmi (vč. návykových látek, partnerů apod.) v tomto vývojovém období[67] a omezené možnosti zcela odstranit jednou vzniklou digitální stopu, totiž může dospívajícím neuváženou drobností vzniknout výrazný problém pro celý život.

Rozšířenost užití digitálních stop pro tento účel lze doložit výzkumy:

- 59 %[68] - 75 %[69] potenciálních zaměstnavatelů dělá rešerši žadatelů o zaměstnání na sociálních sítích;
- totéž dělá 91 % personalistů[70], využívají především Facebook (76 %), Twitter (53 %) a až následně specializovanou profesní sociální síť LinkedIn (48 %), 69 % dotázaných někdy odmítlo žadatele kvůli jeho digitální stopě;

[63] viz Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009 2014
[64] POŽÁR 2005, s. 282
[65] WEAVER 2010, s. 26
[66] GRAYSON 2011, s. 9-10
[67] VÁGNEROVÁ 2000, s. 210
[68] Careerbright. You have been searched - What did we find about you? In: EKE 2012
[69] 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
[70] SWALLOW 2011

- 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.[71]

Digitální stopa může člověku, o kterém vypovídá, pomoci, pouze pokud prezentuje jeho kvality, ale stejně tak může mít negativní důsledky, pokud prezentuje jednání proti zájmům zaměstnavatele. Mezi ně lze zařadit[72] 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. problém může představovat i zjištění nepravdivého údaje o kvalifikaci.

Monitoring v HR (řízení lidských zdrojů), ať žadatelů o zaměstnání nebo zaměstnanců, slouží jako prevence problému. Když už k němu dojde, přichází ke slovu jiné uplatnění digitálních stop, které jsou vyhledávány, analyzovány a vyhodnoceny v rámci forenzního, příp. kriminálního vyšetřování. Mohou prokázat jak alibi, tak i spáchání nežádoucího jednání. Uplatňují se všechny typy digitálních stop, roli mají především ty, které jsou méně pod vlivem člověka, tj. pasivní stopy. 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 o elektronických komunikacích, který byl po zásahu Ústavního soudu[73] právě v této oblasti upraven pro větší ochránu soukromí. Mobilní zařízení lze ale při vyšetřování využít i jako mikrofony, a to i při vypnutí po vzdálené aktivaci[74]. Počítačová kriminalita, příp. kriminalita počítačově související (např. e-mail po vraždě nebo kamerový záznam spáchání trestného činu)[75] patří k základním využitím digitálních stop pro legální účely, jak je patrné v kap. 2 při definování tohoto pojmu. Na straně pachatelů i vyšetřovatelů jsou často používány sofistikované metody práce

[71] GRAYSON 2011, s. 9
[72] MOORE 2012, s. 86; SWALLOW 2011
[73] Nález Ústavního soudu ze dne 22. 3. 2011, spis. zn. N 52/60 SbNU 625
[74] GRAYSON 2011, s. 11-12
[75] PORADA 2006, s. 4-5

s digitálními stopami[76]. Rak a Porada[77] uvádějí, že digitální stopy při šetření nejsou používány jen pro doložení klíčových činností, ale i pro budování profilů zájmových osob, např. pomocí záznamů e-komerce. Z toho je patrné, že digitální stopy si ve vyšetřování různých typů nekorektního jednání budují své místo, ať bylo jejich cílem cokoli, protože dokládají nejen podněty k řešenému činu, ale i k osobám, které jsou s ním spojeny.

Kriminálistika spadá pod výkon veřejné správy. V ní se digitální stopy uplatňují v mnoha dalších směrech. Slouží často pro ochranu zájmů státu nebo jiných lidí než toho, kterého se týkají (např. ve veřejných informačních systémech typu katastr nemovitostí si může kupující ověřit majitele a případná břemena na kupované nemovitosti). I to je jeden z důvodů, proč dochází k otevírání informací veřejné správy veřejnosti (např. podle zákona o informačních systémech veřejné správy musí být všechny veřejné rejstříky a systémy dostupné i přes internet), přestože to snižuje soukromí občanů. Vedle těchto informačních zdrojů spojitelných často s určitou osobou, stát prosazuje zavádění elektronických služeb do svých činností (e-Government), kdy stát pro své potřeby vytváří nebo požaduje po uživateli vytvoření digitálních stop, které sám využívá[78]. Jedná se například o různé elektronické identifikační karty (např. občanský průkaz se strojově čitelnými údaji nebo elektronické zdravotní karty, např. Karta života Zdravotní pojišťovny Ministerstva vnitra ČR). Stát se tak stává správcem velmi rozsáhlé databáze digitálních stop o každém občanovi, které mohou být zneužity, např. nesprávným chováním úředníka[79]. Pro užití digitálních stop pro své potřeby se ale neomezuje na údaje, které mu byly na vyžádání poskytnuty (např. různými formuláři, může je spojit s veřejně dostupnými údaji, třeba pro identifikaci podezřelých osob z daňových podvodů). Právě tento účel je jednou z funkcí nástroje E-Benefits systém[80], jehož využitím stát usiluje o svou vlastní ochranu využitím všech typů digitálních stop, které se mu nabízí ke zpracování. Vedle ochrany finančních zájmů státu jsou digitální stopy využívány i pro ochranu před

[76] Formou kazuistik prezentuje LATTA 2011
[77] PORADA 2006, s. 14
[78] Výhody i nevýhody v oblasti omezení soukromí podrobně popisuje LYON 1994
[79] 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
[80] NIXON 2010, s. 151-168

nepřáteli státu na úrovni politické, vznikají např. různé algoritmy pro vyhledávání možných projevů teroristů.

Přestože jedinec může pociťovat narušení soukromí, různé typy institucí využívají jeho digitální stopy legálně. Určité typy digitálních stop vznikají i proti vůli člověka, kterého se týkají, většinu ale může ovlivnit. Pak zbývají pro prevenci vzniku a řízení digitálních stop možnosti technických nástrojů a chování. Řešení jsou sice omezenější, na druhou stranu většina z těchto užití respektuje určitou hranici, za kterou by neměly jít třeba proto, že si potřebují udržet důvěru lidí, aby byly jejich služby nadále využívali. V případě internetových útoků je situace naprosto opačná a i když zde mohou pomoci právní opatření, problémy, které způsobují subjektům informací, přesto převyšují výše popsané.

2.2.2 Útoky se zneužitím digitální stopy

Typy užití digitálních stop 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.). Tato omezení se netýkají útoků zneužívajících digitální stopy. Sama ztráta či získání informace je „*významným motivačním faktorem pro páchání trestné činnosti*“[81]. Cílem může být získání dalších, citlivějších informací (viz kap. 2.1) nebo poškození uživatele či jeho zařízení (především dat). Obecně mohou být internetové útoky cílené (zaměřené na konkrétní cíle) nebo necílené (plošné, např. hoax). Často se ale v konkrétním případě jedná o stav mezi těmito extrémy, protože určitá cílenost může být již jazykovou mutací, což je relevantní zaměření pro české prostředí. Necílené útoky bývají méně efektivní. Proto oslovují více možných obětí, proti tomu cílené svou konkrétností a zaměřením na charakteristiky relevantní pro konkrétní cíl jsou sice náročnější, ale o to úspěšnější. Z hlediska zaměření této dizertační práce budou popsány typy útoků, které slouží k získání citlivějších informací, dále útoky cílené pomocí zjištěných digitálních stop a nakonec budou stručně zmíněny nejčastější typy útoků, kde jsou digitální stopy využity jen pro podporu úspěšnosti útoku, který je ve své podstatě nepotřebuje.

[81] POŽÁR 2005, s. 53

Jak je uvedeno v kap. 2.1, mezi typické útoky pro další získání informací je možné zařadit phishing a pharming, které jsou založeny na kontaktování uživatele a jeho přesvědčení o nutnosti zadat autentizační a případně i další údaje do připraveného formuláře, který je podvržený útočníkem. Nejznámější jsou tyto útoky ve spojení s finančními institucemi, jako jsou např. banky nebo spořitelny, ale tento útok na ně není omezený, může se jednat i o údaje do elektronických aukcí, sociálních sítí apod.[82] Základní metodou zde je phishing, který využívá formuláře pro údaje obvykle ve formě podvržené webové stránku. Útok lze proto rozpoznat díky nesprávné URL adrese, která neodpovídá instituci, za kterou se vydává, a to jak v uvedených informacích, tak obvykle i v grafické podobě. Proti tomu pharming využívá tzv. *DNS cache poisoning*, kdy dojde ke změně záznamů DNS pro převod jmenných adres na IP adresy[83], a to buď uložených v počítači uživatele, nebo dokonce přímo v DNS serveru. Při pharmingu je pak na správnou adresu zobrazena podvržená stránka, odhalení je tím náročnější. Aby kontaktní zpráva působila důvěryhodně, využívá sociálního inženýrství (viz kap. 2.1) a obvykle i úpravy odesilatele v hlavičce e-mailu (proto je častá žádost o neodpovídání, jako důvod bývá uvedeno automatické generování e-mailu). V případě, že se útok podaří, jsou obvykle autentizační údaje využity ke krádeži identity (viz dále v této kapitole).

K získání autentizačních údajů může dojít i uhodnutím či zjištěním specializovaným softwarem. Jak by mělo vypadat silné heslo, aby se omezilo, až znemožnilo prolomení, popisuje kap. 3.2. Obvyklý postup totiž spočívá nejdříve v hádání autentizačních údajů, např. v poli heslo je zkoušeno slovo *heslo*, řetězec *123456*, datum narození a další zjištěné informace o zkoušené oběti. Pokud se ho nepodaří uhodnout, dochází k automatizovanému hádání, nejdříve slov ze slovníku s drobnými variacemi (vložení číslice, psané pozpátku apod.) a nakonec zkoušení všech kombinací znaků, které je ale při dlouhém hesle časově náročné. O prolamování hesel se nepokouší jen kriminálníci. Podle výzkumu[84] ve Velké Británii 25 % dospívajících někdy zkusilo prolomit přístup do facebookového účtu jejich kamaráda, přestože si byli vědomi toho, že to není správné.

Jiným častým útokem pro získání informací jsou různé varianty malwaru (škodlivý kód). Není nutné je klasifikovat, protože v praxi jsou charakteristiky

[82] KIM 2011, s. 677
[83] KRÁL 2006, s. 230
[84] WEAVER 2010, s. 27

spojovány a často proto nelze konkrétní malware zařadit do jediné kategorie. Pro oblast digitálních stop stojí za zmínku spyware (základní charakteristikou je shromažďování libovolných informací a jejich odesílání na definované místo), keylogger (vytváří a odesílá záznamy stisknutých kláves), password stealer (spyware specializovaný pouze na autentizační údaje) a ransomware (využívá vydírání, např. znepřístupněním dat, pohrůžkou trestního stíhání za porušení zákona, pohrůžkou zveřejnění zjištěných informací apod.). Všechny tyto typy malwaru se mohou objevit i na nedostatečně zabezpečeném veřejném počítači, např. v knihovně, kde se vlivem použití mnoha uživateli výrazně zvyšuje přínos pro útočníka a naopak problémy pro uživatele i provozovatele. K nákaze může dojít různými způsoby, aktuálně je běžné infikování přes USB disk považovaný za ztracený, přes stažený software ze služby pro sdílení souborů, jako ovládání prvku ActiveX na webové stránce, přes přílohu v e-mailu, přes neošetřenou zranitelnost v prohlížeči, přehrávači videí, klienta pro zprávy atd.[85]

Mezi útoky patří nabourání se do počítače přes malware typu backdoor (zadní vrátka, umožní ovládání počítače nebo služby na dálku) nebo přes otevřené porty zjištěné jejich skenováním. Tyto postupy mohou vést až k plnému ovládnutí počítače, příp. alespoň možnosti procházet a případně i upravovat data v něm uložená, tj. získat přístup k digitálním stopám přímo v zařízení uživatele. Posledním uvedeným útokem pro získání informací jsou útoky na majetek, které mohou mít formu zjištění informací z odpadků (elektronických i papírových), ale také vykradení domu a tím získání zařízení s uloženými digitálními stopami. K tomu přispívá zveřejňování informací o místě, kde se člověk nachází, např. na sociální síti nebo geolokační hře (typu Foursquare). Pro upozornění na tento problém vznikla (a krátce v roce 2010 fungovala) stránka pleaserobme.com[86].

Při zjištění dostatku informací o oběti se za ni může začít útočník vydávat, jedná se tedy o krádež identity. Podle toho, jaké různé údaje zjistil, a kde se jimi může dostatečně prokázat, může jménem oběti dělat vše, co mu tato krádež umožňuje. 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, může začít urážet její přátele a budovat negativní

[85] KIM 2011, s. 684
[86] Pervasive advertising 2011, s. 98

digitální stopu, která může oběti ublížit v osobním i profesním životě, jak již bylo uvedeno. 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, a dodatečné informace prokazují jeho příslušnost k dané osobě. Náprava důsledků krádeže identity je velmi složitá, Identity Theft Resource Center odhaduje její časovou náročnost v průměru na 330 hodin[87].

Především k dětem jsou z hlediska bezpečnosti digitálních stop směřovány informace k sexuálně orientovaným počítačovým incidentům, jako je grooming a sexting. Grooming představuje získání digitálních stop, často z přímé komunikace mezi obětí a útočníkem, kdy cílem je sexuální zneužití dítěte. To přitom nemusí probíhat jen pohlavním aktem ve fyzickém prostředí, může mít i nekontaktní formu, jako svlékání dítěte před webkamerou (to může vést k sextingu, viz další odstavec) nebo vystavení dítěte obscénní komunikaci.[88] Pokud má dojít ke kontaktnímu zneužití, bývá dlouhodobě budována důvěra dítěte, aby souhlasilo se schůzkou. Opět má 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) partnera[89]. Přitom je běžné, že útočník mění své jméno, věk i pohlaví[90]. Problém je, že děti se často mylně domnívají, že by v komunikaci dospělého poznaly[91], čímž se zvyšuje rizikové chování. Schůzka je možná i v případě, že útočník o oběti zjistí, kde se nachází, což může být snadné díky již zmíněné oblibě geolokačních her, sociálních sítí a zveřejňování místa bydliště, školy a kroužků. Kybergrooming není jen záležitost preferenčních pedofilů[92], 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. 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[93].

[87] KIM 2011, s. 678
[88] VANÍČKOVÁ 1997, s. 12
[89] ŘÍČAN 1990, s. 197
[90] Využití internetu dětmi ve věku od 12 do 17 let 2006
[91] Safer Internet for Children 2007
[92] VANÍČKOVÁ 1999, s. 33
[93] LEANDER 2008, s. 1261

S groomingem souvisí sexting, tj. zasílání sexuálně explicitního obsahu spojeném s obětí[94], který může být následně zveřejněn. Problém se obvykle vyskytuje u dospívajících, kteří si tyto dokumentace posílají v partnerském vztahu, ale po jeho ukončení může s cílem pomsty dojít ke zpřístupnění materiálu dalším lidem. Toto byl případ Jessicy Logan a Hope Witsell, které v důsledku sextingu spáchaly sebevraždu[95]. Sexting je problémem i v České republice, v roce 2012 poslalo 8,99 % a zveřejnilo 7,23 % dětí fotografii nebo video, na kterém byly zobrazeny částečně či zcela nahé[96]. Podle National Center for Missing & Exploited Children 51 % dívek, které takové materiály poslalo, k tomu bylo tlačeno chlapcem[97]. Vzhledem k obsahu materiálů u dospívajících při sextingu v podstatě dochází k šíření dětské pornografie, které je trestné.

Zneužitím sexuálního zobrazení dítěte proti němu je naplněna charakteristika kyberšikany, která spočívá v poškození s využitím informačních technologií[98], ať už má formu ponižování, pomluvy, pronásledování, sexuálního harašení, záznamu násilí nebo jinou. Kyberšikana proti tradiční šikaně má specifika, která zesilují důsledky pro oběť, jsou vázány především na neustálou dostupnost komukoli. Ke kyberšikaně se tak mohou přidat nejen děti z okolí, ale miliony lidí na internetu, únik je v podstatě nemožný. Protože při kyberšikaně vznikají digitální stopy poškozujícího jednání, problémem je dlouhodobější působení na oběť a možnost, že se poškozující obsah objeví kdykoli znovu. I v tomto případě již mezi důsledky kromě psychických obtíží patří případy sebevražd dětí, např. Megan Meier[99]. Původci kyberšikany si často nejsou vědomi toho, že jinému ubližují, považují své jednání za nevinnou hru[100]. S kyberšikanou úzce souvisí stalking, nebezpečné pronásledování, které oběť také poškozuje, protože stalker chce, aby o jeho činnosti věděla. Podle Moore[101] zatím stalkeři neobjevili plně sílu informačních technologií a stále se silně váží na tradiční metody, je tedy pravděpodobné, že v budoucnu tento problém vzroste. Stalking je v České republice trestný čin, ale až po překročení stanovené úrovně (dlouhodobé, min. 4-6 týdnů,

[94] DÖRING 2014
[95] DÖRING 2014
[96] Výzkum rizikového chování českých dětí v prostředí internetu 2013 2013
[97] GRAYSON 2011, s. 30
[98] LIVINGSTONE 2011, s. 61
[99] KIM 2011, s. 679
[100] Safer Internet for Children 2007
[101] MOORE 2012, s. 90

opakované, min. 10 pokusů, obtěžování přítomností útočníka s důvodnou obavou o život či zdraví oběti či jejích blízkých)[102].

Mezi další internetové útoky by bylo možné zařadit různé typy nevyžádaných zpráv, které zneužívají digitální stopy v podobě kontaktních údajů, které jsou často shromážděny automaticky pomocí robotů (např. rozpoznání typického tvaru e-mailové adresy při procházení webu nebo diskuzních fór) nebo jsou prodávány jejich databáze. Tyto zprávy se obvykle šíří plošně, jejich význam pro zde řešenou problematiku je tedy omezený. Další internetové útoky, které podobně jako nevyžádané zprávy s digitálními stopami souvisí téměř výhradně na úrovni získání kontaktní informace, není pro cíl této práce relevantní.

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

2.3 Ochrana digitálních stop před nechtěným užitím

Jak je uvedeno především v kap. 2.2.1, 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 hodnocení digitální stopy lze rozlišovat informace podle toho, jak snadno umožňují identifikaci člověka nebo využití či zneužití jejich obsahu třetí stranou, přičemž i to se často spojuje s potřebou identifikace. Kategorizace informací z tohoto hlediska je podrobněji popsána v kap. 2. Kvantitativní rozměr digitální stopy je podstatný proto, že čím více informací o subjektu je dostupných, tím snazší je využití[103] (podobně jako u kvalitativního přístupu).

[102] ŠÁMAL 2010, s. 3006 – 3008
[103] ANGWIN 2010

Pro podporu bezpečnosti digitálních stop lze využít různá opatření jak pro předcházení rizikovému chování v podobě nevhodného vzniku digitálních stop, tak v jejich řízení, vč. odstranění, a v řešení informačních incidentů, které digitální stopy využívají v neprospěch osoby, které se týkají (viz kap. 2.2.2). Využít lze základních pravidel informační bezpečnosti, chování člověka pro odpovědné budování digitální stopy by nemělo být paranoidní, ale uvážlivé. Pro podporu bezpečnosti pak lze využít i různých typů softwarů a online nástrojů, které mohou přispět v různých, ale spíše dílčích oblastech bezpečnosti digitálních stop. Jako prevence, ale také pro řešení již uskutečněného informačního útoku, mohou pomoci právní akty. Je evidentní, že pro podrobnější popis těchto řešení na různých úrovních není s ohledem na odlišné zaměření této dizertace prostor. Z toho důvodu se dále tato práce omezuje na prostředí knihovny. V případě bezpečného chování, které musí uskutečnit jedinec sám, pak na oblasti, které může knihovna podpořit, především vzděláváním. Vzhledem k tomuto posunu jsou všechny tři oblasti možné aplikace bezpečnostních opatření pro digitální stopy popsány v následující kapitole a jejích podkapitolách.

3 Informační bezpečnost v knihovně se zaměřením na digitální stopy

Knihovníci, stejně jako rodiče nebo učitelé, mají možnost využít různých typů opatření pro řízení bezpečnosti digitálních stop svých uživatelů, dětí. Každé bezpečnostní opatření ale snižuje komfort nebo i možnost svobodného přístupu k informacím, což je zásadní hodnota reprezentující knihovnu. Knihovna proto nemůže využít všech možností, které se jí pro zvýšení bezpečnosti nabízejí, ale musí je zvažovat, aby nalezla co nejlepší rovnováhu mezi přístupem k informacím a jeho bezpečností. Knihovnám toto zvážení není možné připravit na úrovni šablony, vždy záleží na individuálním posouzení, např. na základě dřívějšího chování dětí na počítačích v knihovně (podle specifických charakteristik skupiny uživatelů v dané knihovně mohou být zastoupeny různě často odlišná rizikové chování nebo informační incidenty, preferována může být více také odlišná mediační strategie – viz níže v této kapitole). Sama knihovna by měla uvážit, jaké hodnoty vyzdvihuje vůči svým uživatelům, jakou si buduje reputaci. Při zvažování strategií bezpečnostních opatření je kromě jejich nasazení nutné zvažovat i specifikum spočívající v tom, zda při strategiích vytvářejících záznamy o činnosti dětí na internetu nebo jejich zjištění knihovníky budou tyto informace vnímány jako soukromé a tedy dostupné jen dítěti a knihovníkovi, nebo i rodičům dítěte jako jeho zákonným zástupcům[104]. Toto poskytnutí informací by mohlo silně poznamenat důvěru dítěte v knihovnu pro oblast informační bezpečnosti a mohlo by snížit zde prezentované výhody knihoven pro řešení problematiky. Na základě toho si sama určí poměr různých typů mediačních strategií v oblasti internetu, která bude odpovídat zastávaným hodnotám a potřebám.

Mediační strategie knihoven v oblasti práce na internetu jsou popsány jen omezeně[105]. Více pozornosti je věnováno školám[106], primárně se ale odborné publikace zaměřují na rodiče[107], jako klíčové subjekty při řízení přístupu dětí k internetu. Při stanovování možností mediací knihovnou se lze inspirovat právě strategiemi odlišných subjektů. Opatření, která lze aplikovat, jsou předmětem

[104] WOLD 2010, s. 72
[105] WOLD 2010
[106] LIVINGSTONE 2011, s. 121-127
[107] LIVINGSTONE 2011, s. 103

následujících podkapitol a částečně jsou přeneseny i do kap. 4.3 Bezpečnost digitálních stop ve vzdělávání v knihovnách (aktivní mediace). Pro přiblížení typů mediačních strategií pro informační bezpečnost (tedy nejen digitálních stop) je dále využito dílčích opatření, která do nich spadají a která sloužila pro jejich operacionalizaci v rámci výzkumu EU Kids Online[108]:

- Aktivní mediace používání internetu (bez omezení na informační bezpečnost): rozmluva o činnostech dítěte na internetu, přítomnost (rodiče) při použití 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 použití internetu, doporučení způsobů chování k jiným lidem online, mluvení o reakcích na pocit poškození něčím na internetu, pomoc v minulosti s něčím poškozujícím dítě na internetu;

- Restriktivní mediace (stanovení pravidel pro uvedené činnosti): rozdávání osobních informací na internetu, nahrávání fotek, videí nebo hudby k sdílení s dalšími, stahování hudby nebo filmů přes internet, vlastní profil na sociální síti, sledování videoklipů na internetu, použití služeb Instant Messagingu;

- Monitoring: navštívených webových stránek, profilu dítěte na sociální síti nebo v online komunitě, přátel nebo kontaktů přidávaných k profilu na sociální síti, zpráv v e-mailovém nebo Instant Messagingovém účtu dítěte;

- 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.

Mediace na všech těchto úrovních i způsobech může být využita i v prostředí knihoven. Jejich volba by měla vycházet ze znalosti různých alternativních přístupů a vědomí jejich výhod i nevýhod. Vliv může mít také prostředí, tj. co je pro danou komunitu obvyklé a akceptované. Podle EU Kids

[108] LIVINGSTONE 2011, s. 103-130

Online[109] patří Česká republika ke státům, kde je nejvíce zastoupena aktivní mediace použití internetu (využívá jí 96 % rodičů) i internetové bezpečnosti (94 % rodičů), naopak v restriktivní strategii patří ČR mezi nejméně ji využívající (78 % rodičů). V oblasti monitoringu a technické mediace Česká republika vykazuje spíše středové hodnoty v zastoupení. Pokud tedy knihovny budou reflektovat přesvědčení rodičů o vhodných přístupech, měly by se zaměřit na aktivní mediace a méně restriktivní. To je i vhodný přístup pro co nejmenší ovlivnění přístupu dětí k informacím – nebudou v něm omezovány, spíše bude rozhodnutí přeneseno na ně. To odpovídá také názoru Wolda[110] na základě jeho výzkumu mezi učiteli a knihovníky v Norsku. Aktivní mediace použití internetu současně vede k snížení rizikového jednání i poškození dětí na internetu, naopak technická nemá na riziková jednání vliv[111]. Zajímavé je, že aktivní mediace internetové bezpečnosti a monitoring vedou ke zvýšení rizikového jednání, nicméně se může jednat o strategii učení pro vyrovnávání se s riziky[112]. Proti tomu podle jiného výzkumu[113] vede diskuze dětí s rodiči o problémech zpřístupňování osobních informací na internetu ke snížení tohoto jednání dětí.

Z hlediska jiného členění se ukazuje[114], že všechny mediační strategie s rostoucím věkem dětí ubývají, především mezi 14 a 15 rokem života, při hodnocení dle socio-ekonomického statusu nejsou rozdíly kromě aktivní mediace, která se při vyšším statusu také objevuje častěji, což může naznačovat 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 Digital Divide, proto je vhodné zvážit i tyto faktory při nastavování mediační strategie knihovny podle prostředí.[115]

Protože dítě je samostatný jedinec a jeho názor nemusí odpovídat tomu dospělého, je podstatným zjištěním EU Kids Online[116], že dle 72 % dětí by se

[109] LIVINGSTONE 2011
[110] WOLD 2010
[111] DUERAGER 2012
[112] DUERAGER 2012
[113] ÁLVAREZ 2013
[114] LIVINGSTONE 2011
[115] ÁLVAREZ 2013
[116] LIVINGSTONE 2011

neměly měnit rodičovské mediace, snížení nebo zvýšení zájmu rodiče o dítě na internetu se objevují ve srovnatelném množství ve zbývajících odpovědích. V ČR přitom zájem o zvýšení zájmu patří mezi nejméně vyjádřené (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). Z toho vyplývá, že české děti by v knihovně pravděpodobně uvítaly volnější použití internetu a také by mohlo být vhodné doplnění aktivní mediace rodičů jinými subjekty, aby se snížilo množství dětí, které se bezpečnostními doporučeními neřídí, ale ignorují je. Pokud tímto subjektem bude škola, je možné vzít v úvahu zde zjištěné zastoupení mediace, podle EU Kids Online[117] 73 % dětí si je vědomo, že učitel využil alespoň jeden ze sledovaných postupů aktivní mediace (81 % při libovolném ze zjišťovaných), ale také že aktivní mediace ve škole s věkem dítěte roste (proti klesání v rodině), přestože i v nižším věku děti internet používají. Stále tedy zbývá poměrně výrazné zastoupení dětí, pro které by bylo vhodné hledat jiný zdroj mediace. Výhodou škol, kterou uznávají i knihovníci, je jejich možnost zasáhnout všechny děti[118]. Poměrně výrazný, především v České republice[119], je vliv vrstevníků i v mediaci použití internetu, což přispívá k vhodnosti přístupu aktivního učení, který je aplikován v navržených lekcích metodiky v této práci (viz kap. 8.2). Subjektem pro poradenství o internetové bezpečnosti mohou být i knihovny, především pokud budou rozvíjet připravenost na tento úkol, protože již v současnosti je děti uvádí mezi zdroje pro tyto rady[120], byť ne ve výrazné míře.

Wold[121] 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, které jsou v silněji formálních prostředích, jako je škola, nepředstavitelné. Podle jeho výzkumu sami knihovníci vidí internetové služby v knihovně jako pokračování jejich tradiční role zpřístupňování informací[122]. Tyto služby zahrnují (především u dospívajících) komunikaci přes

[117] LIVINGSTONE 2011
[118] WOLD 2010, s. 71
[119] LIVINGSTONE 2011, s. 124
[120] LIVINGSTONE 2011, s. 127
[121] WOLD 2010
[122] WOLD 2010, s. 67

internet, nejen vyhledávání informací, podpora těchto činností zlepšuje i vztah dospívajících ke knihovně[123]. Právě tento vztah představuje problém, se kterým se v současnosti knihovny snaží vyrovnat.

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 nejvíce zastoupené[124], aktivní, mediační strategie, podporuje efektivitu všech těchto oblastí a současně představuje jádro této práce, proto se mu věnuje 4. kapitola.

3.1 Právní předpisy

První úroveň ochrany je dána nikoliv na úrovni konkrétního člověka, ani instituce, ale na úrovni státu. Ten nastavuje minimální úroveň ochrany digitálních stop pomocí právních aktů, stejně jako v jiných oblastech. Zákon musí dodržovat každý, v opačném případě může být potrestán stanovenou sankcí za daný prohřešek. V případě bezpečnosti digitálních stop uživatelů v knihovnách proto knihovna musí v první řadě mít jistotu vlastního zajištění vůči bezpečnosti na úrovni ochrany soukromí jejích uživatelů, kterým poskytuje přístup k internetu. Musí tedy řešit své postavení v situacích:

- dává k dispozici nástroj, pomocí kterého mohou vzniknout, být získány a využity (či zneužity) digitální stopy,
- nabízí elektronickou službu (informační systém), v rámci kterého je nakládáno s digitálními stopami,
- sama knihovna může být subjektem, který digitální stopy konkrétních lidí tvoří a spravuje (účty uživatelů pro potřeby knihovny).

Právo je komplexní oblast, kde nelze na konkrétní situaci obvykle aplikovat jediný předpis, ale je nutné vzít v úvahu vazby a také specifika konkrétní situace. Přesto je možné identifikovat základní předpisy, které se nejčastěji vztahují k výše

[123] WOLD 2010, s. 68
[124] LIVINGSTONE 2011, s. 104

uvedeným situacím. Všechny dále uvedené předpisy jsou využity ve znění platném ke dni 31. 8. 2014.

V první řadě, pokud bereme v úvahu právní sílu předpisů, je nutné uvést Listinu základních práv a svobod, na kterou další jmenované dokumenty v zásadě navazují. Listina stanovuje nejobecnější garance, které jsou následně specifikovány v zákonech a odvozených právních aktech. Pro oblast digitálních stop se jedná především o čl. 10, kde je postupně zaručeno právo na ochranu osobnosti člověka na úrovni pověsti, důstojnosti, jména a cti, což mnoho hrozeb zneužívajících digitální stopy překračuje, např. kyberšikana, krádež identity apod. Blíže k podstatě digitálních stop mají následující odstavce. Ochrana před neoprávněným zásahem do soukromí je poměrně spekulativní oblast, protože každý člověk definuje hranici soukromí na odlišné úrovni. Nicméně jedná se právě o soukromí, které je ohroženo při získávání digitálních stop, o jejichž možné dostupnosti subjekt údajů nevěděl (ať už proto, že je vytvořil někdo jiný, nebo že si uživatel nebyl vědom technické možnosti získat k těmto datům přístup). Poslední odstavec zaměřený „*na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*“[125] je podrobněji rozveden níže u zákona o ochraně osobních údajů, který je ním úzce spojen. Za zdůraznění ovšem stojí, že Listina uvádí údaje o osobě, což je výrazně širší definice než osobní údaj dle zákona č. 101/2000 Sb. Dále je podstatný čl. 13 garantující ochranu tajemství listovního a jiných písemností a záznamů uchovávaných v soukromí nebo zasílaných poštou, podávaných telefonem, telegrafem a podobným zařízením, tedy i internetem. Na toto, stejně jako na zmiňovanou ochranu osobních údajů, navazuje trestní zákoník (§ 182 a § 183), kdy hranice tajemství přesahuje obsah komunikace a dokumentů, ale ne metadatové údaje, přestože i ony mohou prozradit podstatné informace. Naopak čl. 17, odst. 4 dává právo svobodně vyhledávat a šířit informace, což ale lze omezit zákonem pro ochranu druhých.

Specifický je trestní zákoník, protože jen jeho porušení může vést k odnětí svobody, tedy vyšší sankci než v případě práva občanského, do kterého především spadají dále řešené zákony. Trestní zákoník zahrnuje v současnosti 421 paragrafů, z nichž mnoho může být využito při specifických situacích, kdy došlo ke zneužití digitálních stop. Jako příklady lze uvést: § 228 Poškození cizí věci (byl použit při

[125] Usnesení č. 2/1993 Sb.

prolomení přístupu k uživatelskému účtu v počítačové hře a jeho zneužití[126]) nebo § 354 Nebezpečné pronásledování (projev musí trvat min. 4-6 týdnů, pokud probíhá v elektronickém prostředí, je subjekt pronásledován právě s ohledem na s ním spojené digitální stopy, např. vydávání se za oběť, snaha poškodit reputaci oběti, opakované kontakty s upozorněním na známé informace o oběti). Jiným směrem využití trestního zákoníku je oblast činů proti majetku při zneužití počítačového systému, který upravují §§ 230-232. V těchto případech je trestný neoprávněný přístup k datům, ať už dojde k jejich zneužití nebo ne, je možné jej využít např. při procházení elektronického profilu ve službě, ze které se předchozí uživatel veřejného počítače zapomněl odhlásit. Naopak přihlašovací údaje jsou samy o sobě chráněny, a to jak na úrovni získání, tak i přechovávání, pokud je prokázán úmysl je využít. Poslední z této série činů je poškození dat nebo zásah do vybavení počítače z nedbalosti, ke kterému dojde v případě vzniku škody při výkonu funkce, povolání, postavení apod., což může být nedbalostní jednání knihovníka třeba při pomoci uživateli s problémem na počítači, resp. na internetu. Zásah i z nedbalosti v zastávané pozici je také v případě neoprávněného nakládání s osobními údaji (§ 180), které spočívá v neoprávněném osvojení, zpracování nebo zpřístupnění, příp. porušení mlčenlivosti o osobních údajích.

Podobně i občanský zákoník doplňuje průřezově mnoha zákonů. Z hlediska řešeného tématu stojí za zmínku § 2950 Škoda způsobená informací nebo radou: „*Kdo se hlásí jako příslušník určitého stavu nebo povolání k odbornému výkonu nebo jinak vystupuje jako odborník, nahradí škodu, způsobí-li ji neúplnou nebo nesprávnou informací nebo škodlivou radou danou za odměnu v záležitosti svého vědění nebo dovednosti. Jinak se hradí jen škoda, kterou někdo informací nebo radou způsobil vědomě.*“ Je diskutabilní, zda by knihovník (povolání) mohl být vnímán uživateli jako odborník v případě poskytnutí rady v oblasti informační bezpečnosti např. na semináři s dobrovolným účastnickým poplatkem, pokud uživatelé budou vnímat knihovnu jako instituci zprostředkovávající přístup k internetu a s tím související služby dle knihovního zákona, patří to tedy do základu jejich pracovní činnosti a tím i odbornosti, pak by to bylo možné. Nicméně se jedná o vyvratitelnou domněnku.

[126] Česká Televize 2013

Z dalších zákonů je pro digitální stopy prvořadý již zmiňovaný zákon č. 101/2000 Sb. Stanovuje ochranu při jakémkoli nakládání s osobními údaji mimo vymezené výjimky. Základní charakteristikou osobních údajů je dle § 4, písm. a) jejich schopnost identifikace konkrétní fyzické osoby (jednou informací nebo jejich souborem). 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). Tyto typy informací jsou proto chráněny tak, že za jejich neoprávněné shromažďování nebo zpracování libovolným způsobem (mimo výjimky, např. zpracování pro osobní potřebu fyzické osoby) může být udělena sankce. Jak již bylo uvedeno, Listina základních práv a svobod chrání šířeji vymezené informace, udělení sankce je ale problematické. Pokud tedy knihovna pracuje s digitálně uloženými osobními údaji, musí dodržovat povinnosti správce, resp. zpracovatele osobních údajů (např. získání souhlasu subjektu údajů, jeho informování o zpracování, skartace po uplynutí nezbytně nutné doby pro účel zpracování apod.). Subjektem údajů ale nemusí být jen aktuálně registrovaní uživatelé knihovny, ochrana osobních údajů se týká např. i v dobré víře sdílených nebo zveřejněných identifikačních údajů (vč. fotografie) osoby, která má vysokou pokutu za nevrácené výpůjčky nebo poškozovala fond knihovny. Pokud jsou osobní údaje zpracovávány digitálně, zákon stanovuje povinnost informační systém zabezpečit na různých úrovních proti možnosti zneužití, vč. neoprávněného přístupu. Zajištění tohoto typu digitálních stop je tedy na knihovně.

Lze navázat zákonem č. 480/2004 Sb., konkrétně jeho částí o službách informační společnosti, které jsou poskytovány na žádost, přičemž žádost i služba sama jsou řešeny elektronicky, slouží zejména pro vyhledávání a zpřístupňování informací. Může se jednat o různé typy služeb, kdy je na základě typu členěna odpovědnost poskytovatele služby. Konkrétně knihovna může takto být poskytovatelem různých rejstříků, např. s informacemi o výhercích soutěže, dětech, které vystavovaly svá díla, nebo třeba o autorech publikací. Může se ale jednat i o jiné digitální stopy než jen osobní údaje, které jsou však s ohledem na předchozí popsaný zákon nejvíce problematické a je možné přes ně nejsnáze být sankcionován. Z hlediska zákona o některých službách informační společnosti je poskytovatel služby odpovědný za obsah, pokud se dozvěděl o jeho protiprávnosti,

tj. např. když subjekt, kterého se dané informace týkají, upozorní, že si takové zpracování nepřeje, pak jejich další ponechání ve službě by bylo jejich přesunutí do položky nelegálního obsahu a postih by mohl následovat i z hlediska zákona o některých službách informační společnosti. Jak již bylo uvedeno, nejedná se jen o osobní údaje, problém může vzniknout u libovolného typu digitálních stop, pokud nějak došlo k porušení zákona a knihovna to zjistí.

Jak je patrné z posledního zákona, bylo by možné pokračovat v přehledu právních předpisů dál, ale jejich vztah k řešené problematice by byl slabší a právní přehled problematiky není předmětem této dizertační práce. Na závěr je ještě nutné poukázat na to, že i když zákonná úprava existuje, její role při ochraně digitálních stop 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 tento člověk musí vědět, že existuje právní úprava dané oblasti a že by ji překročil, nefunguje tedy bez určité osvěty. Současně ne pro každého je obava ze sankce dostatečná, aby jej odradila.

Pokud tedy právní úprava neodradí, může být využita při represi. I zde se objevují významné problémy. Prvním je působnost práva, která je ohraničena státními hranicemi a občanstvím (teritorialita[127]), což je na internetu snadné obejít, např. využitím elektronických služeb, jejichž poskytovatelé nemají pobočku v ČR, příp. využitím skrytím datovými přenosy přes různé státy, kdy není výjimečný problém v předávání informací. V mezinárodním prostředí sice existují snahy o harmonizaci práva, především v rámci Evropské unie k tomu dochází, problémy se ale objevují při jednání o dotčení suverenity států, která i navzdory k spojení v Unii musí být dodržena. Zásadní vliv má také délka a složitost vzniku a úprav právních aktů, který naprosto neodpovídá vývoji informačních technologií, proto je možné právní postih jen u omezeného množství internetových útoků. 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 zde zákona (Policie ČR[128], Úřad pro ochranu osobních údajů[129] atd.). Poškozený také vůbec nemusí vědět, že existuje právní úprava, která by mu pomohla a že tedy existuje

[127] Podrobněji např. NOVOTNÝ 1997; SMEJKAL 2001; MATĚJKA 2002
[128] Působnost dle zákona č. 273/2008 Sb.
[129] Působnost dle zákona č. 101/2000 Sb.

možný způsob 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 represe je zpětná aplikace, jelikož některé internetové útoky mohou způsobit nevratné následky, např. znásilnění nebo sebevraždu (viz kap. 2.2.2). Represe sice může pachatele postihnout, rozhodně to ale není možné považovat za dostačující řešení.

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 měly být jejich nevýhody zohledněny zavedením i dalších typů bezpečnostních opatření.

3.2 Technické zabezpečení

Na úrovni konkrétního zařízení, tedy méně plošně dopadající opatření než legislativa, ale stále zasahující více uživatelů počítače[130], je možné využít technických řešení. Právě na ta se dříve informační bezpečnost omezovala[131], s rozšiřováním sociálních hrozeb založených na komunikaci (např. kyberšikana) je ale evidentní, že technická řešení jsou jen jedním z prvků bezpečnostních opatření (viz kap. 2). Vzhledem k tomu, že umožňují určitým problémům předcházet automatizovaně při shodném použití různých nástrojů, je nutné jim věnovat odpovídající pozornost, ale neomezovat se na ně.

Z hlediska technických řešení pro bezpečnost digitálních stop v knihovnách je nutné uvažovat dvě základní úrovně: síťovou, pokud je v knihovně více než jeden počítač, a koncové stanice. Oblast zabezpečení na úrovni sítě nebude podrobněji rozebírán, protože překračuje úroveň odbornosti, kterou lze očekávat u knihovníka, v ní bude potřebovat odborníka, správce sítě, pokud mají být opatření sofistikovanější. Knihovník by nicméně měl mít představu o možnostech, které v tomto směru existují, byť by je nedokázal vysvětlit do hlubších podrobností nebo sám aplikovat. Měl by ale být schopný vysvětlit uživateli, že tato opatření v knihovně jsou a jak jej ochrání. Naopak o bezpečnosti koncové stanice by měl

[130] Využíváno v širším slova smyslu, tj. stolní, přenosný (vč. tabletů) i kapesní (hl. smartphony)
[131] Viz např. POTÁČEK 2003-

mít pokročilejší znalosti, které mu umožní jednoduchá řešení případných problémů a odpovídají řešení i na úrovni běžného domácího počítače. Je zde tedy výrazně vyšší pravděpodobnost nutnosti poradenství i protnutí tématu při vzdělávání nejen o informační bezpečnosti, ale o jakékoli práci s IT, protože k ní bezpečnostní prvek patří. Samotné zařízení umožňuje bezpečnostní opatření, která je možné rozdělit do tří kategorií: operační systém a webový prohlížeč jako základní software pro ovládání počítače, příp. internetu, software a online nástroje využívané pro elektronickou aktivitu, tedy ne primárně pro zajištění bezpečnosti. Třetí kategorií jsou právě nástroje a software specializované na zabezpečení počítače.

U operačního systému záleží na jeho charakteristikách, vývoji a bezpečnostní politice. V tradičnějším prostředí (stolní počítače a notebooky) je stále silně převažující rozšíření systémů Windows, nejčastěji ve verzi 7[132], v mobilním prostředí se v roce 2013 nejvíce prodávala zařízení s Androidem (78,4 %) a iOS (15,6 %)[133]. Tato tři prostředí se liší již svojí podstatou a umožňují i potřebují odlišná řešení. Přesto je možné vymezit alespoň základní úroveň bezpečnostních pravidel, 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 ihned jak je to možné ošetřeny zjištěné slabiny v informačních systémech. Řešení je možné provádět vždy v každém softwaru, ale především v síťovém prostředí je vhodné uvažovat o tzv. Patch managementu, tedy právě řízení aktualizací, updatů a upgradů, kdy je možné využít zvláštní nástroje[134], které provedou potřebný postup na všech zařízeních v síti, umožňují také testovat systémy po instalaci nebo vést dokumentaci. Z hlediska digitálních stop aktualizace brání jejich neoprávněnému získání i zneužití přes známou a popsanou zranitelnost, na kterou existuje řešení.

Dalším krokem je využití autorizace (stanovení oprávnění) a odpovědná práce s ní. V prostředí Windows se jedná především o uživatelské účty, které by měly být přiděleny vždy jednomu uživateli s tím, že nastavená oprávnění by měla odpovídat znalostem uživatele. Uživatelské účty jsou použitelné i v prostředí

[132] Windows 8 ztratily podíl na trhu 2014
[133] Gartner Says Annual Smartphone Sales Surpassed (…) 2014
[134] Např. RingMaster's Automated Patch Management nebo Lumension® Patch and Remediation

Android od verze 4.2 Jelly Bean[135]. Na jiné úrovni autorizace odpovídá udělení oprávnění aplikaci, která 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 také autentizace (prokázání identity), která je podstatná nejen u operačních systémů. V jejich případě je autentizace využívána obvykle 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 přejít do režimu vyžadujícího heslo a také mít nastavený co nejkratší (ale neztěžující použití) interval přechodu při zapomenutí manuálního nastavení. Autentizace se typicky provádí pomocí hesla. Tradiční hesla jsou textová. Pro ně jsou poměrně známá pravidla, aby heslo bylo možné považovat za dostatečně silné, jsou v oblasti použitých znaků, délky i práce s ním, např. pravidelná změna po určitém období[136]. Mnohá pravidla jsou ale přenositelná i na jiné typy hesel, především v mobilním prostředí se prosazující 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[137], tedy jejich neoprávněné zjištění pozorováním při zadávání. Existují i další postupy autentizace, někdy kategorizované podle toho, čím je totožnost prokazována[138]: znalostí (právě popsaná hesla), vlastnictvím (např. mobilní telefon při SMS s kódem, který je nutné zadat), bytím (*something you are*, tj. biometrické ověření, dnes ne nedostupné, především otisk prstu nebo rozpoznání tváře), příp. ještě činností (např. behaviorální analýza typického jednání na počítači) a přiřazeným (typicky jméno a příjmení, které bylo přiděleno externím subjektem bez ohledu na samotného uživatele). Základem funkčnosti autentizace je nejen vhodná iniciace, tj. bezpečný postup ověření, ale také ukončení činnosti s danou identitou, tedy důsledné odhlašování od všech služeb. Hesla ale jsou využívána i na vyšší úrovni

[135] Jelly Bean 4.2 [2012]
[136] Podrobné vymezení pravidel pro silná hesla a jejich užívání, vč. tipů pro praktické vyvážení použitelnosti a bezpečnosti uvádí BOTT 2004, s. 111-123
[137] POŽÁR 2005, s. 119
[138] NIXON 2010, s. 154

než konkrétní služby, především v bezdrátových sítích je zásadní udržení bezpečnosti hesel, protože cizí připojený počítač v síti může mít přístup k přenášeným datům[139]. Protože knihovny nabízí přístup k internetu i prostřednictvím Wi-Fi bez hesla, měly by být uživatelem zvažovány informace přenášené tímto způsobem.

Dalším klíčovým softwarem z hlediska digitálních stop v knihovně je webový prohlížeč. Data, která ukládá do počítače bez použití internetu, si může uživatel poměrně dobře uvědomovat. Ale internet i samotný prohlížeč ukládají množství dat tak, že si toho uživatel nemusí ani všimnout. Použití internetových služeb může vést k přesvědčení, že vše je v internetu, ať je služba ovládána z libovolného počítače a nezáleží tedy na tom, jak je technicky vyřešena bezpečnost v knihovně. Podobně jako operační systémy, i prohlížeče se poměrně liší, a to i na úrovni možností nastavení pro zvýšení bezpečnosti. Vhodné je proto v nainstalovaných prohlížečích zvážit různé možnosti a pokusit se o nastavení, které by v první řadě neomezovalo výrazněji možnosti práce s internetem (tj. příliš striktní), ale současně zajistilo co nejvyšší bezpečnost. V oblasti digitálních stop se jedná především o sekci soukromí, kde je možnost práce s Cookies, které fungují právě na principu digitálních stop, ovšem jejich zakázání v podstatě znemožňuje práci s internetovými službami (mnoho jich funguje na personalizované úrovni, která při zákazu Cookies není realizovatelná), dále je zde možnost smazání různých digitálních stop, např. historie prohlížení, uložená uživatelská jména a hesla, příp. našeptávače (dokončování formulářů). Cookies 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[140]. Protože některé společnosti se rozhodly vyjít vstříc zákazníkům s nabídkou tzv. opt-in přístupu v oblasti Cookies (uživatel není sledován, pokud se nerozhodne jinak), může zde být právě možnost nastavení informace pro servery, zda uživatel prohlížeče chce či nechce být sledován.

Někteří uživatelé neberou ohled na vznik digitálních stop přes prohlížeč, příp. omylem vytvoří stopu, kterou pravděpodobně nechtěli (např. nepřečtením varování), nemažou data, která se v počítači ukládají, např. ve stažených souborech, atp., je proto vhodné podpořit zabezpečení digitálních stop v tomto směru ze strany

[139] SALTZMAN 2008, s. E. 14
[140] BOTT 2004, s. 42

knihovny. Možná a pracná je manuální správa takto vzniklých dat, existují ale také automatizovaná řešení, např. obnovení počítače při každém startu do výchozího nastavení, vč. uložených dat. Zůstává problém, že stopa může být dostupná mnoha lidem od rána do druhého dne, kdy je odstraněna. Jinou možností je využívání již popsaných uživatelských účtů, kdy se data ukládají jen do datového prostoru dostupného výhradně oprávněnému uživateli.

Pro doplnění bezpečnosti slouží aplikace typu antimalware, firewall, antispam, filtr obsahu, antiphishingový nástroj nebo anonymizér. Existují i sofistikovanější řešení, která jsou ale finančně a na údržbu náročná, proto jim pro knihovny není nutné věnovat větší pozornost. I v případě jmenovaných nástrojů je vhodné uvést, že všechny mohou (a měly by) fungovat jak na úrovni vstupu do sítě (perimetr), tak i na všech koncových stanicích. Z hlediska digitálních stop jsou podstatné především antimalwary, které jsou běžně označovány antiviry, ale zahrnují také specializované antispywary a antirootkity, přestože i tyto typy malwaru (škodlivého softwaru) mohou spyware a rootkit identifikovat, kvůli širšímu zaměření ale v tom nejsou tak úspěšné. Protože spyware sleduje uživatele, vytváří nebo shromažďuje o něm digitální stopy a následně je zasílá na stanovené místo, je z hlediska tématu této práce nejvýznamnější z antimalwarů. Mezi spyware patří také keyloggery, které podle Gemerské knižnice Pavla Dobšinckého již byly pokusy v knihovně nainstalovat, stejně jako pokusy vypnout antivir[141]. Proti tomu firewall oddělující chráněnou a nechráněnou část sítě (ne vždy internet, mohou to být právě veřejné počítače) může pomoci při zjištění odesílaných informací, nebo naopak při jejich přijímání, pokud jsou vyhodnoceny jako nevhodné. Pomáhá také k zjištění skenování portů a při řešení otevřenosti nevhodných. Antispam, stejně jako filtry obsahu a antiphishingové nástroje pomáhají nepřímo s digitálními stopami, ale až v případě jejich zneužití.

Vhodné je využívat šifrování. To může být aplikováno na různých úrovních. Základem by mělo být využití šifrovaného protokolu, kde je to možné (SSL/TLS[142] využitý např. v komunikaci se servery pomocí HTTPS protokolu). Šifrování je ale vhodné použít také na úrovni uložených dat (souborů, složek, harddisků atd.), především pokud jsou ukládána v Cloudu. Další z možných oblastí šifrování může

[141] E-mailová komunikace přes elektronickou konferenci Andersen ze dne 1. 4. 2014
[142] CHANDRA 2009, s. 252

být komunikace, např. pro šifrování e-mailů lze použít software PGP, příp. v jiné formě jsou šifrovací algoritmy využívány v elektronickém podpisu, který neslouží pro ochranu důvěrnosti (podepsanou nezašifrovanou zprávu si může přečíst kdokoli, kdo k ní získá přístup), ale zajistí kontrolu integrity, identifikaci a autentizaci podepisujícího a nepopiratelnost.

Vedle těchto spíše šířeji využitelných nástrojů existují i takové, které jsou zaměřeny sice na dílčí, ale specifické problémy s digitálními stopami. Jak již bylo uvedeno, žádné technické opatření neznemožní uživateli vytvářet digitální stopy zpřístupněním informace v elektronickém prostředí, např. při komunikaci. Pomůcky v oblasti prevence vzniku digitálních stop proto jsou spíše na úrovni komunikace počítače se serverem.

Pro tuto práci jsou zásadním nástrojem anonymizéry sloužící k omezení sdělování informací při pohybu na internetu. Jedná se o informace o používaném zařízení, anonymizéry nepomohou s těmi, které uživatel na internetu zveřejňuje, proto i je nutné doplnit je vhodným chováním. Anonymizační nástroje fungují na různých úrovních, kdy výraznější rozdíly lze najít při vymezení tří přístupů: anonymní mód v prohlížeči, proxy-anonymizér a Onion routing. Anonymní mód v prohlížeči je vhodné použít na veřejných počítačích, umožňuje bez omezení využívat internetu, vč. přihlašování, vracení se mezi stránkami apod., ale po zavření okna prohlížeče jsou všechny informace uložené v prohlížeči smazány (nesmazány zůstávají stažené soubory). Toto řešení nicméně nemění situaci vůči druhé straně, např. webová stránka, kterou uživatel navštíví, zjistí totožné informace, jako kdyby byl použit neanonymní mód prohlížeče. Druhá jmenovaná úroveň je výhodnější, staví mezi zařízení uživatele a druhou stranu komunikace přes internet proxy server, který část údajů o uživatelem použitém počítači nahradí vlastními, čímž uživatele skryje, ale ne výjimečně jen z části. Další úrovní je Onion routing, který využívá většího množství proxy serverů, čímž by mělo dojít k úplnému skrytí uživatele[143]. Primárně slouží ke skrytí údajů o zařízení uživatele, také pomáhají k ochraně před sledováním navštívených webových stránek, které nezjistí ani poskytovatel připojení k internetu. Nevýhodou tohoto postupu je ale zpomalení připojení k internetu vlivem čekání na přenosu z nejpomalejšího zařízení v stanoveném řetězu

[143] HUSSAIN 2012

proxy serverů. Nejznámějšími[144] z těchto služeb jsou TOR a JonDonym (jinak také Java Anon Proxy nebo JAP), které ukazují, že i zde mohou být různé přístupy. TOR využívá jako proxy servery počítače různých lidí, kteří se k tomuto využití nabídli[145], ne všichni ale se zcela dobrými úmysly, může se tedy objevit proxy server, který naopak informace ukládá. Proti tomu JonDonym sice není tak robustní a rozšířený, uvedenému riziku se snaží předcházet ve spolupráci s univerzitami[146].

V oblasti legálního plošného shromažďování informací o uživateli dominuje oblast reklamy. Vzhledem k rozšíření různých typů cílené reklamy a možností státu a současně zájmu firem, které reklamu provozují, působit na zákazníky pozitivně, vznikly iniciativy především v angloamerickém prostředí (USA, konkrétně Federal Trade Commision, a Velká Británie), které vedly k vytvoření možnosti oznámit, že uživatel nechce, aby byl sledován, a daný server to bude respektovat. Ve Velké Británii má výsledek podobu zákona[147], který byl rozvedený průvodcem[148] vydaným pověřenou dozorovou institucí. Podle nich je mj. vyžadováno, aby server získal aktivně projevený souhlas se sledováním pomocí Cookies, při návštěvě stránky, která tedy chce Cookies uživateli uložit, je proto obvykle zobrazena o tomto informace, kdy uživatel musí souhlas vyjádřit zakliknutím. Jedná se tedy o aplikaci principu opt-in, tedy možnosti být zařazen do sledování, což odpovídá evropské směrnici 2009/136/ES[149], která ale navzdory stanoveným lhůtám ještě nebyla přenesena plnohodnotně do českého prostředí.

Proti tomu Federal Trade Commision iniciovala možnost aplikace opačného principu, tj. opt-out, tedy informování serveru o tom, že uživatel nechce být sledován[150]. To je uskutečněno pomocí projektu Do not Track, kdy je informace pro server umístěna v HTTP hlavičce při komunikaci. Respektovat toto přání se podle projektu zavázalo mnoho reklamních skupin, ale skutečnost ukázala, že tyto sliby nebyly příliš zohledněny v praxi[151]. Ukazuje se, že přestože se jedná o zajímavou myšlenku, bez opory ze strany státu a právních aktů nebude příliš funkční. Přesto inspirovala vznik více podobných iniciativ, ke kterým se ale

[144] JonDonym, AN.ON and Tor [b.r.]
[145] Tor: Overview [b.r.]
[146] Benefits of JonDonym [b.r.]
[147] Velká Británie 2011
[148] Electronic Communications Regulations 2012
[149] Směrnice Evropského parlamentu a Rady 2009/136/ES
[150] Federal Trade Commission Decision and Order 2011
[151] Overview [b.r.]

přihlásilo méně reklamních organizací, např. Network Advertising Initiative, About Ads, Your Online Choices, Privacy Choice (TrackerBlock).

Jiný přístup volí další typ produktů, které identifikují sledovací nástroje na webu, se kterým počítač aktuálně komunikuje, přičemž uživateli nabídnou seznam těchto sledovacích prvků pro volbu, které chce povolit a které blokovat napříč různými stránkami. V seznamu může být kromě prosté identifikace zařízení také informace o společnosti, na kterou se váže, informace o typu zjišťovaných dat, o možnosti sdílení se třetími stranami a délce uchování sledovaných dat. Zástupcem této kategorie je Ghostery, který také nabízí funkci odstranění Flash a Silverlight Cookies[152], se kterými mají některé nástroje problém.

Využití digitálních stop z vyhledávání mohou omezit falešné dotazy zasílané do vyhledavače pomocí zvláštního nástroje. Zástupcem této oblasti je TrackMeNot, který ve stanovených intervalech zasílá nahodile vytvořené dotazy do vybraných vyhledavačů a tím znehodnocuje vypovídací hodnotu takto shromážděných digitálních stop. Jednodušší variantou je použití stejného vyhledavače více lidmi s různými charakteristikami (při personalizaci, např. v Google, s bezpečnostním rizikem přihlášení různých uživatelů pod stejným účtem). Jiným přístupem k ochraně digitálních stop ve vyhledavači je využití proxy serveru vůči vyhledavačům, který může být plnohodnotný nebo jen službou pro tento účel, např. Random Search Engine.

Pokud digitální stopa vznikne, pro automatizaci a zjednodušení základního vyhledávání informací o vlastní osobě (viz kap. 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 částí 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 kap. 2.1). Jinou kategorii zjištění existující digitální stopy zastupuje možnost stažení kopie dat z Facebooku (od roku 2010). Zásluhu o vznik této možnost 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,

[152] Live! Ghostery V.2.1 for Firefox 2010

jaké informace o něm shromažďuje[153]. Přesto existují dohady, že rozsáhlý seznam informací[154] neobsahuje všechny zpracovávané Facebookem[155].

Při správě počítače je možné využít nástroje, které usnadní jejich odstranění tak, že není nutné procházet manuálně všechna klíčová úložiště, ale lze je vyprázdnit najednou. 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[156], 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 and LinkedIn[157]. Problém může být v tom, že pro splnění své funkce nezbytně vyžaduje zadání přístupových údajů do služeb pro úpravu v nich uložených digitálních stop.

Z uvedeného přehledu je patrné, že sice existují technické pomůcky pro bezpečnostní řešení digitálních stop, jejich funkce jsou ale omezené a specializované. Využití různých přístupů pro zvýšení bezpečnosti by bylo pro běžné užití složité. Je proto vhodné vybrané dle potřeb uživatele využít, ale primárně usilovat o bezpečné chování pro prevenci vzniku digitálních stop, protože možnosti zpětného řešení jsou výrazně složitější.

Tento přehled různých směrů, ve kterých je možné aplikovat technická řešení pro zvýšení bezpečnosti uživatele v knihovně, ukazuje, že možností je mnoho. Problémem u všech zůstává, že je možné je obejít, pokud ne v daném okamžiku, tak při zvýšení výkonu počítače (např. problém délky klíčů při šifrování) nebo zjištění nečekaného problému (objevení zranitelnosti v informačním systému). Obejít ho se ale může pokusit také uživatel, kterého má chránit, např. dostupné jsou návody na překonání blokování Facebooku ve škole[158]. K tomu může dojít, pokud jeho chování nevyužívá produktů technických opatření, např. nečte varování zobrazená bezpečnostní aplikací, nebo pokud si není vědom toho, že hrozba, proti které je řešení postaveno, je vyšší než pozitiva, která z jeho překonání

[153] SOLON 2012
[154] Viz Přístup k osobním údajům na Facebooku 2014
[155] Get your Data! [b.r.]
[156] MOORE 2012
[157] Web 2.0 suicide machine [b.r.]
[158] XNOTION 2010

plynou. I technická prevence, podobně jako právní, je tedy nutně spojena s osvětou, aby mohla být efektivní. Podle Herrington[159] je také přínosnější než přísná restrikce pomocí bezpečnostních nástrojů, které omezují svobodný přístup k informacím, i těm opravdu hodnotným.

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. Proto je vhodné uvažovat také nad bezpečností na nižší úrovni než zařízení, tj. u uživatele, kterých se může i jednoho počítače střídat mnoho. Podstatné pro tuto práci je vymezení, jak a proč by se měla promítat do prostředí knihovny a nezůstávat pouze na úrovni vlastního rozhodnutí uživatele.

Jak již bylo uvedeno, knihovna pracuje s digitálními stopami svých uživatelů. Je proto zásadní i z hlediska dodržení zákona o ochraně osobních údajů, aby sami knihovníci dodržovali pravidla bezpečného chování a nekompromitovali uživatele třeba i neúmyslným prozrazením. Nejedná se jen o údaje o osobě registrovaného uživatele, zásadní informací je také jeho čtenářská historie, která představuje citlivý osobní údaj[160]. V zásadě stejným typem informací je tedy také historie při použití internetu ve smyslu historie v prohlížeči a stažených souborech, které ale nejsou explicitně určeny jako chráněné. I v rámci udržení etiky přístupu a důvěryhodnosti knihovny by měly být tyto informace uvažovány jako podstatné pro ochranu. Z toho vyplývá, že pro ochranu uživatele počítače v knihovně je zásadní také úroveň bezpečného chování pracovníka knihovny.

Pro podporu bezpečného chování samotných uživatelů knihovna často využívá stanovení pravidel v knihovním řádu[161], kde je možné uvést i pravidla bezpečného chování uživatele na internetu, která využitím počítače v knihovně uživatel akceptuje. Je ale otázkou, zda si je toho vědom, tedy zda si knihovní řád

[159] HERRINGTON 2010, s. 10
[160] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2002 2009
[161] Např. Vzorový knihovní řád Knihovnického institutu Národní knihovny ČR (Vzorový knihovní řád, 2014), který je sice i přes aktualizaci 19. 7. 2014 v oblasti práce s IT zastaralý (viz použití disket pro ukládání informací v čl. 8, odst. 4), ale slouží jako vodítko pro prvky, které jsou při přizpůsobení knihovního řádu v jednotlivých knihovnách zvažovány.

přečetl a pochopil jeho obsah. Protože se jedná o právní dokument, který především dětem může být nepřístupný (ve smyslu reálného seznámení se s obsahem na úrovni pochopení). Přesto pro určitou část uživatelů knihovny, kteří se s knihovním řádem seznamují, se může jednat o kanál sdělující pravidla bezpečného chování lidem, kteří využívají různých služeb knihovny, může tedy zasáhnout jako osvěta části uživatelů. Kromě knihovního řádu mohou bezpečnostní doporučení v oblasti digitálních stop být distribuovány v knihovně dalšími způsoby, např. zobrazení na monitoru v podobě spořiče obrazovky nebo na ploše, může být vyžadováno potvrzení seznámení se s nimi před spuštěním webového prohlížeče, mohou být uloženy na nástěnce (např. nad počítačem) nebo na stole ve formě letáků apod.

Jinou možností, jak se knihovna může zapojit do podpory bezpečného chování uživatelů na jejích počítačích, je vzdělávání nebo poradenství v informační bezpečnosti, příp. digitálních stop (viz kap. 4.3). Pokud nebude využito osvěty, je potřebným minimem upozornění knihovny na specifika veřejných počítačů, které nabízí. Ty mohou být známé, je ale potřebné podpořit uvědomění si těchto specifik v praktickém využití. Mezi ně patří výrazně vyšší dostupnost digitálních stop, jejichž vznik či odstranění by tedy měl uživatel více řešit než v případě domácího počítače. Odstranění důležitých informací by mělo být podle Saltzmana[162] i na úrovni paměti RAM restartováním počítače, což ale ne všechny knihovny svým uživatelům umožňují. Počítač v knihovně také může být kompromitován fyzickým útokem nebo přes zranitelnost, kdy je zajímavějším cílem, než domácí počítač, protože útok vede k více obětem, které se na počítači v knihovně střídají. O to podstatnější je chování uživatele v oblasti digitálních stop na počítačích v knihovně.

Chování představuje základní přístup k bezpečnosti digitálních stop. Jejich spojení s konkrétní osobou totiž odpovídá řešení opět na úrovni osoby, což je primárně přenositelné napříč použitými zařízeními jen chováním, protože podstatné je, jak je využívá. Toto využití je až na výjimky samostatné, u uživatele není přítomen nikdo, kdo by jej v klíčovém okamžiku varoval, to závisí jen na znalostech, dovednostech, postojích a zkušenostech samotného uživatele. Proto by každý uživatel internetu, při použití měl znát základní pravidla bezpečného chování na internetu a ideálně o nich šířit povědomí k lidem, kteří je nedodržují. Lektoři, učitelé a knihovníci o to více a intenzívněji.

[162] SALTZMAN 2008, s. E. 14

Zranitelnosti a jejich omezování uživatelem vychází z jeho chování v elektronickém prostředí. Vzhledem k trendům vývoje internetu význam chování uživatele roste. Ukázkou je např. princip Webu 2.0, který staví na příspěvcích běžných uživatelů do služby, tj. jejich vytváření digitálních stop, jiným trendem, který je s nimi spojený, je rozšiřování personalizace mnoha služeb vzhledem k tomu, že jejich cílenost je výhodná jak pro uživatele, tak i pro provozovatele služby, jak již bylo řešeno v kap. 2.2.1. Vznik mnoha digitálních stop, které jsou snadno využitelné různými typy třetích stran vzhledem k jejich dostupnosti i jasné vypovídací hodnotě, je dán právě chováním uživatelů. Je evidentní, že mnohem více subjektů dokáže najít uplatnění pro informaci o člověku zveřejněnou na sociální síti než pro verzi webového prohlížeče. Současně technická řešení často slouží jako bariéra, kterou musí uživatel potvrdit, např. webový prohlížeč může zobrazit varování pro uživatele, že SSL certifikát je nedůvěryhodný, je ale na rozhodnutí uživatele, jak na toto varování bude reagovat svým chováním.

Jak bylo právě popsáno, nejsnáze využitelné digitální stopy představují informace, které o sobě nebo o jiném uživatel prozradí. Jejich kategorizace podle využitelnosti, a tím zájmu třetích stran je popsána v kap. 2. Právě úroveň využití, resp. zneužití, by měla odpovídat tomu, jak je uživatel opatrný při zařazení informace do digitální stopy. Obecně lze konstatovat, že bezpečné chování je jen přemýšlení nad možnými důsledky chování a zvážení těch pro uživatele pozitivních a negativních s tím, že výsledné jednání bude odpovídat tomu, jaká kategorie by převažovala. Pokud by totiž vytvoření stejné digitální stopy mělo mít za následek jen nevýznamný přínos pro uživatele, měl by z něj ustoupit. Naopak pokud je pro něj klíčový, měl by vědomě rozhodnout, že je ochotný přistoupit na riziko, že tato digitální stopa bude využita způsobem, který mu nebude příjemný. Toto rozhodování staví na stejných základech jako tzv. risk management[163], který je aplikován v sofistikovanějších řešeních informační bezpečnosti než osobní úroveň. V rámci tohoto přemýšlení se často 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.

[163] POŽÁR 2005, s. 42-43

Pro konkrétnější vymezení vhodného chování pro ochranu digitálních stop je vhodné uvažovat jak na úrovni prevence vzniku digitální stopy, tak úpravě či smazání již existující. První ze jmenovaných přístupů je podstatný proto, že již jednou vytvořená digitální stopa může být mimo dostupnost pro člověka, o kterém vypovídá, informace může být uložena na různých místech, o kterých uživatel neví[164]. I firmy specializované na odstranění digitálních stop se sjednanými dohodami s různými subjekty garantují jen omezené množství vyřešených stop (např. firma ReputationDefender stanovuje tuto hodnotu na 80-90 %[165]). Může se pak objevovat opakovaně i po dlouhé době. Na druhou stranu i při nejlepším chování člověka z hlediska vzniku digitálních stop může nastat problém tím, že informaci o něm vytvoří někdo jiný. Za určitých okolností je tedy možné alespoň omezit potenciál využití digitální stopy tím, že je řešena ta, která je dobře dostupná a tedy i sám člověk, o kterém vypovídá, o ní ví.

Při prevenci vzniku digitální stopy je podstatné omezovat sdělování kontaktních údajů. Ty samy patří mezi snadno využitelné informace, ale mohou také sloužit pro propojování informací z různých zdrojů, protože tyto kontakty jsou obvykle 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 informačního kanálu stačí jméno, příp. přezdívka, je i tento údaj samotný možné považovat za kontaktní. Přezdívka je také velmi problematickou informací z hlediska digitálních stop, protože si ji často člověk přenáší do různých služeb, proto opět dobře slouží k propojování různých informačních zdrojů o člověku. K propojování informací jsou také často využívány fotografie nebo videa, která umožňují dobře rozlišovat mezi jmenovci, slouží tedy k omezení nesprávného propojení zdrojů digitálních stop. Toto odpovídá kategorizacím digitálních stop dle možností zneužití, které byly popsány v kap. 2, síla omezování sdělování dalších informací by měla odpovídat právě těmto možnostem. Vzhledem k možnosti kompromitace služby (nejen nechtěné využití po oprávněném přístupu) je vhodné sdělovat co nejméně všech osobních informaci, a to i v registračních formulářích.

[164] GRAYSON 2011, s. 8
[165] MARTÍNEZ-CABRERA 2010

Zvažovány by měly být samy 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, příp. nedůvěryhodný, kdy informace poskytne třetí straně či s nimi sám nezachází eticky. Na úrovni e-shopů lze pro hodnocení důvěryhodnosti využít různých typů certifikátů, především nejrozšířenější APEK[166]. V případě obchodní transakce typu Consumer-to-Consumer, např. v elektronické aukci, je vhodné využít zprostředkovatelem nastavených reputačních mechanismů jednotlivých prodejců a nakupujících[167].

Dalším typem bezpečného chování je budování pozitivní digitální stopy[168]. Je nereálné v současnosti nemít digitální stopu, spíše je otázkou, co vypovídá o člověku. Tím se jako zásadní postup při budování digitální stopy stává již uvedené přemýšlení nad důsledky, v tomto případě využití dostupných informací. Ty mohou sloužit jak k prezentování schopností člověka, např. vůči možnému zaměstnavateli, tak i k informačnímu útoku nebo jen k prezentaci člověka způsobem, který jej negativně ovlivní (např. pokud možný zaměstnavatel uvidí fotky daného člověka v situaci dokumentující jeho nevhodné chování z pohledu zaměstnavatele). Proto je dobré přemýšlet nejen nad obsahem informace, než se z ní stane digitální stopa, ale také její možný vliv na člověka, kterého se týká, při jejím využití různými subjekty. Např. fotka z oslavy může mít vliv ze strany přátel (pozitivní ukázka společenského charakteru daného člověka a zábavy s ním), tak i ze strany zaměstnavatele (pokud úroveň zábavy převyšuje úroveň, kterou považuje za vhodnou) nebo útočníka (možnost vydírání jak obsahem fotky, tak i třeba jejím zneužitím při fotomontáži a následném poskytnutí další osobě ve vztahu k zobrazenému člověku).

Digitální stopa může vznikat i při útoku, kdy je poskytována informace osobě, která ji pak zneužije. Tento problém není nijak výjimečný, jedná se o situace, kdy je využito tzv. sociálního inženýrství, kterému již byla věnována pozornost v kap. 2.2.2. Pro ochranu proti němu je vhodné ověřování si oprávněnost jakéhokoli požadavku na poskytnutí informace, nejlépe ne elektronicky, aby nedošlo k tomu, že pro ověření bude využit podvržený informační zdroj, s čímž také souvisí to, že by neměly být využívány odkazy ve zprávách, ale postup přes známé oficiální

[166] Certifikáty a ocenění e-shopů [b.r.]
[167] Např. Aukro nápověda [b.r.]
[168] GRAYSON 2011

kanály. Při ověřování či komunikaci se subjektem, který danou informaci žádá, je vhodné navrhovat alternativní řešení, všímat si podrobností a usilovat o vedení rozhovoru tak, aby byly případně identifikovány nepřesnosti při komunikaci v oblasti, na kterou se sociotechnik nemohl dopředu připravit[169]. Protože sociální inženýrství často využívá nátlak přes různé emoce, je vhodné si toto uvědomovat a zpozornět v situacích, kdy by právě emoce mohly vést k rizikovému jednání.

Chování uživatele pro ochranu digitálních stop je navázáno také na vhodnou práci s bezpečnostními prvky, které vycházejí z funkčnosti technických opatření. To znamená, že na technické úrovni při využití vznikají různé varovné signály, na které by měl člověk správně reagovat. Jejich funkce je tedy informační, varovná, může se ale stát, že se jedná o falešně pozitivní oznámení, proto je rozhodnutí dalšího postupu ponecháno uživateli. Navzdory nepohodlnosti pro uživatele je pro zvýšení jeho bezpečnosti vhodné číst různé certifikáty, licenční podmínky, varování, potvrzení apod. Nicméně především licenční podmínky vzhledem k jejich často mnohastránkovému obsahu, i když se jedná o službu využívanou dětmi (např. Facebook), slouží spíše pro právní ochranu poskytovatele služby než pro ochranu uživatele, není možné očekávat, že budou číst celé dokumenty ve všech používaných službách.

Další opatření v nastavení elektronické služby vychází z oprávnění práce s digitálními stopami, které mohou být dostupné jen po ověření identity a odpovídající autorizaci. Je proto zásadní práce s autentizačními údaji, kterým se podrobněji věnuje kap. 3.2. Nutné je poznamenat, že chování při nastavení softwaru a internetových služeb závisí i na úrovni porozumění, což je podle O'Neilla[170] důvod vzniku problému, že třetina uživatelů sociálních sítí neví, jak zde změnit nastavení soukromí. Na úrovni dospělých uživatelů sociálních sítí 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 více než 65 let), současně ale polovina z nich měla určité problémy při řízení nastavení soukromí[171]. Při nastavení soukromí je ovšem nutné následně přemýšlet nad udělováním autorizace s vyšším přístupem k informacím, typicky přidáváním mezi kontakty (např. přátel na sociální síti Facebook) jen osob známých z fyzického prostředí.

[169] MITNICK 2003
[170] O'NEILL 2012
[171] MADDEN 2012

Představené základní principy v oblasti prevence vzniku digitálních stop jsou dlouhodobě a obecně platné, ale samozřejmě existují další možnosti vázané na konkrétní situaci (např. bezpečné chování na sociální síti Facebook v mobilním prostředí se současnými možnostmi nastavení, které je nutné v chování reflektovat). Vzhledem k cíli a rozsahu této práce jim ale nebude dále věnována pozornost. Při vzdělávání o bezpečnosti digitálních stop, které je podstatou této práce, je klíčové právě přibližování problematiky pomocí konkrétnějších situací s ohledem na její rychlý vývoj.

Pokud digitální stopa vznikla, existují určité možnosti řešení. Je ale nutné o tomto vzniku vědět, protože, jak již bylo opakovaně uvedeno, ne všechny digitální stopy člověk o sobě vytváří sám. Při zjišťování existence digitálních stop je nejsnazším postupem jejich vyhledávání v konkrétní službě nebo pomocí internetových vyhledávačů. Tento postup je označován jako egosurfing[172] a především v USA se jedná o často aplikované bezpečnostní opatření[173]. Ten by měl být využíván pravidelně, a to ve vyhledávačích i v sociálních médiích, kde je jednodušší řešení, protože je možné požádat známého o odstranění digitální stopy, kterou vytvořit a která je člověku, o kterém vypovídá, nepříjemná. Pokud digitální stopu vytvořila třetí strana, ke které člověk nemá užší vztah, např. organizátor soutěže, které se zúčastnil, nebo firma, od které si něco koupil, je možné i jeho požádat o smazání této informace. Pokud není možné kontaktovat přímo osobu zodpovědnou za zveřejnění, např. v příspěvku v diskuzním fóru, lze využít oprávnění správce dané služby odstranit tuto informaci. V obou případech by mělo být požadavku vyhověno podle zákona o ochraně osobních údajů i podle směrnice Evropského parlamentu a Rady 95/46/ES. Z rozsudku Soudního dvora[174] (velkého senátu) Evropské unie, vyplývá, že o smazání je možné požádat také internetový vyhledavač, který dané informace neobsahuje přímo, ale indexuje je, zobrazuje ve vyhledávání a umožňuje k nim přístup. V případě, že digitální stopa vznikla působením subjektu, který má tuto činnost danou ze zákona, je nutné se s tímto smířit a být si nadále vědom, že tato informace je dostupná a podle toho by s ní mělo být nakládáno (např. nevyužívat ji jako heslo).

[172] Egosurf © 2014
[173] Egosurfing někdy využito 47 % dospělých Američanů, z nich 25 % opakovaně. Viz MADDEN 2007, s. 7
[174] Rozsudek Soudního dvora (velkého senátu) ze 13. května 2014

Když dojde k odstranění digitální stopy, je vhodné mít jistotu, že byla smazána. V případě výše jmenovaných postupů týkajících se třetích stran jistota nikdy nebude úplná, ale je nutné uvažovat i znalosti člověka, kterého se digitální stopa týká. Podobně jako je apelováno na bezpečné znehodnocení tradičních odpadků[175], je nutné uvažovat i nad elektronickým košem. Umístění souborů do něj totiž nepředstavuje smazání digitální stopy, což ale nemusí být méně počítačově gramotnému uživateli zřejmé, když k vložení do koše použil příkaz *odstranit*. I po odstranění souborů z koše je ale možné je za určitých okolností obnovit pomocí specializovaného softwaru[176], v případě klíčových informací je proto vhodné (i několikanásobné) přepsání[177] nebo zformátování nosiče, na kterém byly uloženy, např. flash disku nebo harddisku prodávaného počítače.

Pro prevenci vzniku digitální stopy je zásadní jednání člověka, technická opatření mohou přispět jen v omezené míře a vždy je možné přes ně přejít a digitální stopu vytvořit. Nejsnáze zneužitelné jsou pak informace, které o člověku zveřejní on sám nebo někdo z jeho okolí zadáním do elektronického prostředí. Je tedy především na chování uživatele, aby se vytvářela pozitivní a co nejméně negativní digitální stopa. Pokud již negativní digitální stopa vznikne, jsou možnosti dané jednáním uživatele omezené, odstranění na žádost je silně závislé na ochotě člověka, který má k tomu oprávnění, příp. na omezených možnostech legislativy, které jsou popsány v kap. 3.1. Zde se tedy výrazněji mohou uplatnit různé nástroje než tomu je u prevence vzniku digitálních stop.

V oblasti chování při řešení bezpečnosti digitálních stop je vhodné v závěru zmínit ještě jednu oblast, kde by knihovníci měli působit. Aby knihovna problematiku řešila opravdu dostatečně, měla by být poradním bodem nejen při předcházení problémům nebo řešení protiopatření, důležité je také správné chování knihovníka, pokud za ním přijde člověk s tím, že je obětí útoku a neví, jak jej řešit. Pokud se jedná o dítě, je nutný ještě citlivější přístup. Vždy je nezbytné, aby knihovník byl pozorný posluchač a umožnil sdělení všech aspektů útoku, které mohou hrát roli při pochopení i řešení situace. I pokud je událost nepříjemná, není vhodné podporovat pocit sekundární viktimizace[178] projevy negativních emocí

[175] MITNICK 2003, s. 164-166
[176] Např. File Scavenger, Disk Checker, Recuva,GetDataBack, Pandora Recovery a mnohé další
[177] Např. pomocí softwarů FileShredder, Secure Eraser, Active@ KillDisk, FCleaner, O&O SafeErase a další
[178] Druhotné poškození řešením incidentu - VÁGNEROVÁ 1999, s. 393

(např. (*To je strašné!*), ale spíše usilovat o přesvědčení dítěte, 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, což samo může být pro dítě někdy velmi náročné, častá je obava ze zákazu dalšího použití internetu[179], v případě překročení zákona při útoku může silně pomoci pravomoc Policie. Pro podporu z psychologického hlediska i hledání řešení, ať už pro dítě nebo knihovníka či rodiče, mohou pomoci horké linky, kde působí školení pracovníci pro tyto případy.

Základem je tedy bezpečné chování, které by mělo být podpořeno všemi možnostmi, které se nabízejí. Vhodné je tedy spojit jak technická opatření, především správné nastavení softwaru v oblasti správy digitálních stop v jeho činnosti vznikajících, tak legislativu využitelnou při internetových útocích i informačních chování uživatelů. Každé bezpečnostní opatření je totiž možné překonat, a čím více bude bariér při útoku, tím je vyšší pravděpodobnost, že některá útok zastaví nebo alespoň omezí. Vzdělání je přitom zásadním prvkem spojeným s každým z těchto tří přístupů k zvýšení bezpečnosti. Současně je vhodné doplnit osvětu o bezpečnostních opatřeních informacemi o možnostech využití a zneužití digitálních stop (viz kap. 2.2 a její podkapitoly), aby si člověk uvědomil, proč je podstatné tato opatření aplikovat v praxi. To ukazuje význam problematiky řešené v této dizertační práci. Vzdělávání v knihovnách o bezpečnosti digitálních stop v kontextu informační gramotnosti bude věnována následující část práce.

[179] JUVONEN 2008

4 Knihovny jako součást vzdělávacího systému

Právo na vzdělání je v ČR zaručeno Ústavou, konkrétně Listinou základních práv a svobod[180]. V souladu s Evropskou unií[181] je zajišťováno nejen formálním vzděláváním, ale i neformálním a informálním[182], protože jejich spojení usnadňuje zavádění celoživotního učení, které se v současné společnosti stává nezbytností.

Základem systému vzdělávání je školství, které představuje formální vzdělávání a spadá pod Ministerstvo školství, mládeže a tělovýchovy. To podporuje rozvoj na všech definovaných úrovních školství: preprimární, primární a nižší sekundární, vyšší sekundární, postsekundární neterciární, terciární a další vzdělávání a odborná příprava.[183] Obsah na primárním stupni školství představuje povinný minimální standard, kterým musí projít každé dítě ve stanoveném věku. Od 1. 1. 2005[184] je vymezen tzv. Rámcovým vzdělávacím programem[185], který definuje tematické okruhy a cílové znalosti, dovednosti a postoje. Jejich konkretizace je ale na škole (formulováno jedinečně ve vlastním Školním vzdělávacím programu) a dále přizpůsobitelné každým učitelem s dodržením nadřazených dokumentů. Mimo vysoké školy[186] jsou státní školy zřizovány obcí či krajem, stejně jako knihovny. Společný zřizovatel je usnadněním spolupráce, která je v jeho prospěch (instituce si mohou vypomoci svou odborností v rámci běžné pracovní činnosti bez dalších nákladů, které jdou z rozpočtu zřizovatele).

Před vstupem na pracovní trh připravuje na profesi na výše jmenovaných stupních počáteční vzdělávání. Mimo něj lze využít třech forem vzdělávání dospělých: všeobecného pro přípravu na studium na střední nebo vysoké škole, dalšího odborného vzdělávání a přípravy (doplnění kvalifikace, vč. v některých profesích požadované pravidelné aktualizace vědomostí) a „*občanského/zájmového vzdělávání (v naší zemi tradičního), které má obecně kultivační charakter a uspokojuje zájmy občanů*“[187]. Další vzdělávání mohou zajišťovat školy, orgány

[180] Usnesení č. 2/1993 Sb., čl. 33
[181] Communication from the Commission of the European communities 2001
[182] Formy vzdělávání, jejich vztah a specifika jsou předmětem kap. 8.1.1 Neformální vzdělávání
[183] Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10
[184] Dáno účinností zákona č. 561/2004 Sb.
[185] Ty existují pro různé úrovně školství: RVP Předškolní vzdělávání, RVP Základní vzdělávání, RVP Základní vzdělávání – LMP, RVP Základní škola speciální, RVP Gymnázia, RVP Gymnázia se sportovní přípravou, RVP Odborné vzdělávání
[186] Ty jsou dle zákona č. 561/2004 Sb. samosprávné
[187] Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 48

veřejné správy nebo jejich vzdělávací instituce, nestátní neziskové i komerční organizace. Přes vzdělávací instituce orgánů veřejné správy a samosprávy do dalšího vzdělávání spadají také knihovny. Přestože knihovny spadají pod Ministerstvo kultury, jsou uznány jako instituce zajišťující významnou část zájmového vzdělávání s jasnou tradicí v tomto směru.[188]

Knihovny přispívají do systému zajištěním neformálního vzdělávání, příp. spoluprací se školami jako externí subjekt formálního vzdělávání, kdy jen zajišťují uskutečnění lekce. Knihovny si nemohou nárokovat místo ve vzdělávací činnosti školy, mohou jen vyjádřit zájem a případně přesvědčit o přínosech, ale rozhodnutí je jen na škole, jaké zapojení knihovně umožní. Přesto spolupráce škol a knihoven probíhá[189] a je hodnocena jako pozitivní (neustupuje se od ní po zkušenosti), proto je na ni možné navázat i tuto dizertační práci. Mnohem více prostoru ale knihovna má v oblasti zájmového vzdělávání, kde dochází k přímému kontaktu knihovny se vzdělávanými bez tak výrazných vlivů prostředníků, jako je tomu u škol. Bez ohledu na to, o jaký typ vzdělávání se jedná, neškolské instituce zajišťují vzdělávání nejčastěji v oblasti výuky cizích jazyků, využívání počítačů, managementu a účetnictví[190]. Z toho vyplývá, že vzdělávání v knihovnách o bezpečnost digitálních stop odpovídá nastavení systému vzdělávání v České republice. Z hlediska formy vzdělávání mimo školské instituce je zdůrazňováno využití škály metod, „*[n]a významu nabývají interaktivní metody výuky: hraní rolí, simulace, případové studie, často z vlastní praxe frekventantů.*“[191] Tato forma je základem aktivního učení a je aplikována také jako výchozí přístup k navrženým lekcím v kap. 8.2.

Přestože se rozvíjí e-learning, stále dominuje prezenční, příp. kombinované vzdělávání, geografické umístění vzdělávací instituce je tedy klíčovou charakteristikou. Významnou výhodou knihoven při vzdělávání je proto fakt, že tvoří systém spolupracujících institucí, který pokrývá celou republiku a knihovny jsou dobře dostupné instituce i pro vzdělávání. Spolupráce knihoven vychází z nastavení systému knihoven[192], které jsou (od největších) zřizovány Ministerstvem kultury, krajem a obcí, v oblasti své specializace mohou pomoci také

[188] Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 50
[189] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012
[190] Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 53
[191] Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 54
[192] Zákon č. 257/2001 Sb., § 3

specializované knihovny. Krajské knihovny (a Moravská zemská knihovna, která plní funkci krajské knihovny dle § 10, odst. 2 knihovního zákona), příp. jimi pověřené knihovny, vykonávají pro knihovny v kraji tzv. regionální funkce, mezi které patří poradenství, vzdělávání a koordinace další činnosti pro rozvoj knihoven a jejich služeb. V metodickém pokynu Ministerstva kultury k zajištění výkonu regionálních funkcí knihoven a jejich koordinaci na území České republiky[193] jsou uvedené činnosti rozvedeny, přičemž předpokládány jsou pro jejich zajištění znalosti knihovníka mj. v oblasti výpočetní techniky a využívání informačních technologií, a to na úrovni ECDL, mezi jehož základní moduly patří i bezpečné používání informačních technologií[194].

Vzdělávání patří dle § 12, odst. 2 knihovního zákona mezi služby základních knihoven, zřizovaných obcemi. Jsou tak schopné přenést vzdělávání v knihovnách co nejblíže cílové skupině. Podle § 4, odst. 3 stejného zákona je na provozovateli knihovny, zda je bude poskytovat (podobně jako třeba možnost reprografických služeb nebo poskytování písemných rešerší), že se ale jedná o žádoucí službu, ukazuje §15, odst. 1, písm. h), protože výchovné a vzdělávací projekty jsou zde zařazeny mezi ty, na které může provozovatel knihovny žádat účelové dotace z veřejných finančních prostředků.

Knihovní zákon nevymezuje předmět nebo formu vzdělávání v knihovnách, jen stanovuje odůvodněnost jeho realizace. Je ale logické, že knihovny vzdělávají v oblastech, kde mohou zajistit kvalitu, tedy primárně v jejich specializaci práce s informacemi. Vedoucí knihovních a informačních služeb na All Hallows' School, Brisbane, dokonce vyjádřila přesvědčení, že „*[d]nes knihovny patří do oboru informací a, pokud chtějí přežít, komunikace.*"[195] To vychází z potřeb pro digitální občanství, v rámci kterého hraje informační bezpečnost zásadní roli, jak je patrné na jeho devíti složkách[196]. Které oblasti by knihovny měly rozvíjet, jsou proto předmětem strategických dokumentů na různých úrovních, které knihovnám ukazují preferované příležitosti vlastního rozvoje, jenž knihovny mohou, ale nemusí využít. V případě využití si budují vlastní postavení[197] a oprávněnost

[193] Metodický pokyn Ministerstva kultury (…) 2011
[194] Sylaby a moduly [2014]
[195] WEAVER 2010, s. 24
[196] RIBBLE, M. Nine themes of digital citizenship. In: EKE 2012
[197] LEEDER 2014

existence, protože odpovídají na společenskou poptávku[198]. Proto bude předmětem následujících částí ukotvení vzdělávání v knihovnách o bezpečnosti digitálních stop ve strategických dokumentech pro knihovny, ale také v informační gramotnosti, která představuje logickou specializaci knihoven při vzdělávání jejich uživatelů. Na závěr bude formou tzv. desk research (výzkum od stolu) popsán současný známý stav jejich plnění, především v České republice, ale i ve srovnání s dalšími státy.

4.1 Strategie knihoven a vzdělávání o digitálních stopách

Služby knihoven jsou v současnosti spojeny s informačními technologiemi. V některých se jedná o doplnění o funkce (např. elektronický proti lístkovému katalogu), jinde je posun výraznější, např. přístup veřejnosti k informacím na internetu. I pro efektivní využití veřejných knihovnických a informačních služeb je proto zásadní, aby byl uživatel do určité míry informačně gramotný. Současně učení uživatelů o práci s informacemi a informačními zdroji patří k tradičním funkcím knihovny, aby ji mohli uživatelé využívat samostatně a nepotřebovali nutně asistenci knihovníka. Je proto logické, že se informační gramotnost uživatelů a samozřejmě i knihovníků objevuje ve strategických dokumentech pro knihovny. Vzhledem k vývoji společnosti se ale do těchto dokumentů, ať na úrovni vzdělávání nebo služeb, objevuje i informační bezpečnost, vč. digitálních stop. Tyto dokumenty by přitom měly být vnímány jako doporučení, kam směřovat pozornost a vývoj knihovny, aby její služby co nejvíce odpovídaly na potřeby společnosti. Některé se zaměřují na knihovny bez omezení, jiné cílí na konkrétní typy. Dále bude na základě významných a pro české prostředí relevantních strategií, představeno postavení bezpečnosti digitálních stop v knihovnách.

Podpora vzdělávání v knihovnách pro potřeby informační společnosti má základ ve Státní informační politice[199] z roku 1999. Vzdělávání bylo prezentováno jako cesta ke konkurenceschopnosti Evropské unie, proto se na něj objevuje důraz opakovaně až do současnosti, někdy s výslovným uvedením knihoven. Informace pro rozvoj občanů přes knihovny byly s rozvojem ICT stále více spatřovány

[198] PINTO 2013
[199] Státní informační politika 1999

v digitální podobě, proto se přístup veřejnosti k internetu dostal do knihovního zákona a také se objevil a roky fungoval projekt internetizace knihoven. Spojení knihoven, IT a vzdělávání je z vývoje patrné. V rámci spolupráce se školami se objevuje i v aktuálně připravovaných strategiích jako jeden z podporovaných prvků vzdělávání v příštích letech[200]. Informační bezpečnost, včetně problematiky digitálních stop, se v koncepcích také objevuje od roku 1999[201] do současnosti[202], protože důvěryhodnost je chápána jako nezbytný předpoklad pro použití veškerých elektronických služeb, od e-komerce po e-Government.

Samotné knihovny a organizace, které je sdružují, také vytváří strategické dokumenty zahrnující jak vzdělávání, tak i téma informační bezpečnosti s digitálními stopami. Zásadní postavení zde zaujímají koncepce rozvoje knihoven, vzhledem k jejich přípravě knihovnami a následné podpoře státu schválením Vládou ČR. Již od roku 2004 se v koncepci[203] objevuje požadavek na vzdělávání uživatelů knihoven vzdělanými knihovníky, kdy mezi podpořená témata patří počítačová a informační gramotnost občanů a zmíněna je i podpora spolupráce knihoven a škol v oblasti informační gramotnosti. Tím je pokryt i předmět této dizertační práce. Následující koncepce pro období 2011-2015[204] navazuje na předchozí v podpoře vzdělávání v oblasti počítačové a informační gramotnosti s důrazem na odstraňování Digital Divide (digitální propast na úrovni přístupu k informačním technologiím i schopnosti je využívat), na což opět navazuje téma digitálních stop. Opakovaně se objevuje i podpora spolupráce se školami při vzdělávání. Vzhledem k tématu dizertační práce je zásadní také výzva k přeměně knihoven v informační, kulturní, vzdělávací a komunitní centra, protože „*[v] souvislosti s rozvojem internetu, masové digitalizace tištěné produkce minulosti i současnosti lze očekávat pokles zájmu o tradiční knihovnické služby. Knihovnám se otvírá možnost soustředit se více na nové potřeby komunity, ve které působí.*“[205] Mezi tyto potřeby bezpochyby patří i bezpečnost digitálních stop, jejíž narušení vede k omezení důvěry a tím i využívání služeb v informační společnosti. Současně koncepce upozorňuje, že na vzdělávací akce navazuje činnost knihovny

[200] Dlouhodobý záměr vzdělávání a rozvoje vzdělávací soustavy ČR (2011-2015) 2011
[201] Státní informační politika 1999
[202] Státní politika v elektronických komunikacích Digitální Česko v. 2.0 2013
[203] Koncepce rozvoje knihoven v České republice na léta 2004 - 2010 2004
[204] Koncepce rozvoje knihoven ČR na léta 2011 - 2015 včetně internetizace knihoven 2012
[205] Koncepce rozvoje knihoven ČR na léta 2011 - 2015 včetně internetizace knihoven 2012

jako kontaktního a poradenského bodu pro uživatele při používání internetu. Protože internetové incidenty představují problém, který je nutný řešit, a ne vždy je toho uživatel sám schopný, lze očekávat potřebu asistence knihovnou právě také v oblasti bezpečnosti digitálních stop.

České strategie reflektují místní specifika, ale navazují na mezinárodní dokumenty knihovnických organizací, především IFLA, která vzdělávání věnuje poměrně výraznou pozornost již řadu let[206]. V dokumentech IFLA mají knihovny v oblasti informačních technologií pro společnost zásadní roli zajištěním infrastruktury, vzdělávání a poradenství. Podporují vzdělávání knihovníků i uživatelů knihovny, a to v informační i počítačové gramotnosti. Vyzdvihována je především role knihoven pro odstraňování Digital Divide jako společenského problému pomocí vzdělávání. Stranou nezůstává ani podpora spolupráce mezi školami a knihovnami v oblasti vzdělávání. Silnou podporu pro význam tématu této dizertační práce poskytuje IFLA Trend Report[207], podle kterého v nejbližších letech bude informační prostředí nejvíce ovlivněno pěti trendy, které jsou silně spojeny s důsledky využívání informačních technologií, přičemž první tři z nich úzce souvisí se vzděláváním v knihovnách o bezpečnosti digitálních stop:

- Nárůst Digital Divide rozšiřováním nových technologií: komentář odkazuje k schopnosti pracovat s technologiemi.

- Vzdělávání („*Online vzdělávání bude demokratizovat a narušovat globální učení.*“[208]): ve výkladu je zdůrazněn růst významu celoživotního učení, především pomocí neformálního a informálního vzdělávání.

- Soukromí a ochrana dat: především sofistikované metody práce s digitálními stopami uživatelů povedou k přehodnocení hranic soukromí, lze očekávat také vážné důsledky v oblasti důvěry v online prostředí.

Jmenované nepodporuje jen IFLA, objevují se i v dalších knihovnických strategiích, např. The Public Library in the Electronic Word[209], vzhledem k významu ale je dostatečně představený trend dokumenty IFLA. Z přehledu

[206] Např. IFLA/UNESCO Public Library Manifesto 1994; Manifest IFLA o přístupu k internetu 2002; The Role of Libraries in Lifelong Learning: Final report of the IFLA project under the Section of Public Libraries 2003; Manifest IFLA pro digitální knihovny 2010
[207] Riding the Waves or Caught in the Tide? 2013
[208] Riding the Waves or Caught in the Tide? 2013, s. 4
[209] PORS [2002]

vyplývá, že vzdělávání o bezpečnosti digitálních stop odpovídá doporučením pro zájmy a vývoj knihoven formulovaným v strategických dokumentech.

4.2 Informační gramotnost

Jak bylo uvedeno v předchozí kapitole, vzdělávání v knihovnách je primárně podporováno ve významu informačního vzdělávání, resp. počítačové a informační gramotnosti. Vzdělávání k bezpečnosti digitálních stop je možné zařadit pod všechny tyto pojmy, pro doložení tohoto tvrzení i pro terminologické upřesnění pro další práci je klíčové vymezit význam a vztah jmenovaných pojmů.

Zřejmě nejméně problémový je termín informační vzdělávání, který je ustálený v českém prostředí, ale jeho výskyt v zahraničních odborných zdrojích je omezený. Preferována je zde spíše práce s pojmem informační gramotnost, kdy informační vzdělávání označuje organizovaný proces vzdělávání s cílem přiblížit se cílovému stavu, kterým je právě informační gramotnost. Tento pojem je již výrazně složitější, protože označuje komplexní schopnost efektivní práce s informacemi a technologiemi s nimi spojenými[210]. Co pod toto široké vymezení spadá, je stále ve vývoji. Přesto existuje definice informační gramotnosti, která je široce uznávaná a na kterou navazuje většina konkretizací ve standardech informační gramotnosti. Všem třem úrovním bude věnována pozornost pro ujasnění pozice bezpečnosti digitálních stop v nich.

Extrémní názory řadí počátky vzdělávání k informační gramotnosti do poloviny 19. století[211], poprvé ale definoval informačně gramotné jedince v roce 1974 Paul G. Zurkowski jako „*lidi vyškolené v používání informačních zdrojů pro svou práci*“[212]. Zvýšená dostupnost informací vedla k potřebě rozšířit tuto definici a v roce 1989 ALA představila vymezení, které je nejčastěji akceptované až do současnosti: „*Aby byl informační gramotný, člověk musí být schopný uvědomit si, kdy je informace potřebná, a mít schopnost najít, zhodnotit a použít efektivně*

[210] Toto široké pojetí pokrývá různé definice, několik tomu odpovídajících uvádí např. LLOYD 2010, s. 42
[211] COX 2008, s. 14.
[212] ZURKOWSKI 1974, s. 6

potřebnou informaci.“[213] Hned v následující větě je přitom uvedena potřeba začlenit takto pojímané gramotnosti do vzdělávacích programů ve školách.

Vzhledem k tomu, že informační prostředí se rychle mění, ale definice je již 15 let stará, objevují se její kritiky[214]. Vlivem nových informačních technologií a zejména rozvojem Webu 2.0 se nabízejí otázky, zda i nově potřebné oblasti je možné pod definici začlenit, nejen oblast zpracování, ale i tvorby a zpřístupňování informací[215]. Právě do ní také spadá téma digitálních stop.

Pro oblast informačních technologií je definováno několik gramotností. Již byla zmiňována počítačová gramotnost, ale lze se setkat i s gramotností digitální, mediální, síťovou nebo tzv. novými gramotnostmi, které se snaží všechny uvedené typy zaštítit. Jak vyplývá ze srovnání definic těchto pojmů[216], informační gramotnost představuje nejširší vymezení, kdy ostatní jmenují specifický přístup k části kompetencí formujících informační gramotnost. Právě ona je také nejvíce spojena s knihovnami, proto bude dále zařazení tématu bezpečnosti digitálních stop řešeno jen v jejím kontextu.

Definice informační gramotnosti je vzhledem k její funkci obecná, je tedy diskutabilní, zda pokrývá bezpečnost digitálních stop. Nejblíže k ní má hodnocení a užití informací, protože uvážlivé chování je zásadním bezpečnostním prvkem v oblasti digitálních stop, jejich využití i zneužití je často spojeno s nedostatečným zhodnocením zpracování digitálních stop a nalezení publikovaných informací může často předejít neoprávněnému vložení důvěry s poskytnutím digitálních stop. Aby bylo možné užití informace označit jako efektivní, nemůže být spojeno s informačním rizikem nebo přímo útokem. Zpřístupnění digitálních stop pak odpovídá užití a rozšiřování informací, které se objevuje v novějších definicích[217]. Pro jasnější doklad vztahu je nutné využít standardy informační gramotnosti. Následně budou popsány vybrané, splňující kritérium odlišnosti.

K primární cílové skupině této práce má nejblíže model Big6™[218], protože se zaměřuje na informační gramotnost od tzv. K12 po dospělé. Tento model je tradiční a odpovídá definici ALA, nezdůrazňuje proto specifická témata jako

[213] Presidential Committee on Information Literacy 1989
[214] Např. LI 2009, s. 570
[215] KOVÁŘOVÁ 2013
[216] KOVÁŘOVÁ 2013
[217] VAN HELVOORT 2010, s. 61
[218] Big6 Skills Overview [b.r.]

informační bezpečnost nebo digitální stopy. Právě to bylo kritizováno a byl kladen důraz na to, aby v rámci složek modelu nebyla opomíjena bezpečnost v kyberprostoru, v níž byla jmenována i ochrana soukromí a dat v elektronickém prostředí, tedy právě oblast digitálních stop[219].

Protože Big6™ není standard, nenabízí proti výše komentovaným definicím konkrétnější vodítka k zařazení bezpečnosti digitálních stop, odkazuje ale na národní standardy informační gramotnosti. Je proto možné navázat standardem Information Literacy Standards for Student Learning[220], který je zaměřený na K12 a podpořila jej i ALA. Dělí se na tři části, z čehož první tvoří jádro informační gramotnosti a další dvě (nezávislé učení a sociální odpovědnost) „*jsou zakotveny v informační gramotnosti, ale popisují obecnější aspekty učení studentů, ke kterému školní knihovní mediální programy také významně přispívají.*“[221] V rámci jádrového standardu se k bezpečnosti digitálních stop vztahuje standard 2 (hodnocení informací kriticky a kompetentně), kde všechny jmenované indikátory odpovídají bezpečnému chování pro prevenci ohrožení digitálních stop. Protože standard je již z roku 1998, neakcentuje příliš produkci informací, nicméně odpovědné vytváření digitálních stop lze zařadit do užití informací (standard 3), především indikátoru produkce a komunikování informací a myšlenek ve vhodných formátech. V rámci širších oblastí se nabízí pro digitální stopy sociální odpovědnost, která je v dokumentu u každého standardu spojena s informační gramotností. Především standard 8, indikátor 3. odkazuje na odpovědné použití informačních technologií.

Jmenovaný model Big6™ i další se odkazují na standard ACRL, který je ale primárně určen pro vysokoškolské prostředí, jak jasně ukazuje jeho plný název Information Literacy Competency Standards for Higher Education[222], je členěn na pět standardů a 22 indikátorů. Podobně jako u předchozího pojetí i zde je vztah bezpečnosti digitálních stop ke kritickému hodnocení zdrojů i informací samotných, tj. standard 3, konkrétně indikátory č. 2 (evaluace zdroje a informace) a 5 (rozhodnutí, zda nová znalost má dopad na individuální hodnotový systém, a přijetí či nepřijetí změny). Zásadnější je ale standard 5 (porozumění etickým,

[219] LI 2009, s. 573-574
[220] Information literacy standards for student learning 1998
[221] Information literacy standards for student learning 1998, s. 1
[222] Information Literacy Competency Standards for Higher Education 2000

právním a sociálním otázkám použití informací a přístup a použití informací eticky a legálně) a všechny tři jeho indikátory, kde se objevují témata jako netiketa, soukromí, zabezpečení dat, bezpečná autentizace apod. Postavení digitálních stop je tedy i v tomto vymezení evidentní.

Jiným uznávaným modelem pro vysokoškolské prostředí je tzv. Sedm pilířů informační gramotnosti[223], v rámci jeho výkladu je stanovena také kompetenční úroveň. Vzhledem k zaměření na jinou cílovou skupinu, ale i význam, je vhodné zmínit, že také on zahrnuje téma digitálních stop. Vztah je patrný v části *Záběr*, kde informačně gramotný rozumí typům informací, které jsou dostupné (což jsou i digitální stopy), a také publikačnímu procesu ve smyslu proč jedinec publikuje a hodnotě informací. V rámci fáze *Sběr* je pak uvedena znalost rizik vyplývajících z pohybu ve virtuálním světě, vztah fáze *Evaluace* byl již komentován výše. Následující *Řízení* zahrnuje porozumění důležitost etického ukládání a sdílení informací a dat, mezi dovednosti je zařazena také demonstrace povědomí o tématech spojených s právy jiných, vč. ochrany dat. Konečně poslední krok *Prezentace* je spojen se znalostí osobní odpovědnosti při uložení a sdílení informací a dat a také při rozšiřování informací a znalostí, patří sem také schopnost budování profilu v komunitě použitím vhodných osobních sítí a digitálních technologií, tento požadavek tedy zcela pokrývá uvědomělé budování pozitivní digitální stopy.

V českém prostředí se prostřednictvím podpory komise IVIG projevuje také vliv standardu CILIP[224]. Ten opět uvádí hodnocení důvěryhodnosti nalezených informací, etiku a odpovědnost při použití informací, komunikaci a sdílení nalezených informací, vč. porozumění výhodám a nevýhodám různých komunikačních kanálů. Právě mezi podstatné nevýhody spojené s mnoha elektronickými kanály patří i digitální stopy. Na závěr standard uvádí i management nalezeních informací, kdy mezi příklady je uvedeno také zabezpečení.

Takto by bylo možné pokračovat s dalšími standardy, nicméně je patrné, že základní vazby se opakují. Proto lze otázku ukotvení bezpečnosti digitálních stop ve standardech informační gramotnosti považovat za uzavřenou. Na závěr je vhodné doplnit, že silněji se opodstatněnost tématu objevuje ve standardech více spojených s informačními technologiemi, např. ISTE (dříve NETS) standardy pro

[223] The SCONUL Seven Pillars of Information Literacy 2011
[224] Information literacy skills 2012

vzdělávání v informační společnosti. Pro tuto práci je podstatný především ISTE standard pro studenty[225], kde v rámci digitálního občanství je požadavek na praktikování bezpečného, legálního a odpovědného použití informací a technologií a na osobní zodpovědnost za celoživotní učení. Soukromí a digitální stopy jsou také často zmiňovány ve standardu FIT (Fluency with Information Technology)[226], na jehož vzniku se podíleli experti na různé oblasti práce s informacemi a informačními technologiemi, včetně knihovníků. Těsnost spojení informační gramotnosti a informačních technologií je evidentní, nicméně otázkou zůstává, nakolik se překrývají. Někdy je počítačová a tím i internetová gramotnost vnímána jako složka informační gramotnosti[227], při tomto přístupu ještě význam digitálních stop vzrůstá. I v tradičních modelech informační gramotnosti prezentovaných výše ale má bezpečnost digitálních stop své místo, stejně jako další témata informační bezpečnosti, především úzce související kritické myšlení a evaluace informací a zdrojů a právní a etické užití informací a zdrojů, včetně odpovědnosti za vlastní jednání v informačním prostředí.

Pro zlepšování informační gramotnosti je nutné „*zabývat se všemi třemi složkami této problematiky: tedy samotným definováním toho (nebo shody o tom), co je informační gramotnost, dále pak vytvořením standardů informační gramotnosti (na různých úrovních) a nakonec problematikou informačního vzdělávání samotného, tedy onoho 'jak učit' informační gramotnost, nebo přesněji přispívat k jejímu rozvoji.*“[228] Jak vyplývá z této kapitoly, bezpečnost digitálních stop do informační gramotnosti patří. Cílem vlastní práce v rámci této dizertace je proto poslední uvedený krok, tedy metodika stanovující jak učit v knihovnách o bezpečnosti digitálních stop.

4.3 Bezpečnost digitálních stop ve vzdělávání v knihovnách

Jak bylo prezentováno v předchozích kapitolách, informační bezpečnost, vč. zaměření na digitální stopy je vhodné uvažovat v rámci služeb knihoven. Vůči

[225] ISTE Standards © 2007
[226] SNYDER c2011
[227] DOMBROVSKÁ 2004
[228] DOMBROVSKÁ 2004

uživatelům knihovny je nejzřetelnější a pro tuto práci nejzásadnější jejich řešení ve vzdělávacích akcích pro veřejnost. Kromě toho, co přináší toto spojení tématu a prostředí knihovnám, je zásadní přínos i pro samotné uživatele, což opět přispívá knihovnám. Knihovny tak dávají odpověď na společenskou poptávku, řeší problém spojený nejen se současnou, ale jistě i budoucí společností, což není pravidlem pro všechny služby knihovny.

Jak bylo popsáno v předchozích kapitolách, pokud knihovny zahrnou problematiku digitálních stop do svých vzdělávacích aktivit, nebude se v zásadě jednat o zcela novou oblast, ale spíše rozšíření podtémat informační gramotnosti, která je s knihovnami velmi úzce propojená. Vzdělávání navíc zvyšuje efektivitu všech typů bezpečnostních opatření pro ochranu digitálních stop, jak bylo prezentováno v kapitolách 3.1 - 3.3. Na základě různých teoretických východisek i praktických zkušeností (viz dále v této kapitole) je možné formulovat množství faktorů, které jasně ukazují možnost plynulého navázání na současnou situaci a přínosy, které zahrnutí vzdělávání o bezpečnosti digitálních stop může přinést:

1. Přístup veřejnosti k internetu

Podle knihovního zákona patří mezi základní služby knihovny umožnění přístupu veřejnosti k volně dostupným informacím na internetu, knihovny proto mají povinnost internet svým uživatelům zprostředkovat, a to zdarma a v případě zájmu s pomocí uživateli. Přitom podle výzkumů čeští uživatelé tuto možnost stále (a stabilně) využívají[229], přestože se zvyšuje počet domácností připojených na internet[230], vede je k tomu často to, že knihovna zprostředkovává v této oblasti poradenství[231], tj. pomáhá s řešením problémů. Mezi ty jistě patří i problémy v oblasti bezpečnosti digitálních stop, k čemuž vede i vyjádření v Manifestu IFLA o přístupu k Internetu: „*Uživatelům by měla být poskytnuta pomoc v oblasti nezbytných dovedností a vhodné prostředí, v němž by mohli poskytnutých informací svobodně a bezpečně využívat.*“[232] Z toho vyplývá, že tento faktor bude podstatný i do budoucna. Podpora vzdělávání pro použití služeb knihovny ale odpovídá ještě více bezpečnosti digitálních stop vzhledem k rozšiřující se komunikaci knihovny

[229] Základní statistické údaje o kultuře v České republice 2012 2013
[230] See the evolution of an indicator and compare breakdowns 2014
[231] QUICK 2013, s. 12-14
[232] Manifest IFLA o přístupu k internetu 2002

s uživateli pomocí sociálních sítí jako Facebook nebo Twitter pro účely propagace, ale třeba i vzdělávání – knihovna by měla tyto uživatele podpořit v tom, aby její služby používali tak, aby se sami neohrozili[233].

2. Lokální vyústění sítě knihoven

Díky hustotě sítě knihoven, která je v České republice nesrovnatelně hustší než v jiných státech[234], je možné téma dostat do mnoha lokalit nejen nárazově, ale trvale. Množství kontaktů se systémem knihoven umožňuje snadnou distribuci jednou vytvořeného řešení vzdělávání o bezpečnosti digitálních stop. To vychází z fungující spolupráce a sdílení lekcí knihovnami[235] nad rámec požadovaný knihovním zákonem, především v rámci regionálních služeb knihoven.

3. Knihovnické organizace pro informační gramotnost uživatelů

Spolupráce v neformálním vzdělávání veřejnosti se odráží ve fungování různých organizací, především IVU SDRUK (Informační vzdělávání uživatelů Sdružení knihoven) a IVIG AKVŠ (Odborná komise pro informační vzdělávání a informační gramotnost Asociace knihoven vysokých škol). Obě instituce, zaměřené na různé typy knihoven i uživatelů, se snaží reflektovat své vymezené prostředí, proto zjišťují podobu vzdělávání v knihovnách, ale vzhledem k rozsahu témat, která se objevují, jsou výsledky spíše rámcové, proto bylo pro potřeby této dizertační práce nutné upřesnění pro oblasti digitálních stop (viz kap. 7.1 a 7.2), její spojení s informační gramotností bylo předmětem předchozí kapitoly.

4. Důvěryhodnost knihoven jako institucí zprostředkujících informace

Knihovna jako informační instituce se musí zaměřovat na informace, nejen na jejich nosiče. Tím se stává druhořadou otázka, zda je informace digitální nebo analogová, obě by měly knihovny řešit stejným dílem. A pokud má být vnímána jako důvěryhodný zprostředkovatel digitálních informací, je nutné, aby při správném využití služeb knihovny nedošlo k ohrožení uživatele. Přístup veřejnosti k internetu by proto sám měl být bezpečný, aby si knihovna udržela reputaci

[233] WEAVER 2010, s. 30
[234] GÉBLOVÁ 2003
[235] Toto tvrzení vychází z frekvence položených a uspokojených poptávek i nabídek lekcí v elektronické konferenci pro knihovníky Andersen a také z e-mailové komunikace s Marikou Zadembskou (Městská knihovna Třinec) ze dne 28. 3. 2013.

důvěryhodné instituce, přestože veřejné počítače jsou obecně považovány za informační hrozbu, do značné míry právě s vazbou na digitální stopy.

5. Důvěra místní komunity založená na dlouhodobém vztahu

Důvěru je nutné budovat dlouhodobě na pozitivní zkušenosti. Dlouhodobý vztah se svými uživateli knihovny mají, až na výjimky se jedná o instituce fungující desítky let. Důvěra uživatelů je závislá na situaci a jednání knihovny, vzhledem k neustálému nátlaku pro udržení finančních prostředků od poskytovatele je ale pravděpodobné, že v případě, že by uživatelé ke knihovně důvěru ztratili a jejích služeb by nevyužívali, vedlo by to k omezení až likvidaci knihovny. Statistiky jejich využití, vč. vzdělávacích akcí (viz kap. 6.3) ale ukazují stálý zájem o služby knihovny, vč. poradenství v práci na internetu (viz 1. bod). K budování důvěry je využíváno i spolupráce s dalšími subjekty, např. jinými příspěvkovými organizacemi v obci, ale i dobrovolnickými jako ekocentra[236], které mohou zprostředkovat navázání vztahu s novými uživateli. Díky dlouhodobému působení si proto různí lidé mohou kdykoli vytvořit ke knihovně vztah a při kvalitních a vždy dostupných službách v něm vybudovat důvěru.

6. Možnost přizpůsobení potřebám známých cílových skupin

Dlouhodobé působení v místní komunitě vede k tomu, že knihovny znají její charakteristiky a potřeby. Tomu pak mohou přizpůsobit lekce o bezpečnosti digitálních stop. To je rozdíl proti specializovaným organizacím pro oblast informační bezpečnosti, jako Národní centrum bezpečnějšího internetu (NCBI) nebo Centrum PRVoK, které jsou centralizované, a tedy vázané na jedno místo, ze kterého dodávají své aktivity nárazově do místa poptávky, pokud je toto mimo velké město, kde daná organizace působí. Proto tyto organizace mají omezené možnosti reagovat na potřeby místní komunity, protože ji, na rozdíl od knihovny, neznají, nedokáží ji přizpůsobit potřebám dané cílové skupiny. Nárazové aktivity také mohou být spojené jen s omezenou úrovní důvěry při řešení citlivého tématu, jakým jsou digitální stopy, protože staví jen na deklarované odbornosti.

[236] Viz např. Ekopolička v blanenské knihovně iniciovaná excentrem Ulita v roce 1999.

7. Neustálá dostupnost pro řešení problémů

Důvěra řešená v 4. a 5. bodě je vázaná také na to, že knihovna je neustále dostupná pro řešení problému, je kdykoli k dispozici, právě když to její uživatel potřebuje, omezená je jen otevírací dobou. Pokud by vzdělávání v knihovnách o bezpečnosti digitálních stop bylo dostatečné na úrovni jednorázové přednášky, stačila by její nahrávka online, v případě fyzického kontaktu pak nárazové zajištění specializovanou organizací. Cílem této práce je ale návrh komplexního řešení, kdy jsou nutné opakované lekce pro různé cílové skupiny (např. pro všechny třídy ve všech ročnících škol a další skupiny osob kromě dětí v lokalitě) a také poradenství v případě problému od subjektu, který má u člověka s problémem důvěru. To musí zajistit důvěryhodná lokální organizace s kapacitou a schopností koncepčního vzdělávání o bezpečnosti digitálních stop.

8. Dostupnost jen v případě zájmu

Knihovna sice je k dispozici uživateli, kdykoli o to projeví zájem, pokud ho ale neprojeví, nemusí být v kontaktu, což je významný rozdíl při řešení digitálních stop. Jak uvádí Wold[237], citlivá problematika informační bezpečnosti by měla být řešena v prostředí, které není formální, ale je důvěryhodné, takže člověk nemá obavu mluvit o tématech, které jsou v jiných prostředích tabu. Po řešení informačních incidentů může být nekomfortní se setkávat s člověkem, který o nepříjemném zážitku ví. To může být problematické při řešení s učitelem, především v menších městech, protože s ním se dítě musí potkávat každý den znovu, v případě knihovníka může po dobu, dokud mu je to nepříjemné, knihovnu nenavštěvovat, příp. návštěvy omezit. Jiným důvodem podporujícím dostupnost v případě zájmu, mohou být situace, kdy knihovna slouží jako alternativa nefungujícího kanálu pro osvětu či řešení problému. Ne každý člověk má v bezpečnosti digitálních stop oporu a podporu v rodině, i vztahy s učitelem nemusí být odpovídající pro řešení této problematiky. Knihovna svým zaměřením na práci s informacemi, vzdělávání a služby pro veřejnost může být ideálním místem, kde hledat podporu v oblasti bezpečnosti digitálních stop, pokud ji není možné získat z míst, se kterými je člověk v každodenním kontaktu.

[237] WOLD 2010

9. Neomezená cílová skupina vzdělávání

Vzdělávací instituce se často zaměřují na určitou oblast zájmu, toto je také omezením pro formální vzdělávání, které je spojeno s jasně danými pravidly, včetně toho, kdo jej může využívat. Dosah škol je mnohdy širší než jen zaměření na aktuální žáky, ale toto rozšíření není neomezené, jedná se například o lekce pro děti v oblastech, které jsou spojené s aktuálními zájmy a potřebami školy, např. při řešení výchovných problémů, zavádění nových technologií pro kontakt mezi rodiči a školou apod. Jedná se tedy o bariéru v celoživotním a zájmovém učení, kterou ale knihovny nemají. Vzdělávací akce v knihovnách jsou obvykle opravdu pro veřejnost, která má o lekci v dané formě zájem, nemusí jít ani o registrované uživatele, pokud se o lekci dozví a mají o ni zájem. Samozřejmě i knihovny, stejně jako školy, snáze informují o svých aktivitách ty, s kterými mají aktuálně navázaný vztah, ale neomezují své služby na ně.

10. Oslovení mnoha lidí přes spolupracující organizace

Jak bylo zmíněno v 2. bodě, knihovna může dosáhnout kontaktu s mnoha lidmi tím, že využije nastavené spolupráce s různými organizacemi, nejčastěji se společným zřizovatelem. To je často případ škol, se kterými knihovny v současnosti již poměrně silně spolupracují i v lekcích informační bezpečnosti. Vzhledem k omezení témat knihovny a spolupráci s mnoha institucemi, např. školami, může jedna knihovna lekcemi o bezpečnosti digitálních stop zasáhnout výrazně více lidí. Stejně tak to může být i jiná instituce, která se této role ujme, z hlediska dalších výhod uvedených výše i specializace na práci s informacemi je ale logické, pokud se knihovna rozhodne tuto roli vykonávat.

Tento přehled prezentoval množství výhod, kterých knihovna může využít a které podpoří její úlohu, pokud se rozhodne řešit společenský problém v oblasti osvěty v bezpečnosti digitálních stop. Problém digitálních stop sice nikdy nebude vyřešen se 100% garancí jistoty bezpečí, protože vždy se může najít nějaká cesta kolem každého protiopatření, každé ale staví bariéru, která může být pro konkrétní útok nepřekonatelná nebo odrazující, protože cíl není tak zajímavý. Proto má smysl učit (se) způsobům omezení ohrožení a aplikovat je v praxi a knihovny v tom mohou velmi pomoci.

Vzdělávací akce iniciované knihovnou nebo jinou institucí jsou vhodným prostředkem pro rozšíření povědomí o řešené problematice. V oblasti informační bezpečnosti je ale nutný i druhý směr, tj. kontaktní bod pro případ, že člověk aktuálně řeší informační problém, se kterým potřebuje pomoci. Knihovny v rámci svých služeb nabízejí podporu uživatele poradenstvím v práci s elektronickými informačními zdroji a službami, je proto vhodné zařadit sem i podtéma bezpečnost digitálních stop, příp. šířeji informací bezpečnost. Právě tento kontaktní bod má svůj význam na lokální úrovni, je jen těžce zastupitelný outsourcingem experta. Jsou sice k dispozici kontakty typu Linka bezpečí, ale v citlivých oblastech informační bezpečnosti může být těžké svěřit se cizímu člověku, výrazně lehčí to může být v místě, kde je jasné, že se téma řeší a že s problémem je osloven ten, koho člověk zná a má k němu důvěru.

V rozhodování knihovny, zda se této role ujme, může hrát svou roli také fakt, že společnost se mění a to zejména vlivem informací, které jsou podstatou knihoven. Je proto nutné, aby se změnily i knihovny, otázkou je jak. Je pravděpodobné, že knihovny v příštích letech budou muset upravit nabídkou svých služeb, aby odpovídala potřebám společnosti, pro kterou fungují a kterou jsou financovány. Bylo by proto logické, aby knihovny využily právě představený potenciál v oblasti vzdělávání o bezpečnosti digitálních stop a odpovědí na tento problém společnosti si upevnily své místo v ní. Neodchýlí se ani od svého tradičního poslání, protože tím jen podpoří své postavení důvěryhodných zprostředkovatelů k informacím pro své uživatele, jen k němu bude směřovat novými způsoby, které odpovídají novým potřebám společnosti[238].

Reálnost řešení tématu podporují existující snahy zahraničních i českých knihovníků zavést jej do svých vzdělávacích akcí. V českém prostředí je obvykle řešena informační bezpečnost, někdy ještě jako dílčí téma práce s internetem nebo počítačem, v případě konkrétněji zaměřených lekcí se objevují především kyberšikana a kybergrooming. V anglicky mluvících oblastech existuje výrazně více lekcí zaměřených na digitální stopy, které jsou pojímány jako součást digitálního občanství a jsou řešeny jak z negativního, tak i pozitivního pohledu.

[238] HERRINGTON 2010

Digitální stopy je sice možné zneužít, ale mohou mít i výrazné přínosy, pokud jsou vhodně budovány. Iniciativa Common Sense Media[239] nabízí mnoho lekcí k informační bezpečnosti a také konkrétně digitálních stop, a to od stupně K2 (přibližně 6-7 let dítěte) po K12 (17-18 let), včetně lekcí pro knihovny. Na ni se s pozitivními zkušenostmi odkazují mnohé knihovny, např. na blozích pro sdílení zkušeností[240], umírněnější, ale jasné ukázky využití těchto lekcí ukazují i webové stránky škol a školních knihoven[241]. Tyto zdroje kladou důraz objektivní pohled na digitální stopy, tedy upozornění na chyby vedoucí k budování pozitivní digitální stopy. Nejedná se ale o jediný vyskytující se přístup, knihovnice na Hong Kong International School uvádí pozitivní zkušenost[242] s lekcí založenou na aktivním učení, kdy studenti vyhledávají na internetu dostupné informace o třech zadaných lidech a následně diskutují o nalezených informacích z hlediska bezpečnosti digitálních stop[243]. Z přehledu je také patrné, že se jedná především o oblast USA, lekce o digitálních stopách lze ale najít i v Austrálii[244].

V případě koncepčního pojetí (opět především USA)[245] je odkazováno i na mnohé další zdroje lekcí, které jsou volně dostupné a všechny se týkají informační bezpečnosti a mnoho z nich digitálních stop. V těchto zdrojích koncepčního řešení je problematika často vyzdvihovaná jako nezbytná komponenta lekcí informační bezpečnosti. To odpovídá doporučenému přístupu pro školní knihovny, podle kterého by měl každý ročník (K1 až K12) zvyšovat znalosti v oblasti odpovědnosti a bezpečnosti v digitálním prostředí, kdy digitální stopy představují jedno ze tří vyzdvižených témat[246]. Lekce o bezpečnosti digitálních stop se objevují také v Evropě, ve vysokoškolském prostředí. Obojí reprezentuje lekce *Who am I? My digital footprint*, která vznikla v Birkbeck Library v programu Informační a digitální gramotnosti[247]. Ve srovnání s primárním a sekundárním školstvím v USA se jedná o výrazně slabší řešení této problematiky.

[239] Scope & Sequence 2012
[240] HEMBREE 2013 (zde problematika prezentována jako součást standardu ISTE – viz kap. 4.2); In the fishbowl 2013; MORRIS 2013; SWETNAM 2013; LIBRARIANTIFF 2014
[241] Digital Footprint [b.r.]; Davis Elementary Internet Safety Month Lesson Plans © 2002-2014
[242] What is a digital footprint? © 2010
[243] FISHER [b.r.]
[244] STOWER 2013; REID 2014
[245] SULLIVAN [b.r.]; Library lessons calendar © 2002-2014
[246] Citizenship in the Digital Age 2012, s. 2
[247] ZAZANI 2013

Situace v ČR je odlišná. Knihovny téma neignorují, často jej ale řeší spíše informativně, tedy v podobě tipů pro bezpečné používání internetu, které je dostupné na webu v různých sekcích, např. počítačové učebny Městské knihovny Litvínov[248] nebo dětského oddělení Městské knihovny Pelhřimov[249].

Knihovny se také zapojují do širších organizovaných snah upozornit na problematiku bezpečného internetu, především v rámci dne bezpečnějšího internetu, na kterém v posledním roce spolupracovalo 24 knihoven (a knihovna Psychiatrické nemocnice Bohnice) formou přednášek, besed, výstav, letáků v knihovnách, tematických testů, soutěží, ale i lekcí, těch ale jen minimálně[250]. Knihovny se do této akce zapojují již několik let, lze najít doklady propagace tématu bezpečnost dětí na internetu již z prvního roku běhu tohoto projektu[251].

Vzdělávací pojetí problematiky knihovny ne vždy řeší vlastními silami, někdy jen nabízí prostředí pro realizaci vzdělávací akce. Často přednášky, příp. besedy vedené zástupci policie[252]. Externistou vedené přednášky si často zajišťují školy samy, bez zprostředkování knihovnou[253]. Obě tato zastoupení mají své negativní stránky, které byly popsány v rámci potenciálu knihoven pro řešení bezpečnosti digitálních stop ve vzdělávání představeném v této kapitole výše. Je ale nutné podotknout, že existují školy, kde téma zajišťuje pracovník školní knihovny, resp. informačního centra[254]. Jindy je možné setkat se s názorem vedení školy, že téma informační bezpečnosti patří knihovně a škola s ní má na tomto zájem spolupracovat[255]. Nicméně názor knihoven je odlišný: „*To téma je pro nás zajímavé a má velkou důležitost, ale myslím, že školám se dostává takovýchto přednášek hodně právě od specializovaných institucí a neziskovek, které se rizikovými tématy zabývají prioritně.*“[256]

Problematika je již zahrnována do vzdělávací nabídky knihoven, především nabízené přímo školám. Jen minimálně jsou zastoupeny přednášky, např. v již

[248] PC učebna 2013
[249] Dětské oddělení [b.r.]
[250] Soutěž a seznam zapojených organizací 2014
[251] Březen měsíc Internetu 2008 2008
[252] např. CHRÁSTKOVÁ KNÍŘOVÁ 2013; BAUEROVÁ 2014
[253] např. Plán ZŠ Aloisina výšina na měsíc říjen 2012 2012 (přestože tato škola uskutečňuje jiné vzdělávací akce i v knihovně); Akce – kyberšikana 2014; Preventivní programy © 2014 (škola si pozvala lektora z občanského sdružení z téměř 30 km vzdálených Letovic)
[254] např. RÁBLOVÁ 2014
[255] Vedle totožného názoru v kap. 9 byl vyjádřen také na semináři IVU 2014 – viz ZAŤKO 2014
[256] E-mailová komunikace s Marikou Zadembskou (Městská knihovna Třinec) ze dne 16. 7. 2014

uvedené Městské knihovně ve Svitavách, nebo lekce pro dospělé, např. jako dílčí téma kurzu Základy ovládání PC v Městské knihovně Přerov, který probíhal šest týdnů od poloviny února do konce března 2014[257]. Na jiné úrovni jsou pak vzdělávací akce ve vysokoškolském prostředí, kdy lze najít zcela ojedinělé zaměření čistě na digitální stopy[258].

V oblasti spolupráce se školami převažují lekce zaměřené na problematiku kyberšikany a kybergroomingu, takové vzdělávací akce již nabízely především městské knihovny[259]. Někdy se lze setkat i s širším pojetím[260], kdy jsou spíše výjimečně zmiňovány mezi řešenými tématy i digitální stopy. Často se také nejedná o lekce využívající možností neformálního vzdělávání (viz kap. 8.1.1), ale spíše jen přednášky, příp. diskuze. Oproti zahraničnímu pojetí digitální stopy nepředstavují téma, které by bylo řešeno jako podstatné a zasluhující si třeba i jedinou lekci zaměřenou jen na toto téma. Podle informací od Aleny Srovnalové z Městské knihovny Rožnov pod Radhoštěm se i toto bude měnit, pro příští rok zde plánují realizaci lekce pro 8. třídy zaměřené právě na digitální stopy[261].

Jak ukázal výzkum od stolu i představené charakteristiky knihoven ve vztahu k tématu, knihovny si jsou vědomy významu problematiky a postupně začleňují alespoň širší informační bezpečnost do nabídky svých vzdělávacích aktivit. S tím, jak jejich počet roste, se do obsahu lekcí dostává také problematika digitálních stop, ale spíše na nízké úrovni, ve srovnání se zahraničím, především USA je potenciál knihoven pro řešení problematiky digitálních stop minimální. Současná nabídka vzdělávání v knihovnách o bezpečnosti digitálních stop ale ukazuje, že má smysl se problematikou zabývat a podpořit její rozvoj nabídkou osvědčené metodiky vzdělávání v této oblasti, která bude odpovídat současným podmínkám v knihovnách. Právě zjištění jejich stavu a ověření připraveného návrhu jsou základní oddíly výzkumné části této práce.

[257] Městská knihovna Přerov - březen 2014 2014
[258] Přednáškový blok 2014
[259] např.: Nabídka knihovnických lekcí a besed na školní rok 2012 – 2013 2012; Na internetu bezpečně 2014; Nástrahy v online světě 2014; PINTÉR 2014
[260] např. ZVONKOVÁ 2009; OGROCKÁ 2013; Barevný svět poznání 2014; Nabídka pro školy [2014]; Nabídka tematických besed pro školy pobočka Jungmannova 2014/2015 pro 1. stupeň ZŠ © 2009 – 2014; Nabídka vzdělávání pro střední školy a gymnázia [2014]; Školy [2014]; ZADEMBSKÁ 2014
[261] E-mailová komunikace s Alenou Srovnalovou ze dne 18. 6. 2014

II. Výzkumná část

5 Vymezení výzkumného tématu

Výzkumná část zahrnuje několik navazujících šetření, která byla nezbytná pro řešení základní výzkumné otázky této práce: Jakými postupy by mělo být efektivně zvyšováno zajištění digitálních stop uživatelů ICT prostřednictvím vzdělávání v knihovnách? Pro informační podporu této otázky je možné vyjít ze zjištění souvisejících výzkumů. V první řadě se jedná o každoročně odevzdávané statistické výkazy knihoven[262]. Zajímavá jsou šetření činnosti knihoven srovnávající Českou republiku s dalšími státy[263]. Existují také šetření (především rozsáhlý výzkum EU Kids online[264]) pokrývající oblast vzdělávání o bezpečnosti na internetu. Průnik všech tří oblastí, tedy bezpečnosti na internetu, knihoven a vzdělávání, je v nich ale zastoupen minimálně.

V této práci je řešeno výzkumné téma vzdělávání o bezpečnosti digitálních stop v českých knihovnách se zaměřením na děti na základní škole. Cílová skupina byla zvolena proto, že spoluprací se základními školami lze zahrnout celou populaci v dané věkové úrovni, a to v období, kdy se formují jejich názory na svět a vědní obory, kam patří i návyky v práci s internetem, proto je snazší vybudovat u nich bezpečné chování. Je totiž nutné u dětí se vzděláváním veřejnosti o digitálních stopách začít a po dobré zkušenosti budou snáze oslovovány ostatní cílové skupiny, jejichž dosažitelnost je omezenější.

Aby bylo možné navrhnout koncepční řešení, muselo nejdříve dojít ke zmapování prostředí, podmínek a limitů, které je nutné respektovat, aby bylo možné návrh aplikovat do praxe. V první části je proto provedena deskripce prostředí, tedy současného stavu vzdělávání v knihovnách v ČR se zaměřením na digitální stopy, resp. informační bezpečnost. Pomocí dotazníkových šetření jsou popsány tři základní oblasti:

- vzdělávání uživatelů v knihovnách, tedy co je předmětem vzdělávacích akcí a jaké postavení mezi tématy má problematika této dizertační práce,

[262] Základní statistické údaje o kultuře v České republice 2012 2013
[263] QUICK 2013
[264] LIVINGSTONE 2011

- vzdělávání knihovníků, které je popisováno jen ve vztahu k předchozímu bodu, aby byl jasný osobní zájem těch, kteří by měli uživatele vzdělávat, o téma digitálních stop, resp. bezpečnosti na internetu a
- postoj knihovníků k vzdělávání o digitálních stopách a jejich zneužití, aby byla zachycena jejich motivace šířit téma mezi uživateli knihoven.

Protože předávat znalosti může jen ten, kdo je sám má, jsou aktuální znalosti v řešeném tématu poprány formou pedagogického testování se srovnáním cílových skupin, které představují knihovníci a studenti oboru informační studia a knihovnictví v ČR, jako budoucí možní knihovnici, kteří budou v oblasti digitálních stop uživatele vzdělávat. Touto formou by měly být zachyceny nejenom znalosti aktuálních knihovníků, ale i těch budoucích s ohledem na to, jak je v této oblasti připravuje jejich vysokoškolské vzdělání, které by mělo kvůli proměně společnosti problematiku digitálních stop zahrnovat.

V části 7 jsou zjištění z jednotlivých výzkumů popsána odděleně vzhledem k odlišným výzkumným otázkám, vzorku apod. Protože ale společně vytváří celý obraz reálných podmínek, do kterých by měly být navrhované lekce zasazeny, jsou následně výsledky propojeny v kap. 7.5. Po deskripci, tedy jak v současnosti tato oblast vypadá, je druhá polovina výzkumné části zaměřena na to, jak by vypadat mohla. Je představena koncepce vzdělávání o digitálních stopách v knihovnách pro 3. – 9. třídu základní školy ve formě konkrétních lekcí a formou akčního výzkumu je vyhodnocena efektivita návrhu.

Akčnímu výzkumu je podrobena jedna z lekcí, a to pro 4. – 5. třídu, která je s ohledem na nastavení školního systému nejsnáze proveditelná v praxi. Současně odpovídá nejčastější cílové skupině vzdělávacích aktivit v knihovnách[265]. Akční výzkum spojuje zúčastněné pozorování, dokumentovou analýzu materiálů vytvořených na lekci s anketní zpětnou vazbou od účastníků lekce a část rozhovorů se zainteresovanými osobami. Předmětem akčního výzkumu je lekce, která má vést děti k tomu, že si samy uvědomí rizikové chování i postupy, jak se mu vyhnout. Akční výzkum slouží k vhodnému nastavení efektivní lekce a tím je naplněn obecný cíl akčního výzkumu, kdy výzkumník spolupracuje se subjekty výzkumu při diagnostikování problému a tvorbě jeho řešení. Smyslem je akcí změnit stav, vyřešit

[265] KOVÁŘOVÁ 2012, s. 44

lokální problém s výzkumným zachycením, které umožňuje opakování výzkumu v nových podmínkách, tj. přenositelnost pro řešení stejného problému v jiné lokalitě[266].

Poslední výzkum má kvalitativní formu, rozhovory s různými subjekty jsou zjišťovány názory k problematice dizertační práce i k realizované lekci (již zmíněná část akčního výzkumu). Rozhovory byly provedeny pro 360° zpětnou vazbu na vzdělávání v knihovnách o bezpečnosti digitálních stop na úrovni obecných i konkrétních (z realizované lekce vycházejících) postojů. V souladu s možnostmi a cíli kvalitativního výzkumu jsou představeny reálné názory, se kterými se lze setkat. Nelze je sice zobecňovat, ale jedná se o východisko pro vytvoření nové teorie v oblasti názorů na problematiku této dizertační práce.

Výsledkem celé výzkumné části proto bude reálný pohled na to, jak vypadá a jak by mohlo vypadat vzdělávání v českých knihovnách o digitálních stopách a jejich zneužití. Tento výsledek je jedinečný v českém prostředí, i v zahraničí nepatří řešená problematika mezi dostatečně popsané, proto její přínos není omezený na české prostředí, přestože je ovlivněn specifiky českých knihoven. Pomocí popsaných šetření bude základní výzkumná otázka zodpovězena prostřednictvím výzkumných podotázek:

PO 1. Jaký je současný stav vzdělávání v oblasti informační bezpečnosti v českých knihovnách s důrazem na digitální stopy uživatelů ICT?

PO 2. Jaká témata by měla být dále prosazována a případně doplněna s ohledem na cítění, zkušenosti a znalosti knihovníků?

PO 3. Jaké vzdělávací cíle splňuje lekce pro 4. - 5. třídu reprezentující vytvořenou metodiku vzdělávání dětí na základních školách?

PO 4. Jaká pozitiva a bariéry spatřují zainteresované osoby ve vzdělávání v knihovnách o bezpečnosti digitálních stop?

Výzkumné otázky i jednotlivá šetření na sebe navazují a navzájem podporují svůj smysl, aby bylo doloženo, že vzdělávání v knihovnách o bezpečnosti digitálních stop má smysl a je reálné. Vzhledem k této návaznosti, kdy další výzkum bylo možné zahájit až po vyhodnocení předchozího, je sice platnost nejdříve realizovaných šetření omezena jejich stářím, přesto jsou stále relevantní a představují nejaktuálnější zdroj východisek pro navazující kroky.

[266] HENDL 2008

6 Výchozí výzkumy

Jak již bylo zmíněno, vlastní výzkumná šetření stavěla na dřívějších zjištěních o českých knihovnách a vzdělávání v nich a také na vzdělávání o digitálních stopách v jiných institucích. Neexistuje sice empirický výzkum, který by mapoval problematiku řešenou v této práci, je ale dostupný dostatek dat k dílčím oblastem a souvislostem, ze kterých je vhodné vycházet při výzkumu vzdělávání v knihovnách o digitálních stopách a obraně proti jejich zneužití. Tyto poznatky jsou shrnuty před vlastní výzkumnou prací.

6.1 Bezpečnost digitálních stop

Výzkumy bezpečnosti uživatelů na internetu lze najít ve variantách zaměření na různá témata i cílové skupiny. Z hlediska tematického pokrytí s ohledem na cíl této práce nejsou zajímavá tolik šetření věnující se technickému zabezpečení počítačů (v nejširším slova smyslu), ale spíše bezpečnému chování uživatelů, které se s využitím určitých technických opatření pojí a společně mají významný vliv na podobu digitální stopy.

EU Kids Online[267] v 25 evropských státech (včetně ČR) v letech 2009-2011 pomocí rozhovorů s přibližně 1000 dětí v každém státě (a ke každému dítěti zákonný zástupce). zjišťovalo informace o rizikovém chování dětí a internetových problémech, se kterými mají zkušenosti. Výzkum se ve vzdělávání omezuje na formální, s knihovnami téměř neoperuje. Podle něj je internet běžnou součástí života dětí a sdílení informací, ať už komunikací nebo vystavováním různých typů obsahu (zprávy, fotky, přenosy či záznamy z webkamery nebo blogy). Setkání s internetovým problémem přiznalo 9 % dětí 9-10 let starých a 11 % dětí ve věku 11-12 let[268].

Mnoho problémů vychází z rizikové komunikace, představu o ní dává použití sociálních sítí. 26 % dětí ve věku 9-10 a 46 % dětí ve věku 11-12 má profil na sociální síti, z toho v mladší skupině 28 % zcela veřejný a 19 % částečně (9 %

[267] LIVINGSTONE 2011
[268] LIVINGSTONE 2011

neví). Ve starší skupině má zcela veřejný profil 26 % dětí, částečně veřejný 24 % (4 % neví). Přitom mnoho profilů obsahuje identifikující informace, 20 % dotazovaných z České republiky má součástí profilu adresu nebo telefonní číslo a v průměru 2,7 ze šesti sledovaných typů informací. Konkrétnější výsledky uvedl Microsoft[269], dle něj považuje 43 % dětí zveřejňování osobních informací na internetu za bezpečné, zpřístupňují skutečné jméno (85 %), fotografie sebe a přátel (71 %), školu (44 %) či bydliště (13 %); z 63 % dotázaných odpověděla na pokus o kontakt ze strany neznámého člověka téměř polovina. Jiný výzkum[270] srovnává rizikové chování dospívajících a dospělých na sociálních sítích dle demografických a psychologických faktorů a frekvence užívání. Nutnost osvěty v online komunikaci podporuje, že dospívající (10-19 let) byli ochotni zveřejnit 13 z 18 sledovaných osobních informací a naopak ve srovnání s dospělými statisticky méně často využívali nastavení soukromí na sociálních sítích. Téměř čtvrtina studentů na sociálních sítích si není vědoma toho, jak snadno může neznámý dospělý získat přístup k jejich osobním informacím nebo s nimi zahájit chat[271].

I v případě, že profil není veřejný a informace jsou sdíleny s omezeným okruhem lidí, může být tento natolik široký[272], že se k osobním informacím může dostat naprosto neznámý člověk. To vychází z množství kontaktů dětí a otevřenosti v sociálních sítích (informace dostupné přátelům přátel v prostředí Facebook). Oolo a Siibak[273] se zaměřili na 14-16 let staré děti, které již více využívají postupy pro uchování soukromí informací, k čemuž aplikují různorodé strategie od omezování uváděných informací pro jejich skrývání mezi dalšími zpřístupňovanými (tzv. sociální steganografie).

Sociální sítě proto mohou být snadným zdrojem informací pro internetový útok, protože z nich lze získat mnoho potřebných údajů snadno na jednom místě. Jedná se také o častý způsob komunikace dítěte, přes který je snadno dosažitelné, a který je pro něj důležitý, je proto problém se v případě útoku (např. kyberšikany) od něj odpoutat. Sociální sítě ale nepředstavují jediné rizikové prostředí, do kterého se děti často samy dostávají. Zmínit lze také např., že třetina dospívajících sdílí své

[269] Polovina dětí reaguje na internetu (...) 2010
[270] WALRAVE 2012
[271] WEEDEN 2013
[272] OOLO 2013
[273] OOLO 2013

internetové heslo s přáteli a čtvrtina neví, že obsah nahraný na internet nemůže být permanentně smazán[274].

Při zohledňování výsledků mezinárodních výzkumů je nutné postupovat uvážlivě, protože byly prokázány rozdíly mezi státy. Vzhledem k lokaci této práce jsou podstatné výsledky pro ČR, která patří ke státům, kde má nejvíce dětí zkušenost s jedním nebo více rizikovými faktory. Zanedbatelné není také její pořadí při srovnání, kolik dětí používá internet každý den a kolik se něčím na internetu cítilo poškozeno[275]. Na druhou stranu je u nich zjištěn jeden z nejvyšších průměrů množství online dovedností.

Výzkum Nebezpečí internetové komunikace[276] mapuje rizikové chování i problémy dětí (11-17 let). Podle výsledků komunikuje na internetu 53,8 % dětí s neznámými lidmi. Rizikovým je sdílení sexuálně laděných materiálů (zkušenost 5,8 % respondentů), nebo jejich odesílání jiným osobám (8,51 % respondentů), přestože za problémové to považuje 73,1 % dotázaných. Vedle těchto obsahů bylo sledováno sdílení dalších osobních informací a jejich zaslání internetovému známému na žádost (hodnoty jsou uváděné za údaji ve stejném pořadí): jméno a příjmení (80,4 %; 48,1 %), e-mail (65,8 %; 25,1 %), fotografie obličeje (58,4 %; 21,8 %), Instant Messengery (21,7 %; 15,1 %), telefonní číslo (19 %; 20,6 %), adresa školy (15,9 %; 5,2 %), rodné číslo (3,45 %; 1,5 %), heslo k e-mailovému účtu (2,4 %; 1,0 %) a PIN kód kreditní karty (1,3 %; 1,0 %). Žádný ze sledovaných údajů nesdílí na internetu 9,6 % dětí a neodešle na žádost 23,3 % dětí. V reálné situaci fotku obličeje požadoval někdo přes internet od 30,5 % dětí a pozitivně reagovalo 52,2 % z nich, což je vyšší hodnota, než byla deklarována sebehodnocením. Ve sledovaných třech letech se množství sdílených i na žádost odeslaných dat (mimo jméno a příjmení) snižuje. Zajímavým výsledkem je, že 30,3 % respondentů do 18 let o sobě na internetu říká vždy pravdu a naopak 2,4 % respondentů absolutně věří tomu, co jim o sobě někdo na internetu říká. Oba údaje vypovídají o silném riziku v chování dětí.

[274] JOINER 2005
[275] LIVINGSTONE 2011
[276] KOPECKÝ 2012

6.2 Vzdělávání o internetové bezpečnosti

Jak vyplývá z předchozí kapitoly, děti se setkávají s problémy často důsledkem vlastního rizikového chování. S ohledem na omezenou možnost použití a snadnost obcházení bezpečnostních opatření proti internetovým útokům v podobě legislativy a technických řešení, se jako stěžejní ukazuje osvěta pro zvýšení internetové bezpečnosti (nejen v případě dětí)[277]. Zejména problémům založeným na rizikové komunikaci lze předcházet někdy jen bezpečným chováním. Předpokladem je znalost vhodných modelů chování, jejichž využití je podmíněno uvědoměním si možných důsledků. Podstatná je tedy znalost internetových hrozeb i protiopatření.

Mezi státy jsou silné rozdíly i ve vzdělávání o internetové bezpečnosti. Srovnání evropských států vytvořil Ranguelov[278], problém je ale s aktuálností výsledků, protože vychází z údajů za rok 2008/2009. Jedná se o nové téma ve vzdělávání a státy teprve hledají cestu, jak jej zařadit. Ze šesti nejčastěji řešených témat je pět rizikovou komunikací či jejím důsledkem (od nejčastějšího: bezpečné chování online, otázky soukromí, kontakt s cizími lidmi, kyberšikana, bezpečné použití mobilních telefonů). Každý stát má odlišný přístup k stanovování způsobu a povinnosti pokrytí témat ve vzdělávání. V České republice je formální školství postaveno na Rámcových vzdělávacích programech, které dávají velkou volnost v pojetí internetové bezpečnosti. Toto nedostatečné ukotvení akcentuje i Kopecký a kol.[279], kteří vidí východisko v kombinaci přímé edukace, mediálních kampaní a pozitivních vzorců chování rodičů, učitelů a vrstevníků. Ranguelov[280] upozorňuje, že celou výuku třídy na 1. stupni zajišťuje jeden učitel, je tedy pravděpodobné, že se obvykle nejedná o odborníka na IT (to se potvrdilo na škole v případové studii, viz kap. 9). Na vyšších stupních je již IT specialista obvyklý, je ale stále otázkou jeho erudovanost v internetové bezpečnosti. Vedle toho existují nabídky neformálního vzdělávání, a to ve spolupráci se školami či zcela mimo ně. Je tedy pravděpodobné, že různé lokality v ČR se budou v tomto směru lišit, neexistuje ale výzkum, který by rozdíly zmapoval. Toto omezení je nutné brát v úvahu i při

[277] RANGUELOV 2010; LIVINGSTONE 2009; MARTIN 2012; KOPECKÝ 2012
[278] RANGUELOV 2010
[279] KOPECKÝ 2012
[280] RANGUELOV 2010

hodnocení kvantitativných výsledků v oblasti vzdělávání o internetové bezpečnosti pokrývajících celou Českou republiku.

Výzkumy vzdělávání o bezpečnosti na internetu se často zaměřují na formální vzdělávání, i při tom se ale ve výsledcích částečně objevují instituce neformálního vzdělávání, včetně knihoven[281]. Hlubší pozornost jim však není věnována. Problém zkoumání jejich postavení ve vzdělávání o internetové bezpečnosti je spojen s omezeními kvantitativních výzkumů, pokud totiž jejich činnost není součástí zkoumaných variant, jejich aktivita se do výsledků nemůže dostat. To je možná důvodem, proč lekce internetové bezpečnosti v českých knihovnách nezmiňuje Ranguelov[282], přestože se v době sběru dat pro jeho šetření (2008/2009) realizovaly. Mimo dílčí lekce byly knihovny zapojeny do mezinárodního Safer Internet Day. Tuto akci Ranguelov[283] zdůrazňuje jako možnost spolupráce institucí na osvětě v oblasti internetové bezpečnosti. Neodmítá ani knihovny, jak je patrné na jeho popisu situace v Řecku. Je tedy pravděpodobné, že české (a pravděpodobně i další) knihovny se do šetření nedostaly z výše uvedeného důvodu, než že by nebyly v zájmu výzkumníka.

Knihovny díky spolupráci s více školami v okolí mohou pokrýt poměrně rozsáhlou skupinu dětí. Právě šířku pokrytí osvěty zdůrazňují Moreno a kol.[284], měla by ale být spojena se zkušenostmi ve výuce o internetu a příbuzných tématech. Přestože knihovníci nemají akreditované pedagogické vzdělání, toto téma se v ČR dostává do jejich odborné přípravy (vyučuje se např. od jara 2014 na Kabinetu informačních studií a knihovnictví Masarykovy univerzity), jsou nabízeny kurzy dalšího vzdělávání pro knihovníky a zkušenosti získávají často z praxe. Může se tak stát, že praktických zkušeností s výukou o internetu a příbuzných tématech má knihovník více než učitel na prvním stupni.

Martin a Rice[285] knihovny zahrnují jako jeden z prvků spolupracujících se školou, příp. jako její součást u školních knihoven (ty mají v ČR jiné postavení než v angloamerickém prostředí, kde vykonávají podobné činnosti jako veřejné knihovny v ČR při neformální spolupráci se školou). V tomto pojetí je celá skupina pracovníků ve vzdělávání (ředitelé, učitelé, knihovníci) považována za klíčovou pro

[281] RANGUELOV 2010; MARTIN 2012
[282] RANGUELOV 2010
[283] RANGUELOV 2010
[284] MORENO 2013
[285] MARTIN 2012

zvýšení internetové bezpečnosti dětí. Podle 47 % respondentů musí spolupracovat s rodiči pro zajištění adekvátní bezpečnosti dětí.

Na zásadním postavení rodičů se výzkumy shodují, ať už se zaměřují na názory rodičů, dětí či učitelů. Podle Moreno a kol.[286], zkoumající všechny tyto tři skupiny a klinické lékaře, 40,3 % respondentů uvádí, že o internetové bezpečnosti by měli pravidelně učit děti rodiče, ti jsou za to primárně zodpovědní, jen podle 20,8 % by to měli dělat učitelé. I zde je z konkretizace demografických dat patrné, že mezi učitele jsou řazeni také knihovníci. Na druhou stranu při dotazování dospívajících, od koho se dozvídali o problematice, jsou na prvním místě učitelé (87,5 %), následovaní rodiči (75 %). Fungování rodičů jako zdrojů osvěty je tedy v praxi méně časté, což je podle Moreno a kol.[287] ovlivněno nedostatečnými zkušenostmi rodičů v této oblasti, především ve srovnání s *digital natives*. Rodiče by ale většina učitelů a klinických lékařů chtěla doplňovat a také by podle Moreno a kol.[288] měla, a to kooperativním způsobem.

Kromě omezení rodičů v jejich zkušenostech s internetovou bezpečností je limitem při vzdělávání přesvědčení, že se problém jejich dětí netýká. Liší se ale názory rodičů a dětské zkušenostmi s problémem (vidění či přijmutí obrázků se sexuálním obsahem, přijímání sprostých či zraňujících zpráv přes internet a setkání off-line s člověkem známým jen z internetu).[289] Přesto se podle stejného šetření většina rodičů snaží aplikovat různé mediační strategie[290] pro zvýšení bezpečnosti dětí na internetu. Přístup rodičů ale nestačí pro řešení bezpečnosti dětí, protože 37 % dětí ignoruje rodiče (málo nebo hodně), ČR je v tomto s 54 % dětí na 1. místě[291]. Postavení rodičů, jako zdrojů osvěty, oslabuje také to, že 50 % z nich nesleduje u dětí dodržování pravidel pro ochranu soukromí na sociálních sítích[292]. To formuje nezanedbatelnou skupinu, pro kterou je nutné hledat jiné formy osvěty. Současně se zde objevuje náznak toho, co zdůrazňují Walreve a kol.[293], tedy že nejde jen o to, aby byly děti a dospívající vzděláváni o internetové bezpečnosti, klíčové je také zahrnout zásadní subtémata, včetně budování digitální stopy, důsledků

[286] MORENO 2013
[287] MORENO 2013
[288] MORENO 2013)
[289] LIVINGSTONE 2011
[290] Podrobněji viz kap. 3 Informační bezpečnost v knihovně se zaměřením na digitální stopy
[291] LIVINGSTONE 2011
[292] Polovina dětí reaguje na internetu (...) 2010
[293] WALRAVE 2012

zveřejňování konkrétních informací a řízení soukromí (*privacy management*). Toto tvrzení si jako hypotézu potvrdili i Weeden a kol.[294]

Mezi informačními zdroji o online bezpečnosti pro děti Livingstone a kol.[295] identifikovali vedle rodičů (63 %), učitelů (58 %) a vrstevníků (44 %) další, mezi nimiž je na 5. místě knihovna. Význam roste s ochotou těchto institucí zapojovat se do celoživotního vzdělávání. Zájem vzdělávat místní komunitu i o internetové bezpečnosti se neřeší jen v České republice, podobné iniciativy je možné sledovat i v USA[296]. Zájem je naopak problematický, když je role v celoživotním vzdělávání přisuzována českým školám, jak zjistily Rabušicová a kol.[297]

Přestože existují výzkumy názorů, kdo by měl vzdělávat děti o internetové bezpečnosti, i nabídky, „*několik organizací, včetně AAP [American Academy of Pediatrics], nabízelo odborné poradenství týkající se bezpečnosti na internetu, ale přístup založený na důkazech vzdělávat mládež o nebezpečí bytí online, v současné době neexistuje.*“[298] V České republice lze zmínit edukaci programem e-Bezpečí, který pro osvětu využívá rozbory kazuistik z ČR i zahraničí[299]. Výše zmíněny byly také důvody, proč by vzdělání v této oblasti mělo být kooperativní i proč by do něj měly být zapojeny knihovny, příp. další instituce neformálního vzdělávání. Je tedy vhodné podrobit vzdělávání v tomto směru dalším šetřením, aby bylo možné hovořit o přístupu založeném na důkazech (evidence-based approach), který je předmětem výzkumné části této práce.

6.3 České knihovny a vzdělávání

Výzkumy realizované v rámci dizertační práce stavěly mj. na výsledcích každoročního statistického vykazování knihoven, které zpracovává Národní informační a poradenské středisko pro kulturu (NIPOS). Pro první výzkum byl s ohledem na dobu jeho realizace výchozí stav v roce 2010, jelikož se ale jedná o každoroční šetření a ostatní výzkumy následovaly v dalších letech, budou zde

[294] WEEDEN 2013
[295] LIVINGSTONE 2011, s. 127
[296] MARCOUX 2010
[297] RABUŠICOVÁ 2004
[298] MORENO 2013
[299] KOPECKÝ 2012

představeny výsledky od roku 2010 do 2012[300] (s ohledem na dobu publikování výsledků za předchozí rok se jedná o nejnovější statistiky v dané době). Toto sledování až do současnosti umožňuje reflektovat výsledky nejen s ohledem na prostředí v době realizace výzkumu, ale i v době publikování práce. Z podobného důvodu jsou představeny také výsledky výzkumu Názory uživatelů na přínosy informačních a komunikačních technologií ve veřejných knihovnách v České republice[301], které byly publikovány v roce 2013. Neovlivnily tedy vznik vlastních šetření, ale jsou významné pro interpretaci výsledků s ohledem na současné prostředí, a to i ve srovnání s dalšími státy Evropy.

Základní přehled o statistických údajích lze vytvořit pomocí každoročních výkazů odevzdávaných knihovnami na základě vyhlášky Ministerstva kultury ČR[302]. Lze předpokládat, že ne všechny knihovny údaje poskytují, mělo by se však jednat o výjimky. Z publikovaných informací je zřejmé, že široká síť knihoven je tvořena především těmi s neprofesionálními knihovníky, jejich vybavení a služby jsou ale výrazně horší než u těch s profesionálními knihovníky[303], kde rostoucí velikost instituce je nepřímo úměrná počtu knihoven, ale přímo úměrná množství vybavení a služeb, včetně vzdělávacích (viz tabulka 1). Hustota knihovní sítě je v České republice nesrovnatelně vyšší než představuje evropský průměr – na 10 000 obyvatel připadá v ČR 5,1 knihoven, zatímco v EU je to 1,3 knihovny[304].

Tabulka 1 Vybavení a služby v roce 2012 podle typu knihovny[305]

	NK	MZK	Krajské	Základní s reg. funkcí	Další zákl. profes.	Další zákl. neprofes.
Knihoven	1	1	13	86	694	4605
Návštěvníků na internetu (v tis.)	182	251	440	846	943	282
Vzdělávacích akcí pro veřejnost	69	148	4225	14379	9068	1333
Návštěvníků vzdělávání (v tis.)	9	1	92	264	227	25

Knihovny poskytují nezanedbatelnému množství lidí přístup k internetu. Proti evropskému prostředí, kde převažuje motivace v bezplatnosti služby a absenci

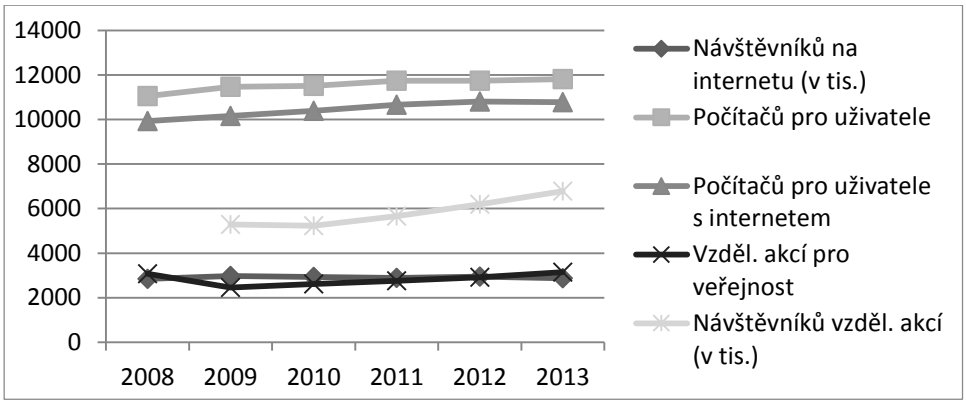
[300] Základní statistické údaje o kultuře v České republice 2012 2013
[301] QUICK 2013
[302] Statistika kultury © 2007
[303] Ve statistice takto nejsou rozlišováni pracovníci dle vzdělání, za neprofesionální je NIPOS označuje, pokud vykonávají svou činnost v knihovně jako dobrovolní knihovníci (ne jako profesi).
[304] QUICK 2013, s. 8
[305] Dle Základní statistické údaje o kultuře v České republice 2012 2013

jiných možností, v ČR jsou uváděny spíše poradenství zaměstnanců a pomoc od jiných uživatelů[306]. Poradenství se objevuje jako významné i při řešení různých služeb a oblastí spojených s prací s informačními technologiemi. Proto je zásadní, aby knihovníci byli pomocníky při řešení problémů. Měli by se tudíž orientovat, vzdělávat a dokázat poradit i v oblasti bezpečnosti na internetu, včetně problematiky digitálních stop. Vzhledem k tomu, že uživatelé v tomto případě neřeší technické zabezpečení (to je záležitostí knihovny), jsou problémy spojeny právě s jejich chováním na internetu, tedy především vytvářením digitálních stop.

Co se týče vzdělávacích aktivit a účastníků na nich, je zarážející nepoměr dvou největších knihoven, kdy Moravská zemská knihovna vykazuje výrazně více akcí než Národní knihovna, ale v počtu návštěvníků je rozdíl obrácený[307]. To zřejmě vyplývá z odlišného přístupu, kdy Moravská zemská knihovna nabízí spíše komornější akce proti masovým v Národní knihovně. Ostatní knihovny jsou vyrovnané v zjištěném průměru 18-25 osob na jednu vzdělávací akci. V průměru nejvíce vzdělávacích akcí nabízí krajské knihovny (325/knihovna), následovány menšími knihovnami – základními pověřenými regionálními funkcemi (167/knihovna), základními s profesionálními pracovníky (13/knihovna) a základními s profesionálními pracovníky (0,3/knihovna). Z těchto výsledků jasně vyplývá, že pokud mají být zkoumány, ale také rozvíjeny vzdělávací akce knihoven, je vhodné se zaměřit především na knihovny s regionálními funkcemi (dle knihovního zákona a jimi pověřené), protože ostatní knihovny vzdělávají spíše výjimečně a změny s největší pravděpodobností převezmou až po ověření knihovnami, které mají širší prostor pro realizaci v této oblasti. Tyto výsledky ovlivnily stanovení cílové skupiny pro rozšiřující výzkum popsaný v kap. 7.2.

Při pohledu na vykázané vývojové tendence dle NIPOS roste „*počet návštěvníků knihoven, kteří využívají i další informační možnosti knihoven, především služby internetu, a kulturní a vzdělávací pořady.*“[308] Stejnou tendenci je možné sledovat již od 2008. Pozitivní vývoj můžeme vysledovat v oblastech souvisejících s tématem této práce, které znázorňuje graf 2.

[306] QUICK 2013, s. 12-14
[307] Základní statistické údaje o kultuře v České republice 2012 2013
[308] Základní statistické údaje o kultuře v České republice 2012 2013



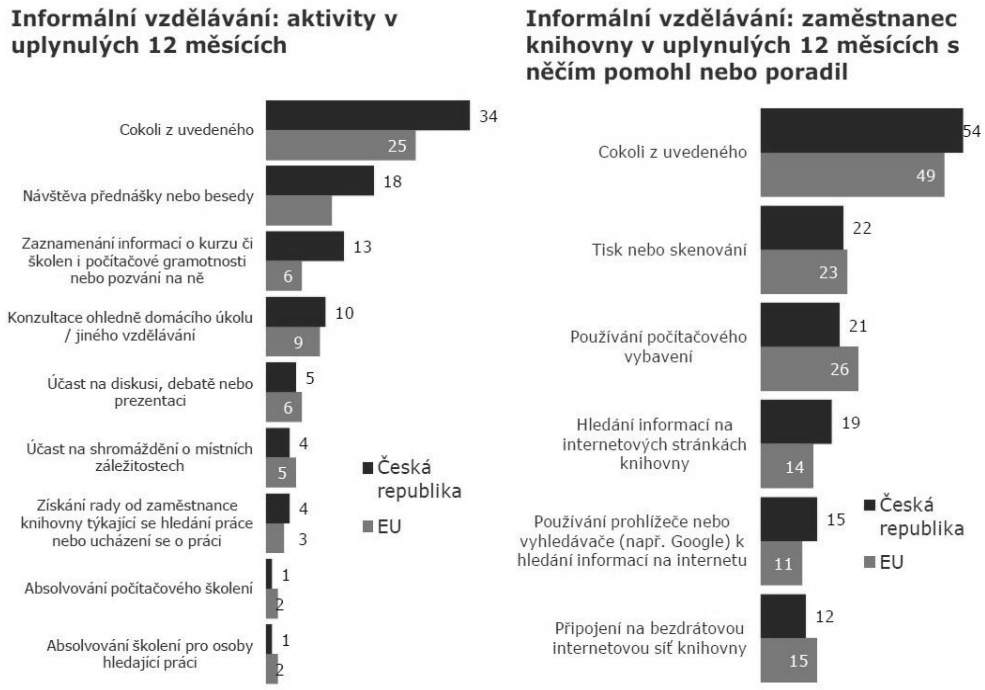
Graf 2 Vývoj vybavení a vzdělávacích akcí v knihovnách[309]

Z grafu 2 lze vyvodit stabilní počet návštěvníků využívajících internet, přestože ve sledovaném období výrazně vzrostl počet domácností připojených k internetu[310]. Lze tedy očekávat, že i v nejbližších letech bude dostatek zájemců o internet v knihovnách, přestože se bude rozšiřovat připojování domácností. Je možné, že stabilita zájmu je důvodem stability vybavení knihoven, protože počet počítačů vykazuje jen slabě rostoucí tendenci, o málo silnější je nárůst připojení k internetu. Z těch, kdo využili internet v knihovně, to 35 % udělalo pro aktivity spojené se zaměstnáním a 23 % ke komunikaci s veřejnou správou (17 % získání informací z internetových stránek, 9 % stahování úředních formulářů a 9 % množství odeslání vyplněných formulářů)[311]. Vzhledem k důležitosti těchto činností pro uživatele je nezbytné, aby byla zajištěna jejich bezpečnost.

Znatelnější růst po počátečním poklesu vykazuje oblast vzdělávacích akcí. Těch dle NIPOS[312] od roku 2009 rovnoměrně přibývá (cca o 1500 akcí za rok) s odpovídajícím růstem počtu uživatelů knihovny, kteří se jich účastní (cca o 50 000 za rok). Díky tomuto růstu se knihovnám rozšiřuje nabídka, která by neměla spočívat jen v navýšení akcí stejného typu, ale je zde prostor i pro nová témata odpovídající současným potřebám uživatelů. Lze tedy konstatovat, že existují podmínky pro zavedení či rozšíření problematiky digitálních stop a jejich zneužití. Při srovnání návštěvnosti vzdělávacích akcí v evropském prostředí ČR s 34 % uživatelů knihoven, kteří se zúčastnili vzdělávací akce v knihovně, převyšuje

[309] Dle Základní statistické údaje o kultuře v České republice 2012 2013
[310] See the evolution of an indicator and compare breakdowns 2014
[311] QUICK 2013, s. 23-24
[312] Základní statistické údaje o kultuře v České republice 2012 2013

evropský průměr (25 % uživatelů)[313]. Co se týká obsahového zaměření i formy vzdělávacích aktivit v knihovně, jsou velmi různorodé a pro téma této práce spíše orientační v mapování vzdělávání a poradenství o práci s počítačem a internetem, graf 3 ilustruje množství informálních vzdělávacích aktivit, které návštěvníci v uplynulých 12 měsících absolvovali nebo o nichž se dozvěděli.



Graf 3 Informální vzdělávací aktivity využité za rok[314]

Organizace, které mají nejblíže k tématu této dizertační práce, jsou IVU SDRUK a komise IVIG. Obě realizují v rámci své činnosti výzkumná šetření[315], která prozatím reflektují téma informační bezpečnosti minimálně. Tvoří výchozí informační pozici pro dále představené výzkumy, protože popisují obsah vzdělávacích aktivit českých knihoven. IVIG se zaměřuje na prostředí vysokoškolských knihoven, zatímco IVU cílí na knihovny, které nejsou specializované, ale slouží celé veřejnosti bez tematického zaměření služeb.

Ve vysokoškolském prostředí[316] se přihlásilo jen 40 % respondentů k realizaci informačního vzdělávání v dlouhodobých plánech škol, ale 73,3 %

[313] QUICK 2013, s. 19
[314] QUICK 2013, s. 20
[315] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012; LANDOVÁ 2010
[316] LANDOVÁ 2010

v rozvojových projektech. Pozitivní je, že více než polovina respondentů (53,3 %) vykazuje existenci koordinátora informačního vzdělávání, čímž knihovna ukazuje své přesvědčení o významu této služby. Podobná pozice ve veřejných knihovnách v rozhovorech byla deklarována jako nedostatečně uznaná a zavedená (viz kap. 9.4.2), což nepřímo vyplývá také z výzkumu IVU. Tento problém není výrazný u krajských a pověřených knihoven, které prezentují častěji systematické informační vzdělávání žáků a studentů středních škol, přestože je otázkou, zda se opravdu jedná o naplnění tohoto označení nebo pouhé diskuze nad souvisejícími tématy. U menších profesionálních knihoven je problém evidentnější, především s ohledem na omezené profesionální možnosti (jeden až dva pracovníci)[317]. Kromě množství vzdělávacích aktivit a zájmu knihoven a knihovníků o rozvoj těchto služeb je pro téma této práce zásadní obsahová náplň vzdělávacích aktivit v knihovnách. Z 15 vysokoškolských knihoven, které byly výzkumu[318] podrobeny, je jasné zaměření na tradiční služby knihovny a práci s informacemi, která není významněji ovlivněna aktuálním vývojem informačních technologií a oblastmi blízkými tématu této dizertační práce, což ilustruje tabulka 2.

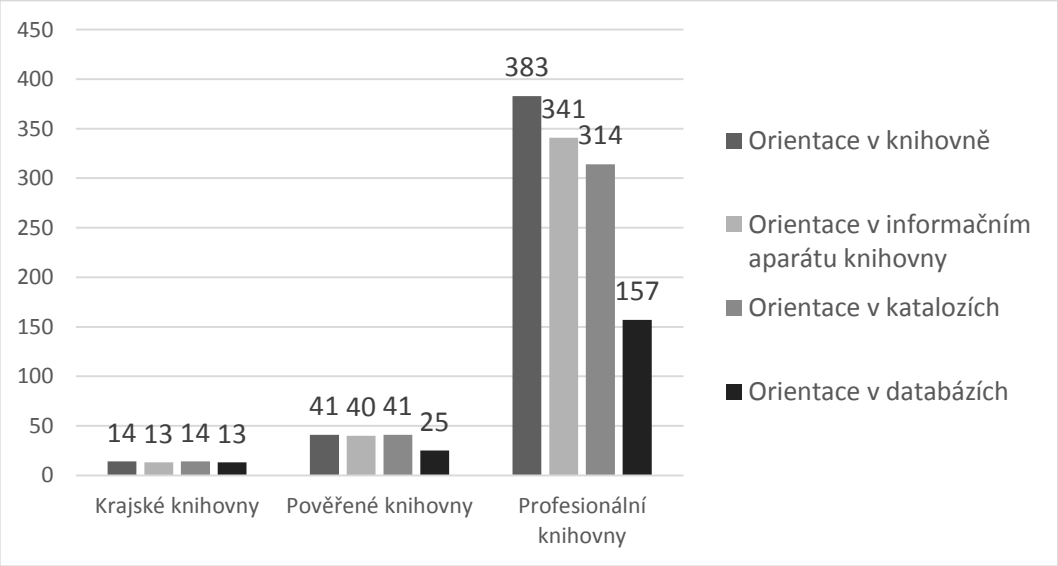
Tabulka 2 Témata vzdělávacích akcí ve vysokoškolských knihovnách[319]

Témata vzdělávacích akcí	Počet výskytů
vyhledávání v katalogu (katalozích)	15
služby knihovny obecně	15
vyhledávání v databázích	14
citační rejstříky	14
rešeršní strategie	13
citování	12
psaní odborných textů, diplomových a bakalářských prací	11
prevence plagiátorství	11
citační manažery a generátory citací	10
repozitáře VŠKP	7
normy	7
patenty	5
jiná	5

Ve vysokoškolském prostředí tedy nejsou dostupné výchozí informace pro výzkum vzdělávání v knihovnách o digitálních stopách a jejich zneužití. Knihovny ale mají poměrně jasnou a sdílenou představu o obsahové náplni lekcí. Horší situace

[317] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012, s. 42
[318] LANDOVÁ 2010
[319] LANDOVÁ 2010

je mezi nespecializovanými knihovnami, kde převažuje nevědomost knihovníků, co má být obsahem vzdělávání jednotlivých věkových skupin a jakými metodami má být jejich učení realizováno[320]. Na druhou stranu je pozitivní, že si knihovníci tento stav uvědomují, stejně jako častou zastaralost výukových materiálů, díky čemuž také vykazují zájem o metodické materiály, které by jim pomohly tento nedostatek redukovat. I přes tento stav informační vzdělávání v knihovnách realizováno je, ještě výrazněji je zde ale patrný sklon k tradičním tématům, jak ukazuje graf 4 Obsah informačního vzdělávání v nespecializovaných knihovnách, což ale není hodnoceno jako pozitivní, jak naznačuje komentář Nejezchlebové[321].



Graf 4 Obsah informačního vzdělávání v nespecializovaných knihovnách[322]

Knihovny tedy mají prostor i důvod věnovat se vzdělávání o digitálních stopách a jejich zneužití. Přesto se stále realizují a zkoumají spíše tradiční témata, která patří do nejužšího jádra informační gramotnosti. Pro rozvoj tématu této práce je proto nutné vlastní výzkumné šetření, ale i vytvoření praktické koncepce vzdělávání o problematice digitálních stop a jejich zneužití, aby bylo možné se zabývat jeho řešením v praxi. Tyto cíle jsou naplněny v následujících kapitolách.

[320] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012, s. 43
[321] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012, s. 45-47
[322] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012, s. 45

7 Prostředí českých knihoven pro vzdělávání o bezpečnosti digitálních stop v letech 2011-2013

Jak již bylo uvedeno, neexistuje empiricky podložený popis, jakým způsobem a v jakém rozsahu knihovny vzdělávají své uživatele v tématech souvisejících s touto prací. Předtím, než tedy bylo možné zaměřit se na možnosti vzdělávání v českých knihovnách o digitálních stopách, bylo nezbytné udělat si představu o kontextu, příležitostech a omezeních, které ovlivňují možnosti nasazení navržené vzdělávací koncepce. Postupně byly v letech 2011-2013 realizovány tři na sebe navazující výzkumy, které mapovaly připravenost českých knihoven na nasazení vzdělávací koncepce o digitálních stopách. Tyto tři výzkumy společně naplňují první cíl této dizertační práce, který spočívá ve vymezení reálné situace a využitelných možnosti v knihovnách pro vzdělávání uživatelů o digitálních stopách. Současně představují nezbytná východiska pro druhý cíl práce, který definuje efektivní využití zjištěných možností.

7.1 Deskriptivní mapování prostředí

Pro empirické zkoumání problematiky této dizertační práce bylo nutné nejdříve zmapovat prostředí českých knihoven ve vztahu ke vzdělávání o digitálních stopách. Deskripce vzdělávacích aktivit českých knihoven je nedostatečně zpracovaná a v době plánování výzkumných šetření pro tuto práci neexistoval dostatek výzkumných zpráv. Jen omezeně mohla nabídnout některá východiska výzkumná šetření popsaná v kap. 6.3. V jejich rámci toho ale nebyla nikde věnována pozornost samostatně informační bezpečnosti, která představuje širší okruh zde řešené problematiky.

Prvotním cílem dále popsaných empirických šetření bylo proto popsat postavení tématu informační bezpečnosti v rámci vzdělávacích aktivit českých knihoven. Úmyslně byla pozornost rozšířena od digitálních stop na širší oblast. V období realizace výzkumu totiž nebylo zcela jasné, zda se knihovny této problematice věnují třeba jen částečně, a pokud ano, z jakých pohledů a v jakém rozsahu s ohledem na ostatní témata, které knihovny do vzdělávání svých uživatelů zařazují. Právě tato kritéria byla shrnuta do výzkumné otázky deskriptivního

výzkumu: Jak je v současnosti zahrnováno téma informační bezpečnosti do vzdělávacích aktivit knihoven? V rámci toho byla dále stanovena výzkumná podotázka, která se zaměřila na danou oblast pro dětské uživatele knihovny s ohledem na další výzkumy v této dizertační práci.

7.1.1 Metodologie úvodního šetření

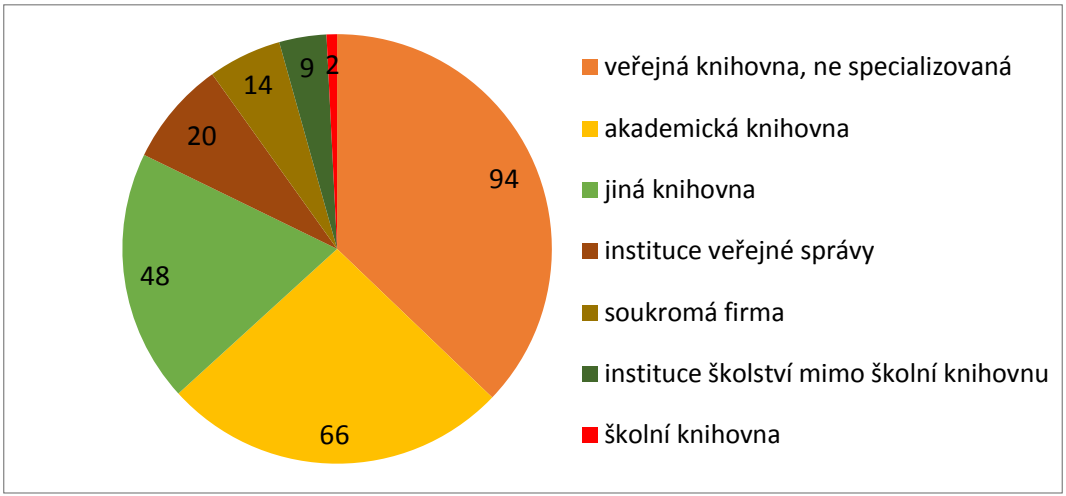
Vzhledem k výzkumné otázce nebylo přistoupeno k náhodnému výběru, protože smyslem bylo spíše získat představu o dalším zacílení výzkumu a zda má vůbec smysl se této problematice věnovat. Bylo ale nutné oslovit co nevíce možných respondentů a pro získání co nejkomplexnějšího obrazu, tedy přiblížit se celé populaci. Protože ale nemá smysl dotazovat se na tuto problematiku např. v oddělení katalogizace, výzkum cílil zejména na knihovníky, kteří se zabývají informačním vzdělávání. I to byl problém při náhodném výběru – dosud neexistuje ani orientační seznam institucí nebo dokonce knihovníků, kteří se této problematice věnují, není ani jasné, kolik jich přibližně může být.

Původní záměr oslovit jen knihovníky věnující se informačnímu vzdělávání byl v první vlně realizován přes výše uvedené organizace sdružující takto zaměřené knihovníky (zde byly o distribuci požádány Hana Landová za IVIG a nejdříve Veronika Peslerová a následně kvůli její nepřítomnosti Jana Nejezchlebová za IVU SDRUK). S ohledem na malou návratnost a se zvážením výše uvedených problémů se stanovením výzkumného vzorku a pokrytí celé ČR bylo následně přistoupeno k co nejplošnějšímu oslovování respondentů přes elektronické knihovnické konference (Andersen, AKM, Drtina, Knihovna, členů ČIS, SKIP, Výchova). Z hlediska populace a výběru vzorku je proto toto šetření možné označit jako cenzus s malou návratností.

Pro sběr dat byl využit elektronický dotazník v aplikaci Survs, jeho přesné znění je uvedeno v příloze 1.1. V souladu s principy deskriptivního výzkumu nebyly stanoveny výzkumné hypotézy, ale pouze již uvedené výzkumné otázky určující zaměření výzkumu na postavení tématu informační bezpečnosti ve vzdělávacích aktivitách knihoven, a to v obecném pojetí a dále obdobně se zaměřením na děti. Proto byly dotazy kladeny tak, aby bylo zjištěno, kolik knihoven se věnuje nabídnutým širokým tematickým oblastem, které byly dále konkretizovány k informační bezpečnosti. Protože nebylo jasné, zda se toto téma

v již aktuální nabídce objeví, byly dále kladeny dotazy na názor respondentů na knihovny jako instituce vzdělávající o informační bezpečnosti. Jiný pohled na situaci měla přinést otázka k znalosti informačních zdrojů na toto téma, protože znalost problematiky je základním předpokladem pro další vzdělávání.

Před distribucí dotazníku bylo realizováno pilotní šetření, na základě kterého bylo upřesněno znění otázek a odpovědí pro jednoznačné chápání. Pro respondenty byl anonymní dotazník přístupný v období 8. - 19. 8. 2011, získáno bylo 180 kompletně vyplněných a 81 nekompletních responsí, po vyčištění bylo možné pracovat celkem s 253 responsemi. Pro interpretaci je zásadní informace o typech institucí zastoupených ve výzkumu, které ilustruje graf 5. Z něj je patrná převaha knihoven podle knihovního zákona (82,2 % respondentů). Ostatní instituce se do dotazníku dostaly s ohledem na oslovování přes knihovnické organizace a elektronické konference pravděpodobně proto, že s knihovnami spolupracují nebo je pro jejich činnost aktivita knihoven důležitá. Protože ale odpovědi mohou zkreslit výsledky mapující činnost, názory a znalosti knihovníků, byli respondenti nepracující v knihovnách z dalšího hodnocení výsledků vyřazeni.



Graf 5 Typ instituce ve výzkumu

Srovnání skupiny respondentů s populací je složité. Lze jej použít jen knihovny, které jsou evidované dle knihovního zákona, díky čemuž o nich existují oficiální statistiky. Na základě posledních publikovaných výsledků[323] je možné alespoň částečné vyhodnocení. Výzkum se uskutečnil v roce 2011, kdy bylo

[323] Základní statistické údaje o kultuře v České republice 2012 2013

evidováno celkem 5408 knihoven, z toho 791 zaměstnávající profesionální pracovníky. Při srovnání celkového počtu knihoven s 210 responzemi knihoven, z nichž některé nejsou evidovány podle knihovního zákona a některé pochází ze stejné knihovny, se může zdát zastoupení poměrně malé. Pokud ale zohledníme, že většina knihoven s neprofesionálními knihovníky se nezapojuje do elektronických konferencí, je již poměrové zastoupení zajímavější a výsledky mohou sloužit k účelu, pro který byl dotazník vytvořen.

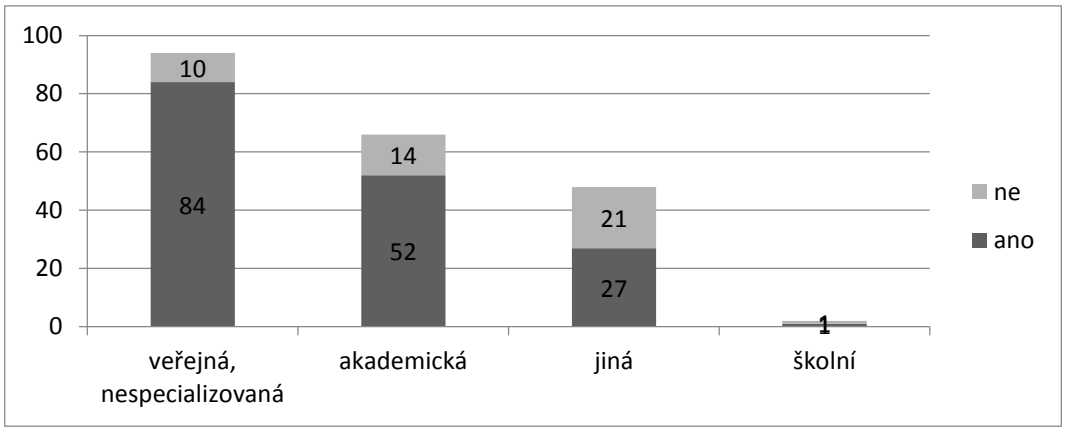
Po získání byla data zpracovávána v nástroji SPSS, pro grafickou úpravu byl použit MS Excel 2010. Cíl výzkumného šetření v popisu postavení informační bezpečnosti ve vzdělávání v českých knihovnách byl stanoven proto, aby bylo pro další práci zřejmé, zda již lze stavět na něčem, co knihovny dělají a využít jejich dosavadní zkušenosti, nebo je nutné začít od budování základů a přesvědčit o smyslu zařazení do vzdělávacích aktivit knihoven. Protože snahou bylo oslovit celou populaci pro výzkumný záměr, jsou dále představeny výsledky zpracované především deskriptivní statistikou. Vzhledem k tomu, že téměř všechny proměnné byly nominální, a také proto, že nebyl realizován náhodný výběr, jsou omezené možnosti statistického zpracování výsledků a jejich vypovídací hodnota. Přesto k nim bylo přistoupeno, kde byly zjištěny výsledky nečekané nebo přínosné pro další postup v této práci.

7.1.2 Výsledky výzkumu

Výsledky výzkumu jsou rozděleny s ohledem na východiska a cíle dotazníku. Nejdříve je popsán kontext vymezením celé nabídky vzdělávání s postupným směřováním k tematické náplni. Následně je omezena pozornost na řešenou problematiku, zde, jak bylo zdůvodněno, na informační bezpečnost. Vzhledem k rychlým proměnám v tématu a již existující nabídce využitelných materiálů byla krátce zjišťována i znalostní vybavenost, v tomto případě na úrovni osvětových informačních zdrojů k tématu informační bezpečnosti. V závěru je prostor věnován i tomu, co respondenti považovali za podstatné v řešené oblasti, ale dotazníkem to nebylo pokryto. Této možnosti využilo jen několik málo zájemců, výsledky ale přinesly zajímavé podněty do dalších šetření.

7.1.2.1 Nabídka vzdělávání a základní témata

Protože se šetření zaměřilo na popis praktické podoby vzdělávání, bylo stěžejní identifikovat zaměstnance instituce organizující vzdělávací aktivity mimo další vzdělávání vlastních pracovníků. Tím došlo k vyčlenění 46 účastníků šetření, kteří vyjadřovali jen názor na problematiku, proti 164 respondentům, kteří poskytli také osobní zkušenost. Poměry nabídky vzdělávacích aktivit dle jednotlivých typů institucí, ilustrované grafem 6, ukazují převahu veřejných knihoven, které nejsou dle knihovního zákona specializované. Akademické knihovny, mezi které patří mj. vysokoškolské, vykazují poměrově větší zastoupení vzdělávacích aktivit, než uvádí výzkum IVIG[324], což může být tím, že jsou uvedeny i lekce mimo informační vzdělávání (např. dle studijních oborů), pokud ale relativní četnost porovnáme s projekty rozvíjejícími informační gramotnost, rozdíl není výrazný (5,5 %). Výraznější rozdíly v zastoupení vzdělávání v knihovnách se objeví při srovnání typů instituce se zaměřením na děti, kde z 62 respondentů, kteří se k němu přihlásili, 80,6 % představují veřejné knihovny, ostatní zástupci jsou jen v řádu jednotek, což odpovídá primárním cílovým skupinám specializovaných knihoven.



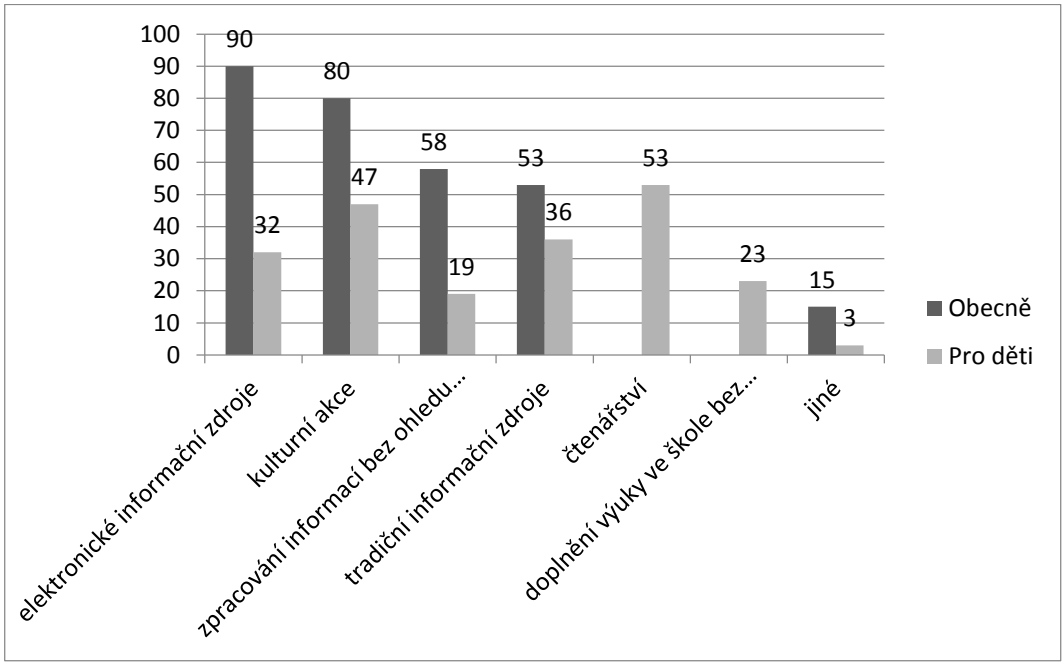
Graf 6 Vzdělávání v jednotlivých typech knihoven

Zásadní bylo mapování témat vzdělávacích akcí v knihovnách, které již nepodléhá statistickému zjišťování státu. Přitom tematická náplň značně ovlivňuje smysluplnost aktivit a jejich důsledky pro jednotlivce. Jak bylo zmíněno v kap. 7.1, částečně je oblast pokryta výzkumy knihovnických organizací zaměřených na vzdělávání, které ale nepřináší odpovědi k tématu této práce. Protože byly

[324] LANDOVÁ 2010

zjišťovány téměř stejné údaje v obecném pojetí a následně s ohledem na výzkumnou podotázku se zaměřením na děti, pro možné srovnání jsou dále popisovány výsledky pro obě tato zacílení společně.

Jak bylo zdůvodněno, téma digitálních stop bylo pro potřeby šetření rozšířeno na informační bezpečnost, která spadá do práce s informacemi v elektronickém prostředí. Výzkum se proto zaměřil nejdříve na to, do jaké míry knihovny do vzdělávání zařazují postupně tyto dva širší okruhy. Důvodem bylo, že pokud by klíčové téma výzkumu nebylo v knihovnách řešeno, bylo by možné stavět alespoň na širší oblasti. Základní členění vzdělávacích aktivit v knihovnách podle prostředí pro práci s informacemi ilustruje graf 7.



Graf 7 Základní kategorie obsahu vzdělávání v knihovnách

Při vědomí počtu dotazovaných realizujících vzdělávání (164) a z nich těch, kteří se zaměřují i na děti (62), se ukazuje zajímavý rozdíl, kdy v obecném pojetí jsou témata různorodá a poměrně vyvážená s ohledem na prostředí zpracování informací, vzdělávání dětí silně inklinuje k rozvoji čtenářství, ke kterému se přihlásilo 84,1 % respondentů relevantních pro tuto otázku. Dalším poznatkem, který by měl být vyzdvižen, je značný rozdíl v obou skupinách při zaměření na práci s elektronickými informačními zdroji. Zatímco v obecném pojetí se jednalo o nejčastější volbu (54,9 % relevantních respondentů), v případě zaměření na děti

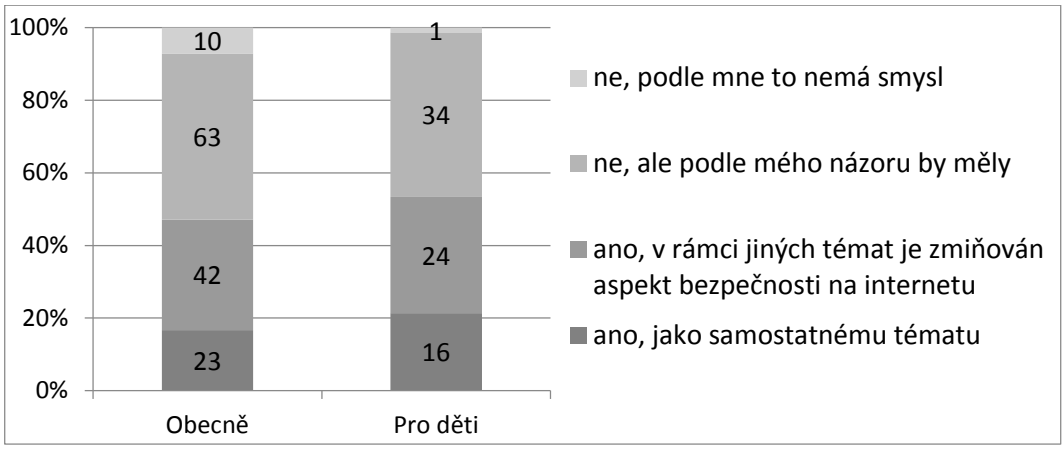
byla až na 4. místě (51,6 % relevantních respondentů) za čtenářstvím, kulturními akcemi a tradičními zdroji. Přitom při srovnání kulturních akcí je rozdíl 27 % a u témat zaměřených na tradiční zdroje 25,5 % ve prospěch akcí pro děti. Témata bez ohledu na prostředí vykazují minimální rozdíl (4,8 %). Výsledky tedy ukazují, že v obecném pojetí jsou témata poměrně vyvážená s mírnou převahou zaměření na elektronické zdroje, zatímco vzdělávací akce pro děti vykazují opačný trend, nerovnoměrné zastoupení témat se silnou převahou čtenářství a tradičních zdrojů.

S ohledem na uvedené výsledky lze konstatovat, že již v roce 2011 bylo možné při zavádění bezpečnosti digitálních stop do vzdělávání v knihovnách navazovat na stávající aktivity, protože pro obě sledovaná zaměření podle více než 50 % respondentů nabízí knihovny vzdělávání o elektronických zdrojích. Lze předpokládat, že s přizpůsobováním knihoven požadavkům společnosti, která se stále silněji komputerizuje, se bude tato hodnota zvyšovat, což naznačuje i růst zájmu knihovníků o problematiku patrný na množství vyžádaných seminářů a zařazení jako stěžejní při setkání knihovnických organizací, např. Podzimního setkání Klubka SKIP 10 (15. 10. 2013), ale také Porada vedoucích pracovníků pověřených knihoven Jihomoravského kraje 25. 9. 2012.

7.1.2.2 Informační bezpečnost ve vzdělávání

Díky dostatečnému pokrytí práce s elektronickými informacemi je možné postoupit ke konkrétnějšímu mapování informační bezpečnosti ve vzdělávání v knihovnách. To bylo v prvním výzkumu nejzazší přiblížení se k problematice této práce, protože při stanovování výzkumné otázky nebylo jasné, do jaké míry je oblast pokryta a jestli má tedy další konkretizace zaměření smysl, protože zvýšení časové náročnosti pro respondenty by mohlo vést ke snížení míry návratnosti[325]. Bylo předpokládáno, že problematika může být řešena samostatně nebo v rámci souvisejících oblastí, ale také že knihovníci mohou vnímat význam tématu, ale nemají podmínky pro jeho zavedení do vzdělávání. To vedlo ke stanovení různých variant přístupu k informační bezpečnosti ve vzdělávání v knihovnách, jejichž výsledné zastoupení znázorňuje graf 8.

[325] ŠVEC 2009, s. 137-139

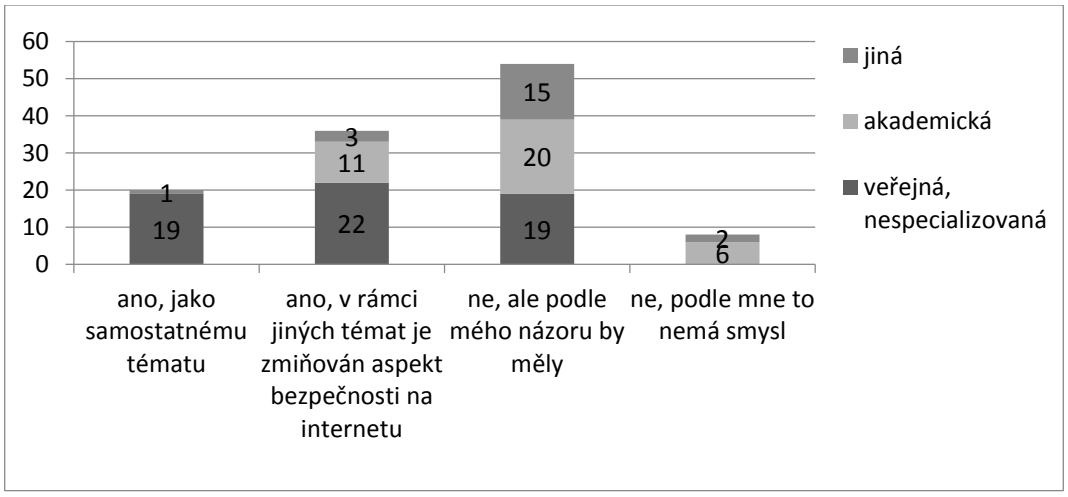


Graf 8 Bezpečnost na internetu v lekcích

Z grafu je patrné, že předpoklady mohly být optimističtější, protože již v roce 2011 informační bezpečnost přibližně polovina respondentů označila za zahrnuté do svých vzdělávacích aktivit, a to jak v obecném případě (47,1 %), tak i se zaměřením na dětské uživatele (53,3 %). Vzhledem k limitům dotazníku nelze konkretizovat podobu lekcí, převažující volba zahrnutí v souvisejícím tématu tedy může mít formu zmínky i rozsáhlého rozboru. Znázornění distribuce pojetí tématu v lekcích ukazuje podobnou tendenci, ale relativní četnosti ukazují, že v případě dětských uživatelů je mírně silnější převaha variant zahrnujících téma, rozdíly však nejsou výrazné, přibližně o 5 % ve všech hodnotách proměnné. Pokud výsledek konfrontujeme s obecnými tematickými zaměřeními, ukazuje se, že v případě dětí je elektronické prostředí méně akcentováno, přitom je ale častěji zapojena informační bezpečnost, zatímco v obecném pojetí je zřejmě pozornost směřována na jiná témata práce s informacemi v elektronickém prostředí.

Při zjišťování postojů knihovníků k problematice informační bezpečnosti ve vzdělávání se ukazuje, že knihovníci jsou jejímu zahrnutí nakloněni, protože pouze 7,2 % respondentů v obecném případě a dokonce jen 1,3 % při zacílení na děti považuje toto za nesmyslné. Protože omezení na děti by se týkalo jen menšího množství respondentů, zejména při sledování právě řešeného postoje k informační bezpečnosti v lekcích, pro konkrétnější určení zastoupení variant v různých typech institucí má smysl je vyhodnocovat jen při obecném zaměření. Z grafu 9 (školní knihovny nejsou zahrnuty kvůli zastoupení jedinou reakcí) je patrné, že lekce k informační bezpečnosti jsou nejčastěji realizovány ve veřejných knihovnách (v 68,3 % z nich). Na druhou stranu o smyslu tématu ve vzdělávání v knihovnách

jsou nejméně přesvědčeni zástupci akademických knihoven, což může mít vliv na to, že jen 29,7 % z nich se přihlásilo k zahrnutí problematiky do lekcí na související témata. Pokud bychom postoj k tématu chápali jako ordinální proměnnou (toto není přesné, výsledek je spíše orientační, protože zahrnutí tématu do vzdělávání ještě není možné vnímat jako důkaz přesvědčení knihovníka samotného, může jít o vliv jiného klíčového zaměstnance instituce), je vhodné srovnání typů institucí na základě mediánu, který je u veřejných nespecializovaných knihoven na hodnotě *ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu*, zatímco u akademických a jiných knihoven je to *ne, ale podle mého názoru by měly*. Rozdíly mezi typy institucí v zahrnutí či nezahrnutí problematiky do vzdělávání jsou statisticky významné při sloučení hodnot zahrnutí tématu podle toho, zda jsou již knihovnou realizovány nebo ne (Pearsonův Chí-Kvadrát 21,947 je statisticky významný na hladině 1 %).



Graf 9 Bezpečnost na internetu v lekcích podle typu instituce

Pozitivní zjištění k postojům na řešení problematiky knihovnami přinesla otázka, zda by podle respondentů knihovny měly vzdělávat děti o bezpečnosti na internetu. Zde jasně převažoval souhlas, opačný přístup se objevil jen výjimečně (v 5 případech, tj. 2,8 %). Vzhledem k tak nízkému počtu není možné statisticky vyhodnocovat jejich zastoupení v dalších kategoriích. Při porovnání s výsledky ostatních otázek se ukázalo, že nikdy nebyla zastoupena jedna hodnota. Zřejmě jediná otázka, kde se shodli respondenti, kteří nevidí význam ve vzdělávání dětí o bezpečnosti na internetu v knihovnách, byla otázka na jim známé preventivní

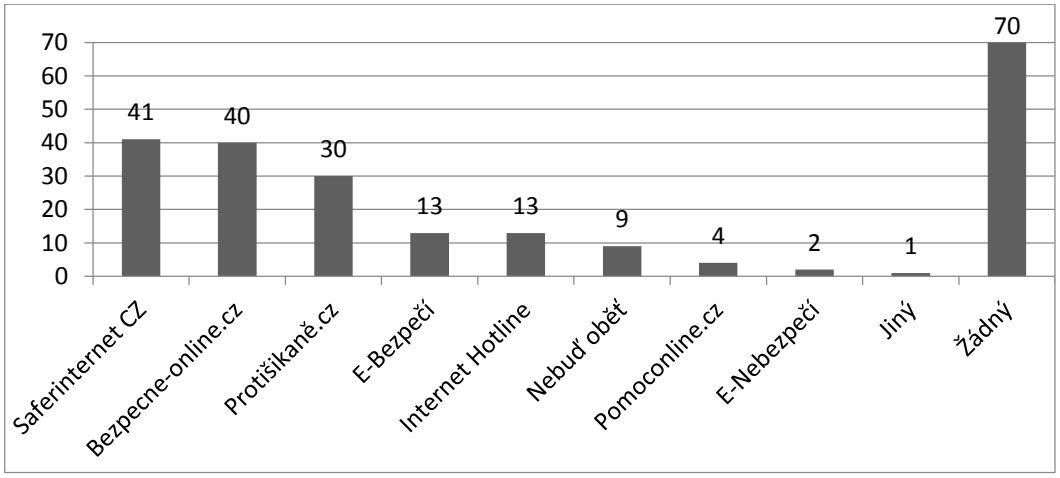
internetové iniciativy, a to že nikdo z nich neznal žádnou z uvedených a ani nedoplnil jinou pro něj známou. Vzhledem k tomu, že se jednalo o jedinou znalostní otázku, navíc sebehodnotící, nabízí se otázka, nakolik si jsou tito respondenti vědomi problémů, se kterými se mohou děti na internetu setkat.

Vedle toho zájem o informační bezpečnost ve vzdělávacích aktivitách knihoven je možné podložit zanecháním e-mailové adresy pro další informace o publikování výsledků šetření 35 dotazovanými (24,0 % z respondentů, kteří neukončili dotazník před touto otázkou). Protože tím je projeven zájem spíše o akademické přehledové informace než o praktickou aplikaci do každodenní práce, o kterou lze s ohledem na omezené časové možnosti knihovníků očekávat větší zájem, je i tento výsledek pozitivní. Ze všech těchto reakcí jasně vyplývá, že je možné i vítané podporovat zavádění problematiky informační bezpečnosti a tím i bezpečnosti digitálních stop do vzdělávání v knihovnách, protože již realizují lekce v širších tematických oblastech a o téma projevují zájem.

V případě, že lekce k informační bezpečnosti jsou již nabízeny, byli respondenti dotázáni na frekvenci realizace. V obecné otázce byly získány jedna až dvě reakce od každého typu instituce mimo školní knihovnu (žádná odpověď), vyšší počet odpovědí přinesly jen akademické (8) a veřejné, nespecializované knihovny (29), právě ty očekávaně zastupovaly jediný typ institucí, který reagoval na stejnou otázku při zaměření lekcí na děti (12). Více než polovina reakcí přinesla neurčitou odpověď nepravidelně, z čehož je opět těžké usuzovat, v jakých řádech je uvažováno. Druhá polovina reakcí s konkrétními odpověďmi se nejčastěji pohybovala v řádu jednotek lekcí za rok (v obecném přístupu 30,8 %, se zaměřením na děti 31,8 %), na druhou stranu zanedbatelný s ohledem na relativní četnosti (obecně 12,8 %, s ohledem na děti 13,6 %) není i počet reakcí v rozmezí jednou za týden až měsíc. Vyšší frekvence se objevovala výhradně u veřejných, nespecializovaných knihoven. Co se týká konkrétních odpovědí (mimo nepravidelně), jsou v obecném pojetí téměř totožné počty odpovědí v rámci kategorií pojetí tématu samostatně nebo v rámci jiné problematiky, při zaměření na děti všechny odpovědi patřily do kategorie samostatné lekce. Vypovídající hodnotu výsledků o frekvenci lekcí je sice nutné brát s rezervou s ohledem na velikost vzorku (39, resp. 22 osob). Nicméně cílem otázky bylo udělat si orientační představu o řádech výskytu tohoto zaměření lekcí, což se podařilo.

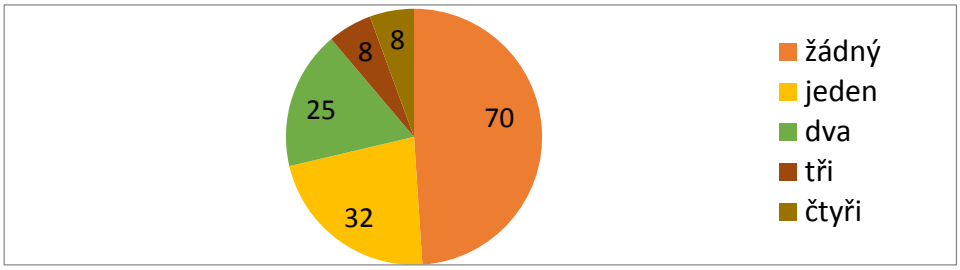
7.1.2.3 Znalost informačních zdrojů k informační bezpečnosti

Vedle otázek pro popis lekcí a názory knihovníků byla pro zjištění jejich znalostí zařazena otázka na preventivní online projekty zaměřené na osvětu v oblasti informační bezpečnosti. Vzhledem k tomu, že na nich je možné nejsnáze najít materiály pro výuku o této problematice a také je možné na ně odkazovat uživatele knihovny pro další informace ve formě přístupné nejširší veřejnosti a konkrétní případy z této problematiky, jsou zajímavé výsledky o tom, které iniciativy jsou známé (viz graf 10) i kolik respondenti označili za jim známé (viz graf 11). Skutečnou znalost by bylo nutné ověřit alternativním postupem, pro který ale v dotazníku nebyl prostor, jedná se tedy o sebehodnotící otázku, jejíž výsledek může být ovlivněn snahou zlepšit svůj obraz ve výzkumu.



Graf 10 Projekty označené za známé

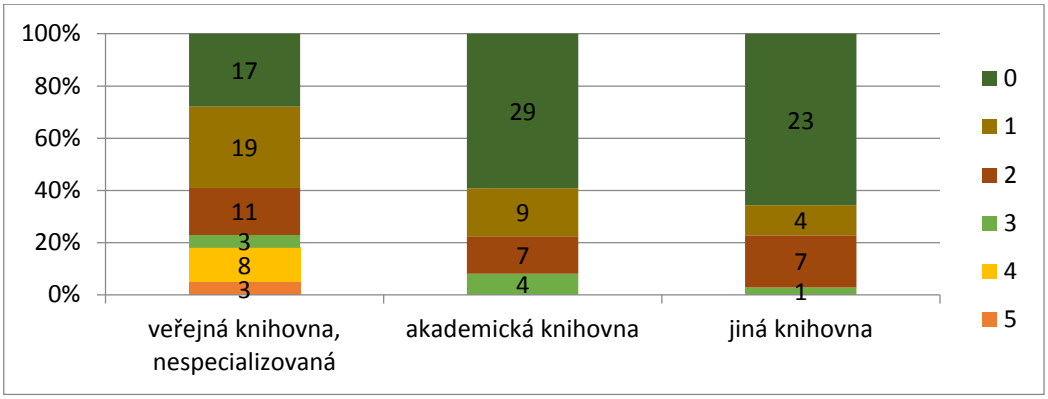
Knihovníci znají materiály Saferinternet CZ. I když jsou dobře provázány jeho dílčí projekty, Bezpečně online, kde lze najít materiály pro lektory, patří mezi známé, ale Pomoc online pro řešení problému mezi nejméně volené. Řádově méně zastoupené jsou iniciativy Centra PRVoK. To je pravděpodobně způsobeno jeho zaměřením na učitele, ale při výukové roli knihovníků by zdroje bylo vhodné využívat, protože často nabízejí kvalitní a pro cílovou skupinu výuky atraktivní materiály. Při variantě odpovědi *jiný* měl být uveden název, výsledné odpovědi ale přinesly jen v jednom případě relevantní výsledek (Minimalizace šikany), jinak se objevovala vyjádření typu „*vím, že existují ,to je vše*“ nebo Alík.



Graf 11 Počet projektů označených za známé

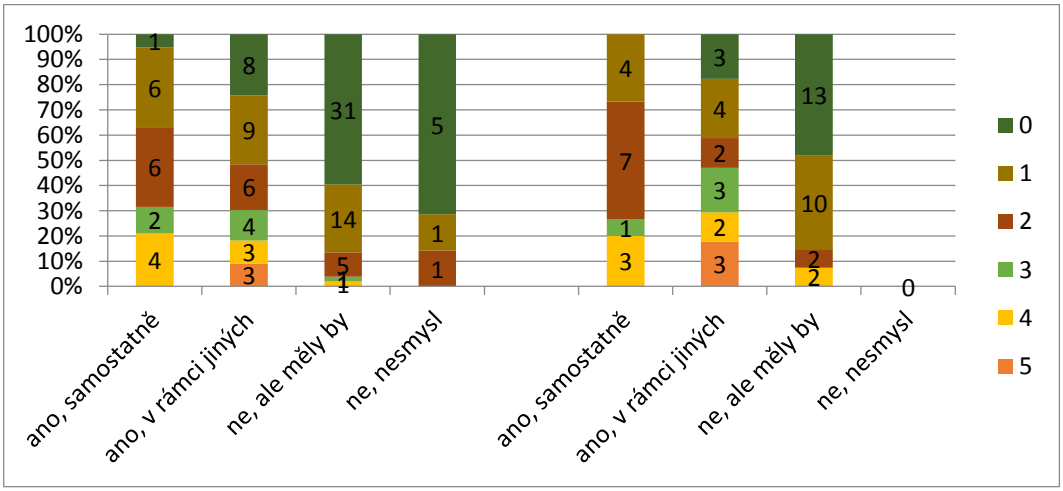
Otázka na preventivní iniciativy představovala jediné zjištění znalostí v dotazníku, proto je důležitým poznatkem, že, přestože se jednalo jen o deklaraci znalosti, 47,9 % respondentů uvedlo, že žádný (nejen z nabízených) nezná, a pouze 9,0 % konstatovalo znalost tří nebo více projektů. To ve spojení se zájmem o zařazení problematiky do vzdělávacích aktivit knihoven ukazuje na potřebu začít u vzdělávání knihovníků samotných, aby mohlo dojít ke kvalitnímu vzdělávání uživatelů knihoven.

I v tomto směru vykazují při srovnání institucí nejlepší výsledky veřejné nespecializované knihovny (viz graf 12 Počet projektů označených za známé v různých typech institucí, opět jsou vyřazeny školní knihovny zastoupené jedinou institucí s hodnotou žádného známého zdroje). S odstupem za nimi se nacházejí akademické knihovny, což lze ale zdůvodnit tím, že většina obecně známých zdrojů k informační bezpečnosti není určena pro akademické prostředí, ale spíše širokou veřejnost. Zdroje vhodné pro akademickou sféru jsou již sofistikovanější a tím i náročnější pro knihovníky, proto je možné očekávat nižší úroveň znalosti. Při srovnání statistických rozdílů mezi těmito proměnnými lze po seskupení pro dostatečné naplněný kontingenční tabulky (sloučeny hodnoty tři a více) zjistit statisticky významný rozdíl (Pearsonův Chí-Kvadrát 21,820 je statisticky významný na hladině 1 %), vztah proměnných je poměrně silný (koeficient kontingence 0,362 s významností 1 %).



Graf 12 Počet projektů označených za známé v různých typech institucí

Při srovnání znalostí projektů dle výskytu informační bezpečnosti v lekcích je patrná souvislost mezi těmito proměnnými, jak ukazuje graf 13. Příčinnost není možné v rámci tohoto šetření konstatovat, je ale možné, že čím více respondenti o problematice informační bezpečnosti ví, tím spíše je zahrnuta do jejich vzdělávacích aktivit nebo i přesvědčení o jejich smysluplnosti. Závislost mezi proměnnými po sloučení některých hodnot (počet známých zdrojů v hodnotách tři a více a zahrnutí problematiky informační bezpečnosti v obecném zaměření i cílení na děti do hodnot podle toho, zda již takové lekce jsou reálně nabízeny nebo ne) je průkazná i statisticky (v obou případech na hladině významnosti 1 %, Personův Chí-Kvadrát je v případě obecném 28,762 a při zaměření na děti 17,774), vztah je přitom dosti silný (koeficient kontingence je v obecném pojetí 0,454 a se zaměřením na děti 0,481, v obou případech opět na hladině 1 %).



Graf 13 Počet známých projektů podle informační bezpečnosti v lekcích (vlevo obecné zaměření, vpravo omezené na děti)

7.1.2.4 Kvalitativní poznámky respondentů

V rámci šetření bylo respondentům umožněno i volné vyjádření jakéhokoli podnětu k tématu šetření. Reakce byly často povzbudivé ve směru pozitivních očekávání od rozvoje impulzů pro knihovny v tomto směru, objevilo se několik nabídek a témat pro spolupráci. Ty přispívají k tomu, co již naznačila otázka na informační bezpečnost v lekcích, kdy právě potřeba pomoci z hlediska zajištění lektora může být jedním z častých důvodů, proč je sice téma považováno za smysluplné, ale není ve vzdělávání v knihovnách nabízeno. Další častější reakcí byl odkaz na spolupráci knihovny a školy v různých formách, např.:

> *„U vzdělávání dětí v této oblasti předpokládám, že se tomu věnují ZŠ na 2. stupni v rámci standardní výuky, pokud nikoliv, je problém v osnovách…“*

> *„myslím, že problematika bezpečnosti dětí na internetu by měla být integrována do výuky informatiky již na základní škole*“

S ohledem na reálnou situaci sice jistě existují místa, kde je vzdělávání dětí v problematice zajišťováno školou, i mezi nimi ale existují takové, které podobně jako knihovny vidí smysl tématu, ale necítí momentálně možnost vlastními silami zajistit jeho pokrytí. A je otázkou, kdo se ujme zaplnění této mezery ve vzdělávání a přitom nebude zajišťovat jen vzdělávání dětí, ale i zbytku společnosti, protože oblast informační bezpečnosti se souběžně s informačními technologiemi vyvíjí tak rychle, že je nutné pro orientaci v této oblasti zajistit celoživotní vzdělávání.

7.2 Rozšiřující deskriptivní výzkum

V návaznosti na první mapování vzdělávání v knihovnách s ohledem na informační bezpečnost, bylo po několika měsících využito dotazníku studentského projektu iNeBe, který probíhal pod vedením Pavly Kovářové, k rozšíření předchozích poznatků. Dotazník byl primárně určený pro zjištění informací pro vybudování portálu o informační bezpečnosti pro knihovníky. K tomu byly navázány otázky rozšiřující předchozí dotazníkové šetření, jejichž cílem bylo posunout poznatky o informační bezpečnosti ve vzdělání v knihovnách na

konkrétní témata v rámci této problematiky, ideálně již s dostatečným pokrytím oblasti digitálních stop. Dále dotazník, s ohledem na výsledky znalostní otázky v předchozím šetření a možnou bariéru vzdělávání uživatelů knihovny právě s ohledem na nedostatečné znalosti samotných knihovníků, řešil zájem o osobní vzdělávání v tomto směru. Vzhledem k silné provázanosti dotazníku s předchozím šetřením jsou závěry obou vyhodnoceny společně.

7.2.1 Metodologie šetření

Šetření iNeBe bylo rozšířením předchozího dotazníku, proto bylo využito podobného přístupu. Snahou bylo oslovit populaci (s vědomím omezené návratnosti), tentokrát jen českých knihoven s profesionálními knihovníky, opět je tedy použit cenzus. Cílová skupina byla zvolena s ohledem na otevírací dobu a vyšší personální zajištění, a tím lepší předpoklady pro realizaci vzdělávání. Snahou bylo omezit proti předchozímu šetření počet institucí neorganizujících vzdělávání. Na druhou stranu byly vynechány specializované knihovny. Neoslovují celou veřejnost, mohly by tedy zkreslovat výsledky tématy, která považují za relevantní svým zaměřením. Cílová skupina reflektovala také výsledek předchozího šetření, kde veřejné knihovny, které nejsou specializované, vykazovaly nejvíce a nejčastěji lekce o informační bezpečnosti. Je tedy vhodné stavět na jejich otevřenosti a určité orientaci v tématu a potřebnosti podtémat i osobního vzdělávání v tomto směru. Pokud se v nich podaří úspěšně zavést vzdělávání v oblasti digitálních stop, příp. informační bezpečnosti obecně, je pravděpodobné, že budou sloužit jako příklad dobré praxe a tedy jako inspirace i pro jiné typy knihoven.

Výzkumná otázka nového šetření byla tedy totožná jako u předchozího výzkumu, bylo ale možné navázat (s ověřením souladu základních východisek) a jít více do hloubky, a to především ve dvou výzkumných podotázkách:

1. **Mají knihovníci zájem o vlastní vzdělávání v oblasti informační bezpečnosti?**

Rozšíření v druhém dotazníku směřovalo i k mapování postojů knihovníků k problematice. Bez jejich vlastní znalosti tématu není možné dále vzdělávat uživatele knihovny, proto dotaz směřoval na vlastní vzdělávání knihovníků pro zajištění předpokladů realizace lekcí v tomto směru.

2. Jaké postavení má problematika digitálních stop mezi ostatními dílčími tématy informační bezpečnosti ve vzdělávání v knihovnách?

Druhá výzkumná podotázka rozšiřujícího šetření navazuje na mapování témat, kdy v předchozím výzkumu bylo zjištěno dostatečné pokrytí širší problematiky digitálních stop a dále proto bylo možné pokročit ke konkretizaci témat směrem k tématu dizertační práce.

Pro získání odpovědí bylo využito opět anonymního online dotazníku, přístupný byl od 2. 1. 2012 do 30. 1. 2012 v nástroji SurveyGizmo. Kompletní znění dotazníku je uvedeno v příloze 1.2. Šíření dotazníku v první vlně probíhalo přímým oslovováním všech relevantních knihoven přes jejich e-mailové adresy. Pokud tyto nebylo možné dohledat a chyběly i webové stránky knihovny, byla tato instituce ze šetření vyřazena. Vzhledem k malé návratnosti byli následně požádáni o pomoc s distribucí regionální metodici v knihovnách a také bylo využito knihovnických elektronických konferencí uvedených na portálu Knihovnického institutu Národní knihovny ČR[326]. Vzhledem k výslednému zastoupení profesionálních knihoven[327] při oslovení přes elektronické konference, které byly využity i v předchozím šetření, se potvrzuje i pro tento i předchozí výzkum užší vymezení populace než všechny knihovny v ČR.

Celkově bylo získáno 121 responzí z jedinečně zastoupených krajských a městských knihoven. Mezi nimi není započítáno 45 dotazníků, které byly pouze otevřeny, nebo do nich bylo zaznamenáno velmi málo odpovědí (tři a méně ze šestnácti) a následně byl dotazník ukončen, a duplicitní odpovědi ze stejných knihoven. Cílem sice bylo pokrýt celou populaci, s ohledem na zájem knihoven o výsledky šetření a jejich omezené časové a lidské zdroje, je možné považovat výsledné zastoupení 18,1 % relevantních institucí za dostatečné[328]. Pro potřeby této dizertační práce by bylo nadbytečné zabývat se všemi výsledky šetření s ohledem na jeho dva různé cíle. Vyzdvižena jsou proto jen zjištění relevantní pro tuto práci, která přináší v oblasti dvou výzkumných podotázek uvedených výše rozšíření

[326] HOCH 2012

[327] Neprofesionální knihovny byly vyřazeny před vyhodnocením dotazníku, stejně jako duplicitní knihovny, kdy byla ponechána vždy dřívější zaznamenaná odpověď.

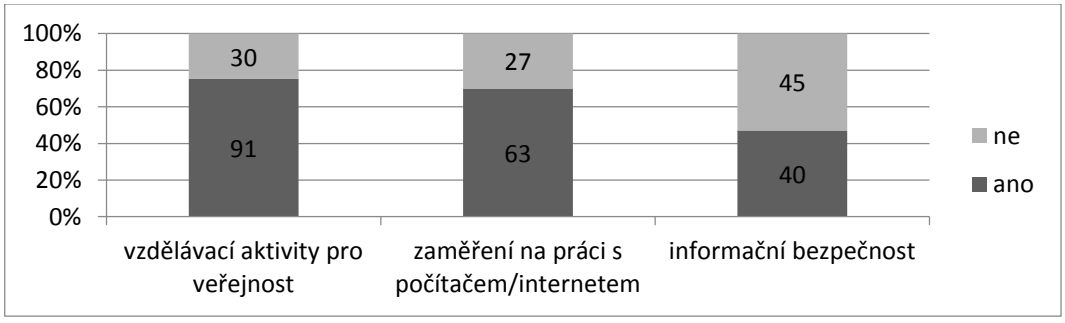
[328] Zastoupení je spočítáno na základě součtu knihoven krajských, základních pověřených regionální funkcí a základních s profesionálními knihovníky po odečtení počtu specializovaných knihoven z roku 2012 podle statistiky NIPOS (Základní statistické údaje o kultuře v České republice 2012 2013)

poznatků z výzkumu popsaného v kap. 7.1. Data byla zpracovávána v softwaru SPSS, pro grafickou úpravu byl použit MS Excel 2010.

7.2.2 Výzkumná zjištění

7.2.2.1 Východiska pro srovnání rozšiřujícího a původního šetření

Pro šetření byla oslovena jiná populace a lze předpokládat, že responze pochází od odlišných subjektů než v případě prvního mapujícího šetření. Proto je nezbytné nejdříve knihovny popsat s ohledem na základní východiska pro další rozšíření, tedy jestli realizují vzdělávací aktivity pro veřejnost, příp. se zaměřením na elektronické prostředí a ještě konkrétněji na informační bezpečnost. Pomocí těchto otázek lze srovnat klíčové charakteristiky v obou výzkumech. Graf 14 při komparaci s obdobnými otázkami v předchozím výzkumu (viz kap. 7.1.2) potvrzuje velmi podobné relativní četnosti sledovaných charakteristik. Vzdělávací aktivity podle rozšiřujícího šetření nabízí 75,2 % dotázaných institucí (rozdíl 2,9 %), a zahrnutí informační bezpečnosti do nich deklarovalo 44,4 % (rozdíl 2,7 %). Mírně odlišný je výsledek u lekcí spojených s počítačem a internetem, protože otázky v obou šetřeních byly položeny značně odlišně – v původním bylo oddělováno téma práce s informacemi v elektronickém prostředí a bez ohledu na typ prostředí, což v obou případech může spadat pod kategorii spojenou s počítači či internetem, proto se v rozšiřujícím šetření výsledek 69,2 % odlišuje od předchozího, kde se k lekcím spojeným s elektronickým prostředím přihlásilo 54,9 % a s prací bez ohledu na typ prostředí 35,4 %. Jiný možný důvod rozdílu by mohl být spatřován v časovém odstupu (5 měsíců), vzhledem k vyváženosti ostatních dvou oblastí ale tento důvod není pravděpodobný.



Graf 14 Vzdělávání v knihovnách dle rozšiřujícího výzkumu

Na základě srovnatelnosti výsledků v obou šetřeních se zvyšuje oprávněnost tvrzení, že knihovny se již věnují souvisejícím oblastem v poměrně výrazné míře, která ale především v zaměření na informační bezpečnost není ideální a měla by být rozšiřována. Je tedy možné vycházet ze zkušeností knihovníků ohledně zájmu a potřebnosti vzdělávání uživatelů v oblasti práce s informacemi v elektronickém prostředí. Protože se také již téměř polovina knihoven snaží do svých lekcí zahrnout téma informační bezpečnosti, lze již stavět i na těchto zkušenostech a dále je rozvíjet.

Rozdělení témat práce s počítačem či internetem a informační bezpečnosti v kontingenční tabulce 3 odpovídá obecnému poměru v kategorii, kdy knihovna má aktivity zaměřené na práci s počítačem či internetem (první sloupec), stejně jako pokud se nevěnuje informační bezpečnosti (druhý řádek). Pokud knihovna lekce cílené na počítač či internet nenabízí, obvykle se nevěnuje ani informační bezpečnosti, což naznačuje vztah mezi oběma tématy, kdy informační bezpečnost není řešena v širším pojetí (manipulace informacemi, hodnocení informací v tradičním zpravodajství apod.), ale především ve smyslu IT bezpečnosti. Pokud jsou nicméně v lekcích zahrnuta tato témata, je blízko k bezpečnosti informací na internetu vzhledem k tomu, jak často jsou nyní informace zprostředkovány informačními technologiemi. Jediným nepříznivým výsledkem z hlediska zahrnutí problematiky do vzdělávání o informační bezpečnosti se zaměřením na digitální stopy proto zůstává více než pětina knihoven, které nenabízí lekce zaměřené na IT, ani informační bezpečnost. Statistickou významnost vztahu proměnných dokazuje na hladině 1 % Personův Chí-Kvadrát s hodnotou 8,225.

Tabulka 3 Srovnání zaměření lekcí

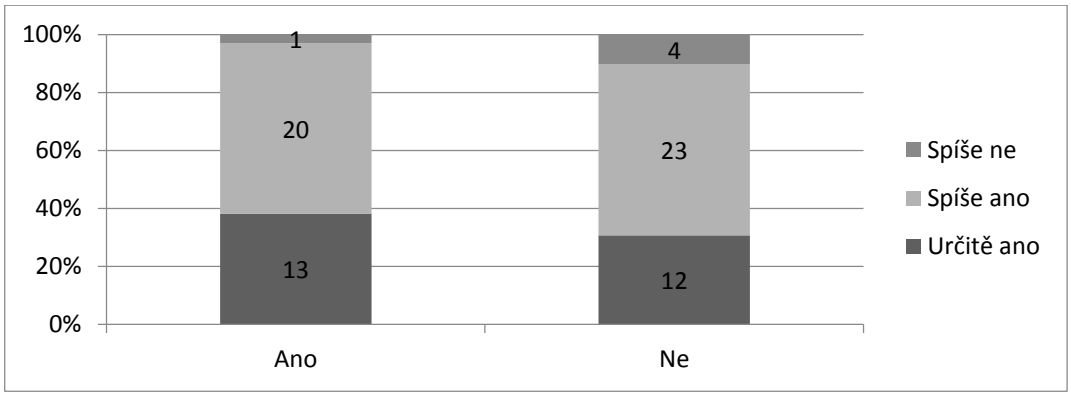
		Vzdělávací aktivita na počítačovou gramotnost nebo práci s počítačem či internetem		Cel-kem
		Ano	Ne	
Informační bezpečnost v některé vzdělávací aktivitě	Ano	33	6	40
	Ne	25	20	45
Celkem		62	27	90

7.2.2.2 Zájem knihovníků o vlastní rozvoj v informační bezpečnosti

V tom, že informační bezpečnost již je v lekcích zahrnuta, lze spatřovat i zájem knihovníků o téma a jeho předání uživatelům knihovny. Pokud jsou lekce realizovány, v knihovně se musí nacházet osoba, která v tom vidí smysl a téma prosadila. V případě, že knihovna téma neřeší, se může jednat o nezájem, ale i o obavu z realizace, která vychází z nedostatečných znalostí, strachu z konfrontace znalostí knihovníka a uživatelů (zejména dětí), nedostatek času či pochopení ze strany vedení knihovny či uživatelů a podobně[329].

Rozšiřující dotazník přinesl ještě pozitivnější výsledek v přesvědčení knihovníků o důležitosti vzdělávání o informační bezpečnosti než předchozí šetření, protože v něm nikdo nevyjádřil negativní postoj k důležitosti problematiky. 66,0 % respondentů uvedlo, že určitě souhlasí s důležitostí vzdělávání o tématu, 32,1 % spíše souhlasí. Protože z otázky není jasné, kdo by měl toto vzdělání realizovat, výsledky je nutné podpořit zájmem knihovníků o jejich vlastní vzdělávání v této oblasti, čímž jsou výsledky přeneseny do prostředí, které je předmětem této práce. Výzkum ukázal pozitivní přístup i v tomto směru, protože 31 respondentů uvedlo, že určitě mají zájem se osobně vzdělávat, 56 respondentů zvolilo variantu spíše ano a 12 respondentů spíše ne. Celkově tedy zájem o osobní vzdělání v řešené problematice projevilo 83,6 % respondentů, což je povzbudivý výsledek pro rozvoj problematiky digitálních stop v knihovnách, nejdříve ve vzdělání samotných knihovníků a následně uživatelů. Vzhledem k minimálnímu zastoupení negativního postoje nemá smysl vyhodnocovat dle tohoto kritéria další otázky, protože distribuce hodnot by byla v neprůkazná. Výsledky i srovnatelnost relativního zastoupení ukazuje graf 15. Rozdíly jsou minimální, pokud by měl být interpretován neprůkazný rozdíl (Pearsonův Chí-Kvadrát 1,715 s hodnotou významnosti p = 0,424), lze konstatovat, že chybějící osobní zkušenost s realizací vzdělávací aktivity o informační bezpečnosti je spojena s nižším zájmem o téma.

[329] Tento nekompletní výčet obsahuje příklady důvodů pro ilustraci, všechny byly jmenovány knihovníky z praxe při různých příležitostech, kdy se vyjadřovali k zavedení tématu do jejich vzdělávacích aktivit.



Graf 15 Zájem o osobní rozvoj dle existujícího vzdělávání o informační bezpečnosti

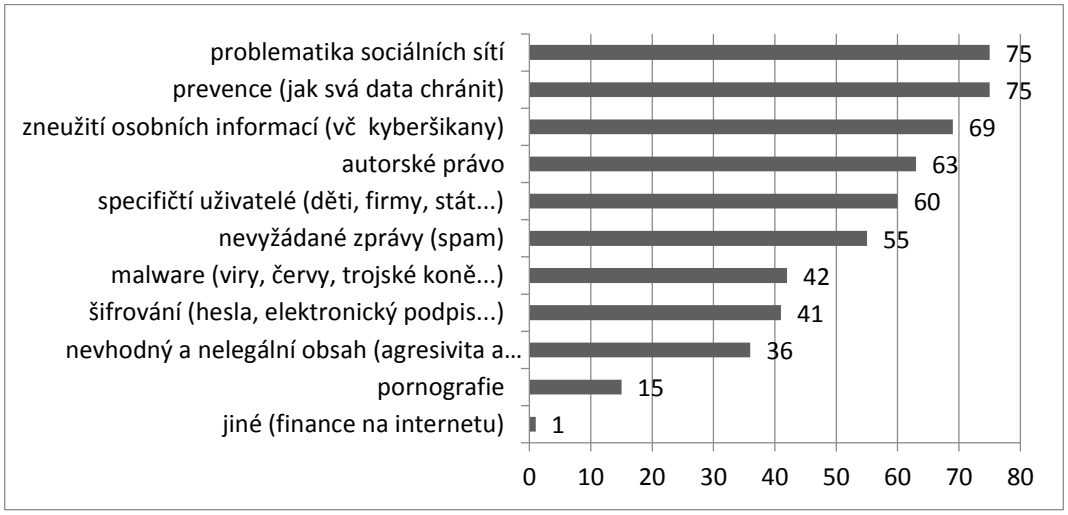
Vyvážená distribuce hodnot je také v rámci skupin vytvořených na základě zájmu o metodické materiály. Ten patří mezi další projevy zájmu knihovníků o zavedení problematiky do knihovny, tentokrát již zcela ve spojení se vzděláváním uživatelů. Zájem o metodické materiály, které by umožnily orientaci v problematice tak, aby knihovníci mohli ve své knihovně přednášet o informační bezpečnosti, projevilo 76,3 % respondentů. Pokud je téma akceptováno jako významné pro služby knihovny (viz kap. 3), odpovídá tento výsledek obecnému přístupu knihovníků v nespecializovaných knihovnách k metodickým materiálům[330]. Vzhledem k tomu, že mezi negativními ohlasy mohou být projevy knihovníků, kteří si chtějí lekce stavět sami a nechtějí být svazováni předpřipravenými metodickými materiály, je tento výsledek až překvapivě pozitivní a ukazuje smysluplnost navržené koncepce vzdělávání (viz kap. 8.2). Zájem o problematiku mezi knihovníky dokresluje také to, že 66 z nich zanechalo e-mailovou adresu jako vyjádření ochoty spolupracovat či využít výukové nebo propagační materiály v oblasti řešené v dotazníku. Pokud je zohledněno, že někteří nechtěli porušit svou anonymitu v dotazníku tímto krokem, jedná se o další validaci pozitivního přístupu knihovníků k problematice informační bezpečnosti, resp. digitálních stop[331] ve vzdělávání v knihovnách.

[330] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012

[331] S ohledem na výklad témat, o která knihovníci projevili zájem, považuji za prokázané, že oblast informační bezpečnosti v knihovnách spojují především s digitálními stopami.

7.2.2.3 Téma digitálních stop v rámci informační bezpečnosti

Druhý dotazník byl do značné míry rozšiřující v tom, že jeho cílem bylo zmapovat, co si knihovníci představují pod informační bezpečností v kontextu knihoven, se kterou operoval tento i předchozí dotazník. Pro zjištění bylo využito nepřímého dotázání. Pro redukci omezení dotazníku byly zařazeny polouzavřené otázky s větším množstvím připravených témat, z nichž měli respondenti vybrat, která by je zajímala v kurzu pro jejich osobní rozvoj. Touto formou knihovníci vyjádřili, která témata informační bezpečnosti vidí jako zajímavá pro prostředí knihoven (viz graf 16). Snahou nepřímého dotázání bylo vyhnout se tomu, aby respondenti označovali témata, která považují za důležitá pro uživatele, ale zprostředkovaná někým jiným než knihovníkem (což by mohlo nastat při položení otázky typu „*Ve kterých subtématech informační bezpečnosti si myslíte, že by měli být uživatelé vzděláváni?"*).

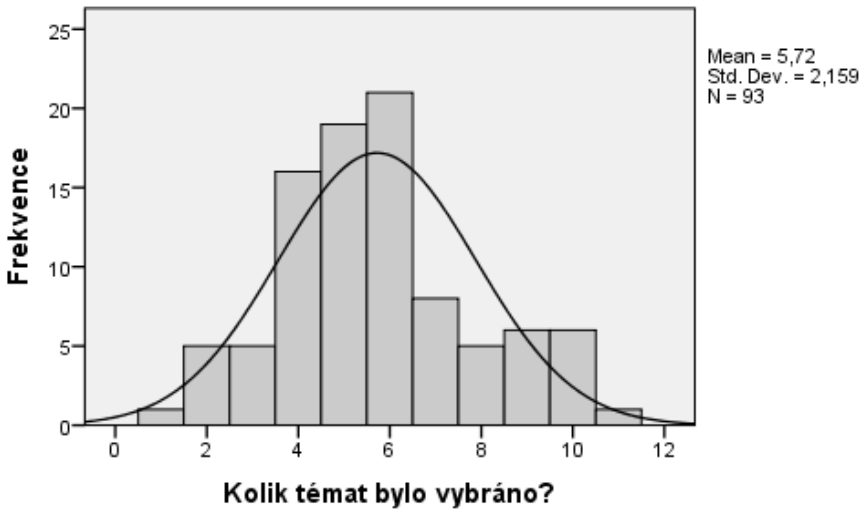


Graf 16 Témata žádaná knihovníky do kurzu

Při analýze témat dle preference mezi knihovníky je patrné, že informační bezpečnost v knihovnách je úzce svázána s digitálními stopami. Ty jsou totiž největší hrozbou sociálních sítí, které byly vyhodnoceny jako nejžádanější téma spolu s prevencí, tedy obecnou snahou se chránit v prostředí internetu. V pořadí následovalo zneužití osobních informací, což opět úzce souvisí s digitálními stopami, ať už zanechanými samotným subjektem informací nebo někým jiným o něm. I upřesňující pojem kyberšikany navádí ke spojení s digitálními stopami,

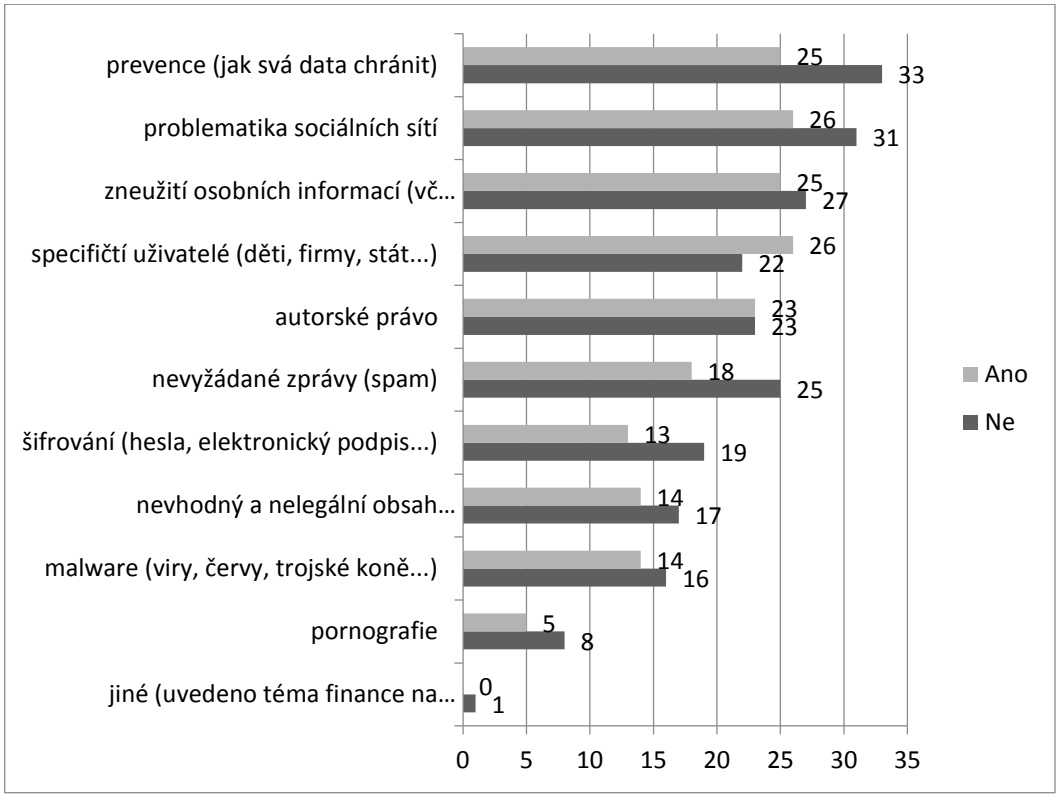
protože jeden z nejsilnějších vlivů kyberšikany proti tradiční šikaně je zvýšení počtu šikanujících a délky šikany s ohledem na dostupnost kompromitujícího materiálu, který odpovídá definici digitální stopy pro tuto práci. Všechna tato témata knihovníci zařadili před autorské právo, které knihovny ve vzdělávacích aktivitách již řeší. Důvodem může být fakt, že pro tuto oblast již existují kurzy určené knihovníkům pro získání potřebných znalostí pro realizaci lekce. Na druhou stranu je z výsledků patrné, že knihovny vnímají tlak veřejnosti na ochranu soukromí na internetu a mají zájem se v této oblasti vzdělávat, což by mělo vycházet z pocitu potřebnosti tématu pro výkon služeb v knihovně.

Při hlubším pohledu na výběr témat se objevuje se křivka odpovídající normálnímu rozložení počtu témat, o které byl projeven zájem (viz graf 17), což je způsobeno těsnou blízkostí středních hodnot (průměr 5,72, medián 6, modus 6), normalita je také ověřena Kolmogorov-Smirnov testem. V distribuci je možné pozorovat mírné pravostranné zešikmení, převažuje tedy zájem o užší tematické zaměření, což přispívá k významnosti nejčastěji uváděných témat. Současně to dává podnět k formě distribuce materiálů pro další rozvoj knihovníků, kteří by neměli být nuceni k plošnému poznávání informační bezpečnosti, ale měla by jim být dána možnost zaměřit se na oblasti, které považují za v daném kontextu přínosné (tj. užší zaměření seminářů nebo možnost otevřených kurzů, kdy se dostanou k libovolnému tématu, aniž by museli čekat na otevírání tematických modulů nebo by museli zvládnout jiné téma jako prerekvizitu).



Graf 17 Počet vybraných témat

Volba témat s ohledem na to, zda již vzdělávání o informační bezpečnosti v knihovně probíhá, je poměrně srovnatelně rozložená v obou skupinách se spíše mírnými výchylkami u jednotlivých témat, které znázorňuje graf 18. Nižší počet reakcí v součtu je dán tím, že někteří zvolili v otázce o zahrnutí informační bezpečnosti do vzdělávání nevalidní variantu *nevím*, proto byli z grafu vyřazeni.



Graf 18 Zájem o téma dle zkušenosti s lekcí o informační bezpečnosti

7.3 Závěry deskripce připravenosti knihoven na digitální stopy

Dotazníkové šetření si nekladlo za cíl přinést přelomové či hluboké nové poznatky. V době, kdy se o tématu informační bezpečnosti v českých knihovnách v podstatě nemluvilo, a proto nebylo jasné, do jaké míry se objevuje v jejich vzdělávacích aktivitách, bylo nezbytné pro další výzkum zmapovat situaci, do které se vstupuje a stanovit již existující základy, na které je možné navazovat. A právě tento cíl výzkum naplnil a dal prostor ke stanovení dalších otázek, které by měly být výzkumně podchyceny. Situace se v posledních letech výrazně změnila, ale informace o řešení problematiky ve vzdělávání v knihovnách jsou stále spíše kusé.

Dochází k němu, ale informování odborné veřejnosti o jeho podobě je nahodilé a nedostatečné, jak ukazuje kap. 4.3. Proto mají výsledky tohoto šetření i navzdory době svého vzniku a změně situace význam.

Výzkumu se zúčastnily především knihovny již nabízející vzdělávání, což ukazuje jejich vyšší zastoupení oproti výzkumům NIPOS[332] a IVIG[333]. Již v roce 2011 bylo poměrně široké pokrytí práce s informacemi v elektronickém prostředí, i když spíše v obecném přístupu, protože pro dětské uživatele byla upřednostňována tradičnější témata, což odpovídá zjištěním výzkumu IVU SDRUK[334]. Základním zjištěním šetření bylo, že knihovny již poměrně často téma informační bezpečnosti ve svých lekcích pokrývají, i když v různé formě, a to jak v obecném pojetí, tak při zaměření na dětské uživatele. Důsledkem proto může být, že děti prezentují knihovny jako zdroj rad o online bezpečnosti[335]. Je samozřejmé, že se to netýká všech knihoven, protože ty pokrývají různá témata práce s informacemi a někdy se vůbec do vzdělávacích aktivit nepouštějí. V případě, že se informační bezpečnosti nevěnují, převažuje názor, že by se toto mělo změnit, protože je smysluplné téma do vzdělávacích lekcí v knihovnách zařadit, opačný názor se vyskytl jen výjimečně. Z šetření jasně vyplynulo, že tématu při zaměření na děti, ale i v obecném pojetí, jsou příznivě nakloněny zejména veřejné, nespecializované knihovny, které převažovaly jak v množství lekcí k tématům o práci v elektronickém prostředí i o informační bezpečnosti, tak i ve frekvenci výskytu těchto lekcí.

V rámci rozšiřujícího šetření se konkretizovaly názory knihovníků na problematiku a témata, která řeší nebo považují za vhodná řešit v knihovně. Pro tuto návaznost bylo nezbytné ověřit, že základní východiska odpovídají původnímu výzkumu, což se potvrdilo. Dále proto bylo možné navázat zjištěním preference subtémat v rámci informační bezpečnosti, z nichž vyplývá zájem o témata spojená s problematikou digitálních stop, což odpovídá doporučením zahraničních výzkumů[336], ale nedostatečně se odráží v současné nabídce lekcí o informační bezpečnosti v knihovnách[337]. Přestože se tedy mapující výzkumy kvůli citlivosti

[332] Základní statistické údaje o kultuře v České republice 2012 2013
[333] LANDOVÁ 2010
[334] NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012, s. 45-47
[335] LIVINGSTONE 2011, s. 127
[336] WALRAVE 2012; WEEDEN 2013
[337] Viz kap. 4.3 Bezpečnost digitálních stop ve vzdělávání v knihovnách

otázek dotazovaly na širší oblast informační bezpečnosti, díky úzkému vztahu v očích knihovníků je možné výsledky přiblížit k tématu této dizertační práce. V závěru je možné konstatovat, že problematika je do značné míry v oblasti zájmu knihoven a je tedy možné navázat dalším rozvojem této oblasti, protože je stále dost velký počet institucí, které vzdělávání o digitálních stopách nezařazují do svých služeb. Příklady dobré praxe a další podpora (např. usnadnění získání znalostí v této problematice) by mohly způsobit silnější rozvoj zájmu knihovníků ve směru řešeném touto prací.

Výzkum také podpořil původní výsledky prokazující zájem knihovníků dále vzdělávat sebe i uživatele v oblasti informační bezpečnosti. V případě uživatelů je zájem navázán na jednotlivá subtémata, především spojená s problematikou digitálních stop, a také na metodické materiály, což podporuje návrh koncepce v kap. 8.2. Zájem je základním předpokladem pro zavedení problematiky do vzdělávání v knihovnách, na který je nutné reagovat se snahou redukovat bariéry v tomto směru, které jsou především časové, geografické a odborné, což lze nejsnáze řešit e-learningovým kurzem zaměřeným přímo na knihovníky bez požadavků na předchozí znalosti. Takový kurz byl vytvořen v rámci projektu VISK2 a je dostupný přes portál Kurzy.knihovna.cz. Kurz je odpovědí na zájem knihovníků o vlastní vzdělávání a také pomůckou pro vzdělávání uživatelů knihovníky s pozitivním postojem k této službě, který byl projeven v obou výše řešených dotaznících.

Pro řešení problematiky v různých směrech, včetně vzdělávání uživatelů, vyžaduje dostatečnou úroveň znalostí knihovníků. Zajímavé poznatky přinesla jediná znalostní otázka v úvodním dotazníku, která metodou samohodnocení zjišťovala obeznámenost respondentů s osvětovými projekty v oblasti informační bezpečnosti. Je možné, že respondenti svým zaměřením nepovažují jmenované projekty za relevantní pro své potřeby, ale ani varianta *jiné* nebyla až na výjimky využita. Značně převažující je tedy výsledek ukazující neznalost respondentů v této oblasti. Protože znalosti představují základní předpoklad, aby mohli být vzdělávaní další lidé, v návaznosti na toto zjištění bylo realizováno hloubkové didaktické testování znalostí knihovníků a studentů informačních studií a knihovnictví jako možných budoucích knihovníků (viz kap. 7.4).

Přestože mapující i rozšiřující výzkum jsou poznamenány nízkou návratností dotazníků, které byly směřovány k celé populaci knihoven relevantních pro šetření, pomocí jejich silného překrytí a výsledků, které si do značné míry odpovídají, je možné dále vycházet z uvedených zjištění. Podrobnější deskripce této oblasti by mohla přinést další zajímavé výsledky, pozornost by například zasloužilo zmapování, jakou podobu má deklarované zahrnutí problematiky informační bezpečnosti do vzdělávacích aktivit v knihovně, tato informace již ale není nutná pro splnění cíle této práce.

7.4 Testování znalostí knihovníků o digitálních stopách

Základním předpokladem možnosti vzdělávat je dostatečná erudovatnost v daném tématu. Po popisu prostředí, do kterého je navrhována metodika vzdělávání o bezpečnosti digitálních stop, je nutné zmapovat připravenost osob, které by ji měly realizovat. Určité pokusy o hodnocení znalostí byly přítomny již v předchozích šetřeních, jednalo se ale spíše o určitou sondu, kdy výsledky neukazovaly výrazně hluboké znalosti knihovníků, spíše naopak, např. sebehodnotící otázka v mapujícím šetření (viz s. 127). Tento přístup je ale nedostatečný, proto bylo vytvořeno samostatné šetření pro zmapování znalostí knihovníků a studentů oboru informační studia a knihovnictví o digitálních stopách, jejich zneužití a ochraně. Vedle deskriptivní funkce bylo cílem šetření také ověřit, jakou úroveň vzdělání o internetové bezpečnosti absolvovali respondenti vykazující dostatečné znalosti v řešené problematice.

7.4.1 Metodologie šetření

Základním předpokladem bylo, že současní knihovníci často neprošli vzděláním o informační bezpečnosti a někdy ani informačních technologií, jejich znalosti budou tedy nižší než u studentů, jejichž vzdělání by mělo odpovídat potřebám současné společnosti, obě témata by tedy alespoň do určité míry měla být v jejich výuce pokryta. Knihovníci oproti tomu procházejí kurzy pro další vzdělávání, ovšem v problematice digitálních stop zatím kurzy nejsou příliš

rozšířené, proto ještě téma nebylo zprostředkováno výraznějšímu množství knihovníků. Uvedené předpoklady vedou k výzkumné podotázce o významu organizovaného vzdělávání pro znalosti v oblasti digitálních stop.

Výzkumná otázka:

Na jaké úrovni jsou znalosti problematiky digitálních stop současných a možných budoucích knihovníků?

Výzkumné hypotézy:

H1: Většina respondentů dosahuje 40-60 % bodů ve znalostním testu na téma digitální stopy.

Dle hlavní hypotéza má široká veřejnost určité povědomí o problémech spojených s digitálními stopami a současní i budoucí knihovníci mají možnost se v případě zájmu vzdělávat dál alespoň v základech problematiky. Nejedná se však o povinnou součást vzdělávání, je tedy na zájmu samotných jednotlivců, zda nabídky osobního rozvoje využijí. Lze proto očekávat, že respondenti budou vykazovat povrchní znalosti v řešené problematice, nebudou ale z většiny dosahovat do horního kvartilu bodů.

Na tuto hlavní hypotézu navazují dílčí hypotézy:

h1: Více než 50 % respondentů dosáhne méně než 50 % maxima bodů.

h2: Průměrný počet bodů je vyšší u otázek k chování lidí než k technické stránce.

h3: Průměrný počet bodů v jednotlivých tematických oblastech se liší.

h4: Respondenti s větším zájmem o téma digitálních stop dosahují více bodů.

h5: Respondenti s vyšším počtem bodů jsou častěji přesvědčeni o smyslu vzdělávání o tématu digitálních stop.

H2: Respondenti, kteří absolvovali rozsáhlejší organizované vzdělávání o digitálních stopách, dosahují vyššího bodového hodnocení v testu.

Hypotéza odkazuje na smysl organizovaného vzdělávání o digitálních stopách, které zvyšuje úroveň znalostí nad úroveň obecného povědomí. V rámci dílčích hypotéz je pak toto ověřováno v oblastech různého pojetí rozsáhlosti:

h6: Současní studenti oboru ISK dosahují vyššího počtu bodů než současní knihovníci a zájemci o práci v knihovně.

h7: Min. 75 % bodů dosahují respondenti, kteří absolvovali více než 3 přednášky nebo samostatný předmět či kurz.

h8: Vyššího počtu bodů dosahují studenti, kteří prošli organizovaným vzděláváním na vysoké škole, než ti, kteří vzděláním prošli na jiné úrovni.

h9: Respondenti, kteří prošli organizovaným vzděláváním, jsou častěji přesvědčeni o smyslu vzdělávání o tématu digitálních stop.

Podobně jako u mapujícího šetření i zde byla snaha zasáhnout celou populaci, která byla zvolena jako cílová skupina šetření. Na jedné straně se jednalo o studenty oboru informační studia a knihovnictví na českých vysokých školách (Univerzita Karlova, Masarykova univerzita a Slezská univerzita v Opavě), kteří představují možné budoucí knihovníky. Na druhé straně tvořili cílovou skupinu současní knihovníci, vzhledem ke snaze o zavedení nové oblasti do jejich činnosti, především vzdělávání, by mělo jít o knihovníky sledující aktuality v této oblasti, a to zapojením do organizací zaměřených na vzdělávání v knihovnách nebo do elektronických knihovnických konferencí. Právě tyto kanály byly využity k distribuci šetření – v případě studijních oborů a organizací bylo využito zprostředkovatele, který informaci o šetření distribuoval.

Test byl zpracován pomocí webové aplikace Survio pro dotazníková šetření, které splňovalo požadavky na formu otázek a odpovědí. Testování bylo k dispozici pro vyplnění v období 21. 6. - 15. 9. 2013. Nevýhodou nástroje, která byla zjištěna až po spuštění šetření, je, že průběžně neukládá již vyplněné odpovědi. Vzhledem k náročnosti dotazníku (jeho plné znění s odpověďmi hodnocenými jako správné je uvedeno v příloze 1.3) se proto podařilo shromáždit jen 213 responzí, všechny ale kompletně vyplněné. Je pravděpodobné, že použití nástroje s průběžným ukládáním výsledků by přineslo vyšší návratnost, i když s nižší úplností odpovědí. Přesto je množství responzí dostatečné pro vyhodnocení výsledků s ohledem na výše uvedené výzkumné otázky. Výsledná data byla zpracována pomocí programu SPSS a graficky upravena v Microsoft Excel 2010.

7.4.2 Výzkumný nástroj

S ohledem na cíle výzkumy bylo jako nástroj zvoleno pedagogické testování pro měření kognitivní úrovně znalostí. Pro jeho bližší popis je možné použít charakteristik testů podle Byčkovského[338]. Jedním z cílů šetření bylo ukázat na dostatečnou úroveň vzdělávání v problematice s ohledem na prokázané znalosti v testu. Test úrovně nebyl kombinován s testem rychlosti, protože pomocí elektronického dotazníku měl každý respondent tolik času, kolik potřeboval. V popisu výzkumu byl pouze orientační údaj o časové náročnosti vyplnění, aby tomu respondenti mohli přizpůsobit čas, který si na vyplnění vyhradili. Uvedený údaj (20 minut) vycházel z pilotního testování nástroje, kterého se zúčastnilo 5 subjektů, a také z orientačního vymezení uvedeného Chráskou[339]. Odhad se následně potvrdil, 69 % respondentů vyplňovalo dotazník 10-30 minut.

Jedná se do značné míry o test výsledků výuky, bylo ale možné sledovat jen formální a neformální úroveň učení. Z hlediska interpretace výkonu se jedná o rozlišující test, tedy sledující relativní výkon jednotlivců ve sledované skupině, protože jen tak je možné srovnání dílčích skupin dle absolvovaného vzdělání. Z hlediska výzkumných otázek je zajímavý i pohled testu jako ověřovacího (test absolutního výkonu), kdy jsou výsledky srovnávány s požadovanou úrovní znalostí (zda jí bylo dosaženo a tím je učivo zvládnuto, bez ohledu na výsledky jiných členů skupiny). Oba pohledy jsou z hlediska cíle výzkumu důležité, proto budou aplikovány při interpretaci výsledků a byly zohledněny i při tvorbě výzkumného nástroje. Jsou proto zařazeny otázky základní, jejichž správné řešení je nezbytné pro prokázání zvládnutí problematiky, ale také otázky rozšiřující, které ukazují hloubku znalostí. Z hlediska plošného uplatnění v praxi je jejich znalosti prospěšná, ale ne nezbytná. Knihovníci v praxi totiž nemusí být experty na problematiku digitálních stop, jejich znalosti by ale měly být dostatečné pro pomoc uživatelům.

Test probíhal po skončení semestru, až na výjimky se tedy jednalo o test výstupní (sumativní). Protože sledoval nejen problematiku bezpečnosti digitálních stop, otázky byly pokládány ze šesti provázaných oblastí, které byly následně vyhodnocovány a srovnány odděleně, jedná se o test polytematický (souhrnný). Jednalo se o témata: vymezení pokrytí digitálních stop, aktivní a pasivní digitální

[338] BYČKOVSKÝ 1982
[339] CHRÁSTKA 1999, s. 42

stopy a problémy s nimi spojené, řešení problémů chováním uživatele, technickými postupy a legislativními možnostmi.

Nebyl použit standardizovaný test, protože v této oblasti neexistuje, test byl ale podroben postupům[340] pro kvazi-standardizovaný didaktický nástroj. Validita vycházela z obsahové náplně předmětů Nástroje a možnosti internetu, Informační bezpečnost (vyučovaný na KISK FF MU), Základy informačních technologií a Zneužitelné informace na internetu (ÚISK FF UK), na Slezské univerzitě v Opavě podobná alternativa nebyla nalezena. Z hlediska obsahové validity z pohledu náplně vzdělávání knihovníků v praxi byl obsah srovnáván s ohledem na známou náplň seminářů pro knihovníky o informační bezpečnosti. Vzhledem k neexistenci přehledu všech lektorů dalšího vzdělávání knihovníků, kteří se tomuto tématu věnují, byla ale možnost srovnání obsahu omezená.

Posouzení stupně validity bylo svěřeno také pěti vyučujícím na oboru informační studia a knihovnictví, jmenovitě se jednalo o Mgr. Tomáše Boudu, Mgr. Michala Černého, PhDr. Martina Krčála, Ing. Martina Součka, Ph.D., Mgr. Gabrielu Šimkovou, PhDr.Ivu Zadražilovou (řazeno abecedně dle příjmení). Na základě získaných připomínek došlo k přeformulování některých vyjádření v testu a k jeho zkrácení odstraněním zavádějících a příliš složitých otázek.

Reliabilitu bylo těžké posoudit. Její úroveň se zvyšuje s počtem otázek v testu[341], na druhou stranu příliš dlouhý test by snížil počet respondentů ochotných jej vyplnit. Vzhledem k polytematickému zaměření bylo množství otázek drženo na středním doporučeném počtu[342], časová náročnost byla zvýšena jejich typem (přibližně třetina ve formě rozsáhlých baterií). Výpočet reliability má vzhledem k počtu testovaných (doporučován je výpočet na základě výsledků stovek studentů[343]) omezenou platnost, přesto však poměrně dobrou. Výpočet reliability je ovlivněn tím, že otázky nejsou homogenní a řazené do sekcí dle témat a v testu je lichý počet otázek. Výsledkem je Cronbachovo Alfa s hodnotou 0,508 a po seřazení otázek od nejjednodušších[344] Guttmanův koeficient pro metodu půlení o hodnotě 0,535. Tyto hodnoty jsou nižší než je vhodné pro didaktický test

[340] CHRÁSTKA 1999
[341] CHRÁSTKA 1999, s. 18
[342] CHRÁSTKA 1999, s. 22
[343] CHRÁSTKA 1999, s. 63
[344] CHRÁSTKA 2007, s. 200-202

(hodnoty by měly být vyšší než 0,8), ale výše uvedená omezení způsobují snížení vypočtených hodnot, proto lze i tyto hodnoty, nižší než doporučené, považovat za ne sice ideální, ale možné pro akceptování výsledku testu. Při odstranění otázek s nevyhovujícími charakteristikami (viz tabulka 5 na s. 155), vychází Cronbachovo Alfa o hodnotě 0,499 a Guttmanův koeficient pro metodu půlení o hodnotě 0,502, které se již více blíží požadované hodnotě 0,6 při tomto počtu otázek.

Do testu byly zařazeny uzavřené a polouzavřené otázky, proto bylo možné aplikovat objektivní skórování výsledků. Otázky prošly výběrem a upřesněním na základě pilotního testování. Pro každé téma byly stanoveny dvě otázky, často ve formě baterií. Pouze v případě technických řešení bylo zařazeno pět otázek vzhledem k šíři tématu a nevhodnosti použití baterie, která byla nahrazena pro srozumitelnost třemi samostatnými otázkami. Otázky byly sestavovány tak, aby nebylo testováno pouze pamětní osvojení učiva, ale také ostatní úrovně v Niemierkově taxonomii výukových cílů[345], tj. porozumění poznatků (předložení v jiné než prezentované formě), jejich použití v typových situacích a v problémových, ve výuce neřešených, situacích.

Tabulka 4 Specifikační tabulka pro test k tématu digitální stopy (dále jen DS)

Tematická oblast	**Č. otázky**	**Téma otázky**	**Úroveň dle Niemierkovy taxonomie výukových cílů**
Vymezení DS	1	Formy DS	Porozumění poznatkům
	2	Užití DS	Použití v typových situacích
Aktivní DS	3	Úroveň zneužití DS	Použití v typových situacích
	4	Deaktivace Facebooku	Použití v typových situacích
Pasivní DS	5	Zdroje pasivních DS	Zapamatování poznatků
	6	Zneužití DS	Použití v typových situacích
Řešení chováním	7	Signály manipulace	Zapamatování poznatků
	8	Formy prevence chováním	Použití v typových situacích
Technická řešení	9	Anonymní prohlížení	Zapamatování poznatků
	10	Proxy server	Zapamatování poznatků
	11	Onion Routing	Zapamatování poznatků
	12	Blokování Cookies	Použití v typových situacích
	13	Specializované nástroje	Použití v typových situacích
Legislativní možnosti	14	Vymezení osobních údajů	Zapamatování poznatků
	15	Digitální stopy při opravě	Použití v problémových situacích

[345] CHRÁSTKA 1999, s. 21

Při konstrukci testu bylo kvůli snaze o objektivní skórování využito výhradně uzavřených úloh, většina s výběrem odpovědí. V případě baterie otázek byla použita matice s výběrem odpovědí. Distraktory, příp. položky v matici, byly řazeny abecedně, aby jejich pořadí nemohlo napovídat správnou variantu. Otázky byly nezávislé, aby nedošlo ke zkreslení výsledků v návaznosti na chybnou volbu v jedné testové položce. U otázek se střídaly přístupy jedné a více správných odpovědí, respondenti vždy byli na tento aspekt upozorněni v zadání otázky. Při vyhodnocování bylo využito jednoduchého skórování, správné odpovědi jsou vyznačeny v dotazníkovém formuláři v příloze 1.3. V případě více správných odpovědí byl získaný počet bodů počítán poměrově, tj. při částečně správné odpovědi bylo skóre spočítáno poměrově dle počtu zvolených a nezvolených správných odpovědí. Vzhledem k anonymitě respondentů a možnosti volby nevím nebyla prováděna korekce na hádání[346]. V případě volby validní odpovědi a varianty *nevím* nebyla validní odpověď hodnocena, protože byla chápána jako hádání správné varianty (vztah k *nevím*).

Znalostní otázky byly ve dvou případech sebehodnotící s doplněním informace o chování pro orientační zjištění rozdílu mezi znalostmi a praktickým jednáním v oblasti bezpečnosti digitálních stop. V závěru byly zařazeny v souladu s pravidly pro tvorbu dotazníku[347] demografické otázky, otázky zjišťující formu dosud absolvovaného vzdělání v řešené problematice (pro možnost srovnání výsledků) a otázky na názor ohledně smyslu vzdělávání o digitálních stopách.

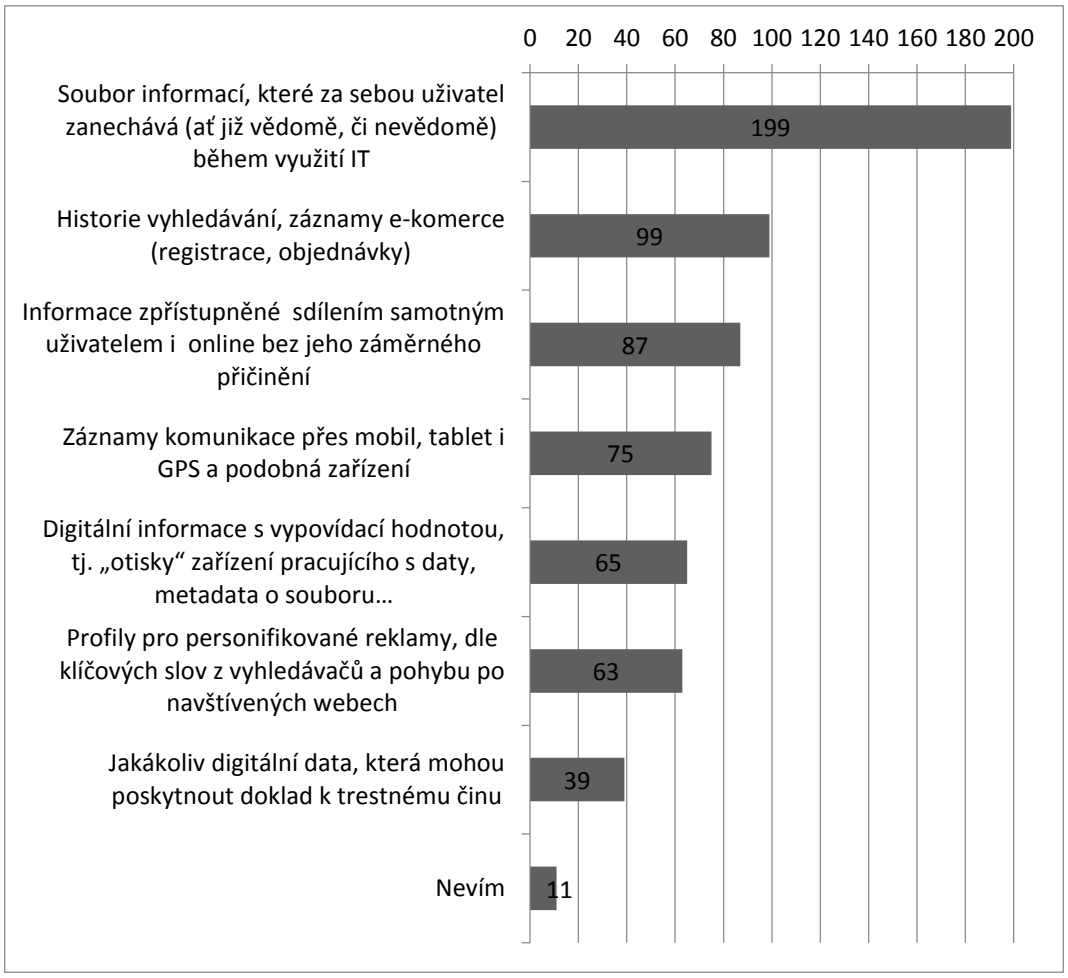
7.4.3 Výsledky výzkumu

Pro analýzu jsou významné nejen získané body s ohledem na demografické údaje, ale také volené odpovědi, které mohou ukázat správná i mylná převažující přesvědčení (znalosti). Základem je proto deskripce odpovědí u jednotlivých otázek, včetně analýzy nenormovaných odpovědí. Následně je možné s využitím otázek vyhovujících didaktickému testu srovnat hrubé skóre respondentů v závislosti na absolvovaném vzdělání a také na zájmu o řešenou problematiku. Výsledky této fáze jsou zásadní pro vyhodnocení výše uvedených hypotéz.

[346] CHRÁSTKA 2007, s. 192-193
[347] HENDL 2008, s. 168

7.4.3.1 Deskripce odpovědí při vymezení digitálních stop

První část otázek byla zaměřená subjektivní vnímání obsahu pojmu digitální stopy (graf 19) a jakou mají respondenti představu o jejich legálním i nelegálním využití (graf 21).

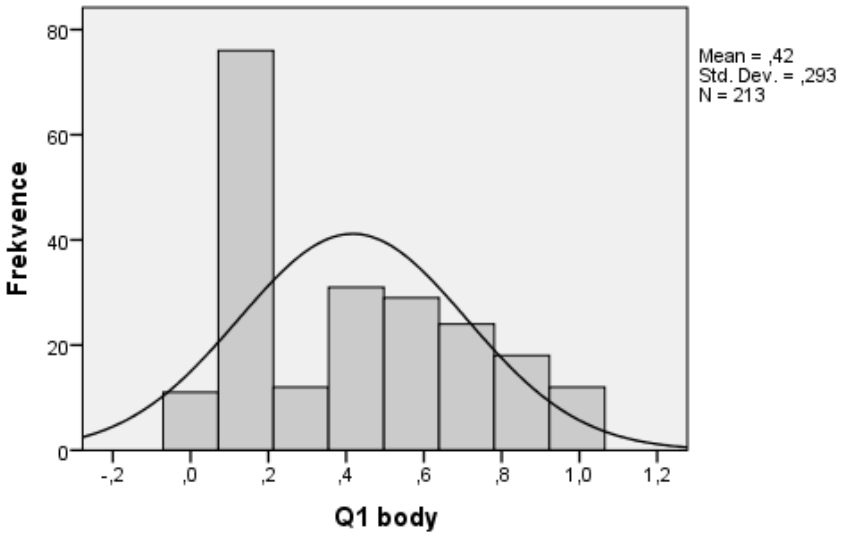


Graf 19 Vymezení digitálních stop

Přestože byla v zadání uvedena možnost volby více odpovědí a všechny nabídnuté byly správné, ve výsledcích převažuje jediná. 93,4 % respondentů označilo jako správnou odpověď „*Soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během využití informačních technologií*“. Přestože ostatní varianty jsou částečně specifičtější variace na tuto možnost, navíc často rozšiřují obsah na informace o uživateli, které zanechává někdo jiný než on sám, volilo je 18,3 - 46,5 % respondentů. 9 z 14 respondentů, kteří nezvolili nejširší

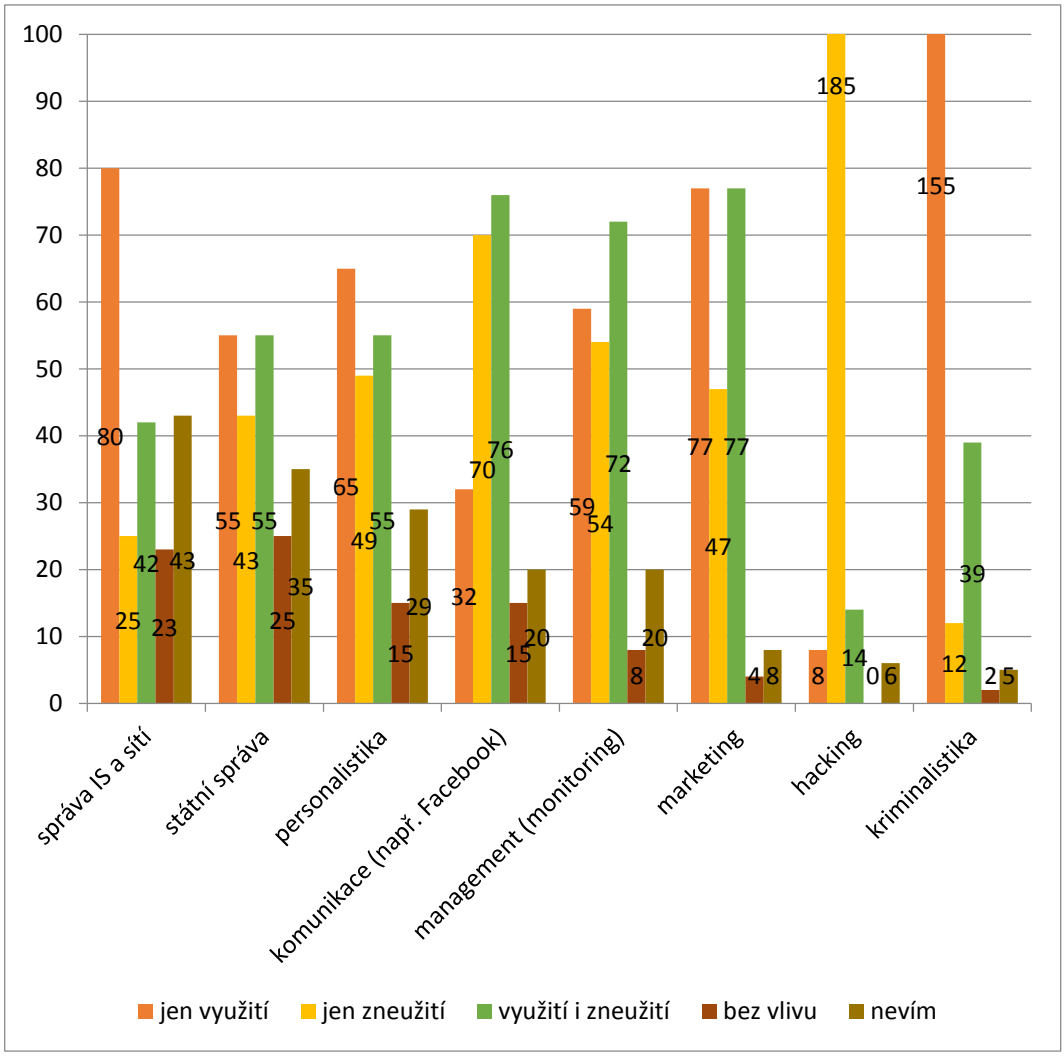
z definic, v této otázce uvedli, že neví, které z vymezení odpovídá pojmu digitální stopy. Je tedy pozitivní, že respondenti obvykle neomezují obsah pojmu na některé úzké vymezení, ale uvědomují si jeho šíři. V opačném případě by to mohlo poznamenat výsledky ostatních otázek, protože by si je respondenti vztahovali jen na dílčí typ digitálních stop. Naopak negativním poznatkem může být, že pod širokým obecným vymezením mají respondenti již omezenou představu konkrétních typů informací, které patří mezi digitální stopy.

Histogram získaných bodů za první otázku (graf 20) ukazuje rozložení, kde jasně vyčnívá modální hodnota vzdálená od ostatních středových. Výrazná je i směrodatná odchylka. Testy prokazují rozložení neodpovídající normální distribuci (Kolmogorov-Smirnovův i Shapiro-Wilkův testy s $p < 0{,}001$). Převažuje volba jediné, nejširší varianty vymezení pojmu, na kterou pojem omezila významná část dotázaných (76 respondentů, tj. 35,7 %). Celkem 61 % respondentů získalo v otázce méně než polovinu bodu, většina respondentů má tedy omezené pojetí digitálních stop. Proti tomu je normálně klesající pravá strana grafu, která ilustruje volbu více správných odpovědí. Všechny správné odpovědi označilo 12 respondentů, kteří představují 5,6 % dotázaných.



Graf 20 Body za Q1 (vymezení DS)

Po vymezení pojmu bylo zjišťováno přesvědčení o možnostech nakládání s digitálními stopami, a to v mezích zákona nebo mimo ně. Jak ukazuje graf 21, respondenti v nabízených oblastech volili velmi rozdílné přístupy.

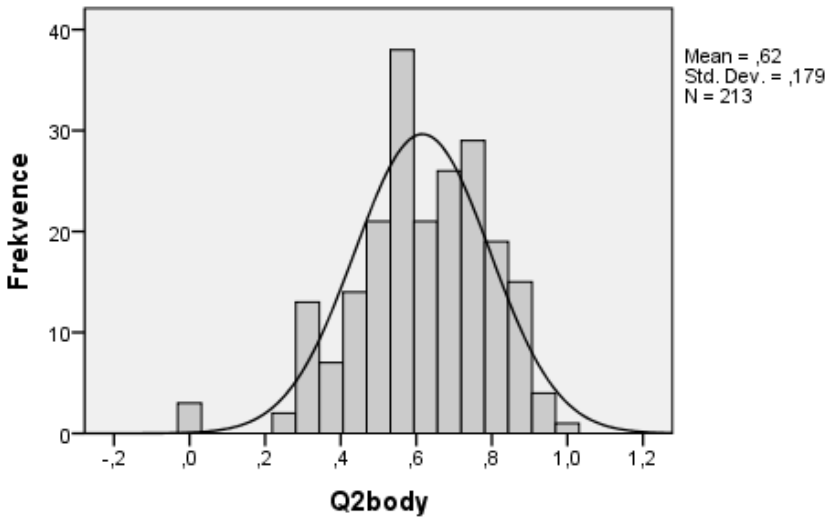


Graf 21 Pociťované oblasti využití digitálních stop

Pouze v případě hackingu se jedná o zneužití informací, což byla také převažující odpověď (86,85 % respondentů). Naopak u kriminalistiky a státní správy by se mělo jednat o využití. I zde s informacemi pracují lidé, kteří mohou informace zneužít, z hlediska jejich funkce by ale tento problém měl být omezen. V případě kriminalistiky správnou variantu zvolilo 72,77 % respondentů, dalších 18,31 % označilo i možnost zneužití, což může reflektovat již popsanou lidskou chybu. Odlišné jsou výsledky státní správy, kde čisté využití zvolilo jen 25,82 % respondentů, stejný počet jich přidal i zneužití digitální stopy a 20,19 % označilo pouze variantu zneužití. Výsledek, zejména při srovnání s kriminalistikou, naznačuje silnou nedůvěru ke státní správě při práci s digitálními stopami. To může signalizovat důvod omezeného využívání e-Governmentu vlivem nedůvěry k práci

státní správy s digitálními stopami občanů. Ostatní oblasti práce s digitálními stopami je mohou využívat i zneužívat, volba obou převažovala u marketingu, mezilidské komunikace a managementu. V případě personalistiky a správy informačních systémů a sítí byla nejčastější volbou jen využití digitálních stop, zejména v případě druhé uvedené oblasti s výraznou převahou.

U této otázky stojí za zmínku výsledek analýzy nenormovaných odpovědí. Chráska[348] uvádí, že pozornost by měla být věnována zejména otázkám, kde přesáhne počet získaných odpovědí 20 %. Tato hranice byla překročena u správy informačních systémů a sítí, blízko k ní má také oblast státní správy. Přitom právě zde bývá poměrně široký soubor digitálních stop, jehož omezení subjektem je často problematické až nemožné. O to více by respondenti měli mít povědomí, o jaké informace se jedná, jakým způsobem je zanechává a jak s nimi mohou jmenované subjekty naložit. Výsledek analýzy nenormovaných odpovědí ukazuje, kterým oblastem by měla být věnována hlubší pozornost při dalších vzdělávacích akcích cílové skupiny. Bodové rozdělení (graf 22) u této otázky je členitější a v průměru vyšší než u předchozí otázky, i zde ale nelze pracovat s normálním rozložením (prokázaly Kolmogorov-Smirnovův i Shapiro-Wilkův testy s hodnotou významnosti 1 %). Otázka je více názorová než znalostní, poměrně dobré výsledky (pravostranné zešikmení) proto mají slabší vypovídací hodnotu.

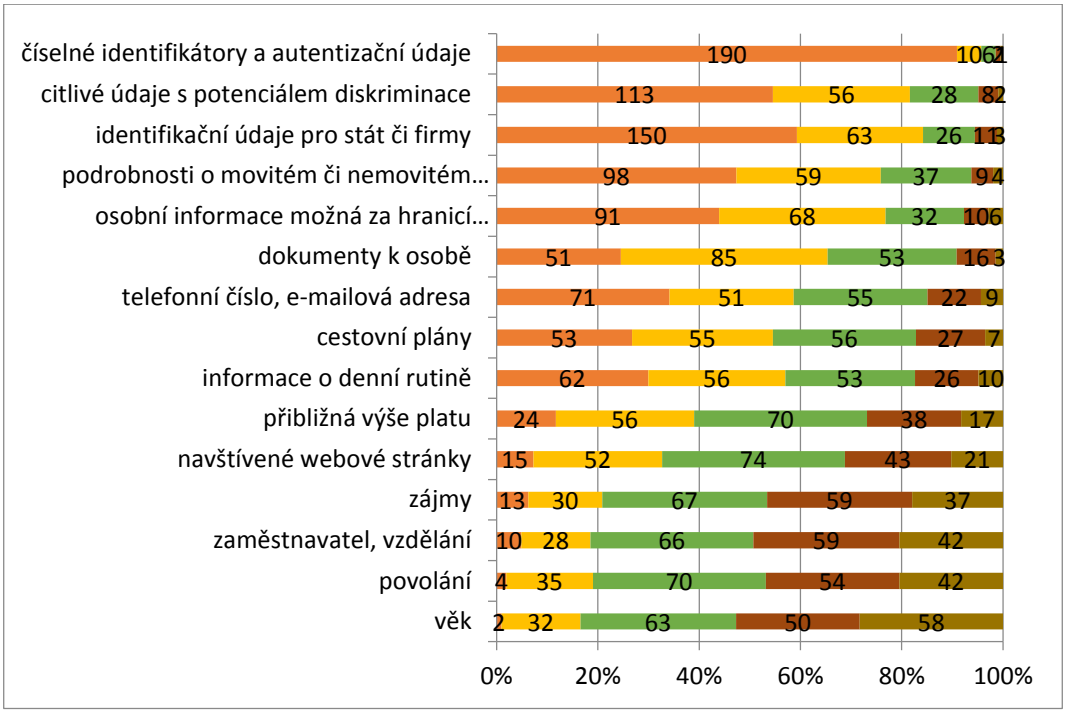


Graf 22 Body za Q2 (využitelnost a zneužitelnost DS)

[348] CHRÁSTKA 1999, 54-55

7.4.3.2 Deskripce odpovědí pro užití digitálních stop

Druhá část otázek se zaměřila na informace, které o sobě sdílí sám subjekt. Základem bezpečnosti je uvědomovat si potenciál zneužitelnosti konkrétních informací a podle jeho úrovně dbát na to, komu a zda je vůbec poskytnout. Logicky se proto nabízelo využít otázky, kde by pomocí Lickertovy škály respondenti vyjádřili své přesvědčení o zneužitelnosti konkrétních typů informací. Zjištěné frekvence jednotlivých volených odpovědí ukazuje graf 23.



Graf 23 Síla zneužitelnosti informací z digitálních stop[349]

Naprosto jednoznačně byly za nejvíce zneužitelné označeny číselné identifikátory a autentizační údaje, které oprávněně označilo za silně zneužitelné 89,20 % respondentů. Citlivé údaje s potenciálem diskriminace či za hranicí soukromí byly v tomto pořadí očekávané, vzhledem k jejich potenciálu uplatnění pro šikanu, vydírání apod., průměrná hodnota uvedené zneužitelnosti je ale překvapivě vysoká. Podrobnosti o majetku na třetí pozici dle průměrného označení zneužitelnosti představují ale ještě překvapivější výsledek. Zatímco ostatní informace lze snadno zneužít mnoha způsoby a osobami, majetkové poměry jsou

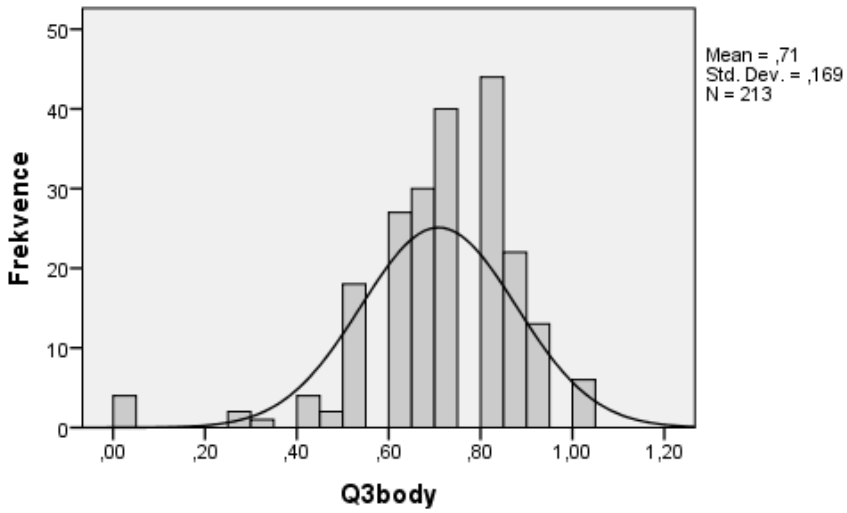
[349] Řazeno dle průměrné zneužitelnosti, škála je zleva doprava od nejvíce po nejméně zneužitelné informace, středová hodnota je označena zelenou barvou.

problematické především atraktivitou pro krádeže, příp. v omezené úrovni pro prodej. Ve srovnání s ostatními nabízenými možnostmi je ale zneužitelnost nižší. Silný kontrast je patrný při porovnání s identifikačními údaji pro stát či firmy, které se objevily až na pátém průměrném místě. Přitom identifikace vůči těmto subjektům je výchozím bodem pro krádež identity a všechny na to navázané typy útoků. Bez těchto informací není možné využití stanovené atraktivity pro firmy jmenované u majetkových poměrů.

Přibližně středových průměrů (2,15-2,9) dosáhly postupně: dokumenty k osobě (vlastní i oblíbené cizí výtvory, fotky…), telefonní číslo a e-mailová adresa, cestovní plány, informace o denní rutině (pravidelná doprava, zájmová sdružení, rozvrh…), přibližná výše platu a navštívené webové stránky. Jedná se o očekávané výsledky, které odpovídají deklarované úrovni zneužitelnosti[350] závislé na kontextu a spojení s dalšími typy údajů. Výjimku představuje přibližná výše platu, která je obvykle označovaná za slabě zneužitelnou (oproti přesné hodnotě), je proto často jednou ze demografických otázek v průzkumech veřejného mínění apod. Tento a výše vyzdvižený výsledek majetkových poměrů ukazuje, že respondenti vnímají za více zneužitelné to, co má přímou vazbu na finanční prostředky a nižší hodnotu přisuzují pouhým informacím, přestože v důsledku mohou způsobit horší poškození subjektu. Za spíše nezneužitelné byly respondenty označeny (s průměrnými hodnotami 3,26-3,5 postupně) zájmy (koníčky, zdroje, názory…), povolání, zaměstnavatel či vzdělání a věk, tyto informace nejsou příliš identifikující, výsledek je proto očekávaný.

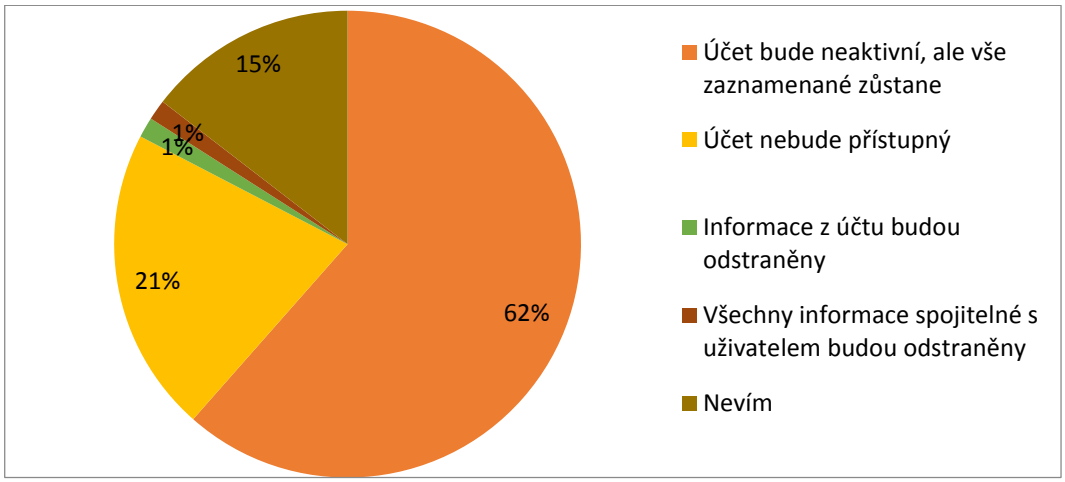
Nebylo možné jednoznačně říct, která z pěti úrovní je správná, bylo ale možné určit, jestli jde o informaci spíše zneužitelnou nebo ne, příp. v závislosti na kontextu někde mezi těmito pozicemi. Pro bodové ohodnocení proto byly za správné označeny nejen hodnoty v polích označených za správné v příloze 1.3), ale i v sousedních polích. Výsledky znázorňuje graf 24. Patrné jsou dobré výsledky respondentů pro tuto otázku (pravostranné zešikmení), které ukazují kvalitní představu respondentů o možnostech zneužití dotázaných typů informací. Ani v tomto případě testy neukazují normální rozložení hodnot.

[350] Např. KRÁL 2006



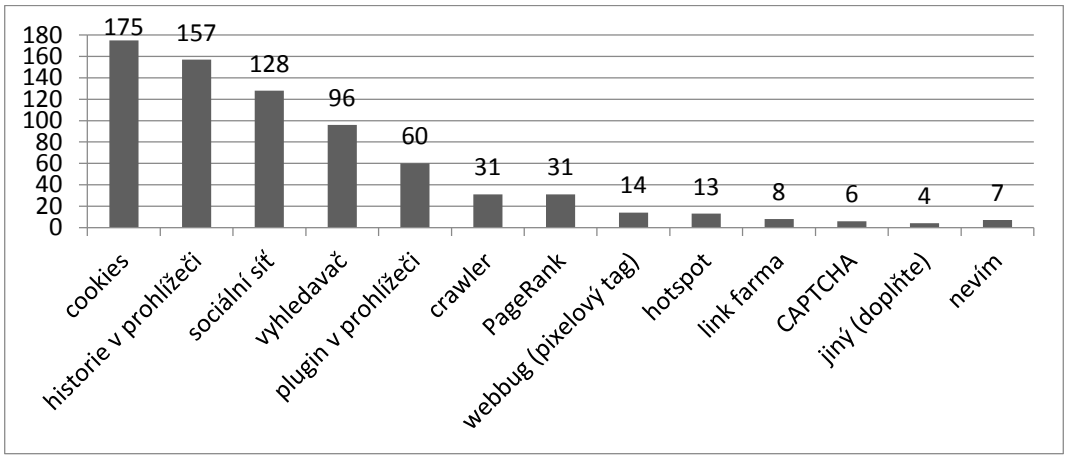
Graf 24 Body za Q3 (síla zneužitelnosti informací)

Druhá z otázek k aktivním digitálním stopám byla napojena na uvědomění si možností omezení přístupu k informacím zpřístupněným subjektem pomocí v současnosti nejrozšířenější sociální sítě v České republice. Zaměření otázky vychází z toho, že sociální sítě představují vzhledem k jejich funkcím nejbohatší zdroj zneužitelných informací. Jak je patrné z grafu 25 Výsledek deaktivace účtu na Facebooku dle knihovníků, většina respondentů zvolila správnou odpověď, dva z distraktorů byly zastoupeny velmi slabě. Je možné, že nebyly funkční, vzhledem k posouzení odborníky při zajišťování obsahové validity lze ale spíše předpokládat dostatečně dobré znalosti respondentů v tomto směru, díky čemuž získalo 61,5 % dotázaných za tuto otázku plné bodové ohodnocení.



Graf 25 Výsledek deaktivace účtu na Facebooku dle knihovníků

Následující otázka pokrývala pasivní stopy vznikající z činnosti uživatele, ale ne přímého poskytnutí informace. Jedná se především o údaje zaznamenávané softwary a internetovými nástroji. Uživatel by si měl uvědomovat jejich činnost a možné postupy pro omezení zanechávaných digitálních stop, možnosti jejich zneužití i opatření proti jejich vzniku jsou ale pro většinu lidí omezené ve srovnání s aktivními digitálními stopami, proto byla problematika zastoupena jen jednou otázkou. Správná odpověď vycházela ze znalosti pojmu a také ze znalosti fungování daného nástroje. Aby obě složky otázky plnily účel, byl mezi varianty zařazen přibližně stejný počet distraktorů jako variant jmenujících nástroje pro automatický sběr digitálních stop, frekvence volby variant ukazuje graf 26.

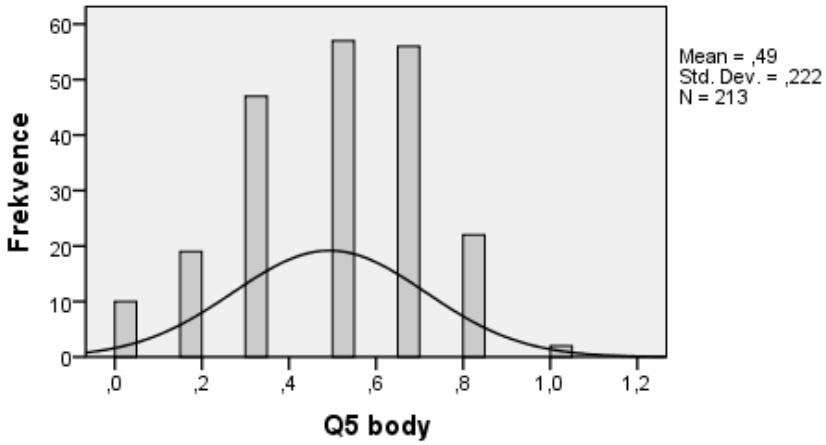


Graf 26 Známé nástroje pro automatický pasivní sběr DS

Více než polovina respondentů správně označila Cookies (82,16 %), historii v prohlížeči (73,71 %), sociální síť (60,09 %), vyhledavač (45,07 %) a plugin v prohlížeči (28,17 %). Velmi malého počtu volby dosáhl webbug (6,57 %), pozitivní ale není také méně než poloviční hodnota uvedená u vyhledavačů a pluginů v prohlížeči, proto by těmto oblastem mělo být v dalším vzdělávání respondentů věnováno výrazně více pozornosti. Nesprávně bylo v 14,55 % případů zvoleno varianty crawler a PageRank, nejedná se ale o výrazně vysoké množství, proto lze vyvodit, že distraktory fungovaly, ale současně respondenti neoznačovali slepě všechny varianty, včetně pro ně neznámých.

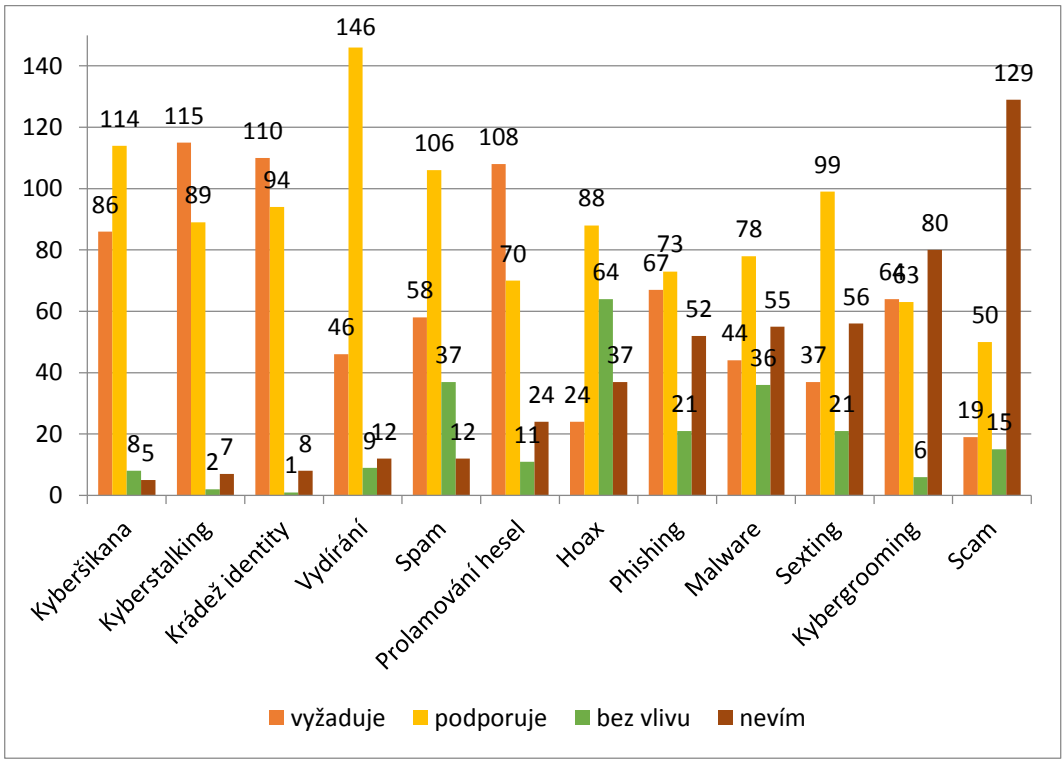
Bodové hodnocení bylo poměrně vyvážené (graf 27), přibližně v polovině možných hodnot se nachází všechny středové hodnoty. Zřetelný je vliv většího množství mírně nadprůměrného výsledku, který vyvážil 29 respondentů (13,6 %),

kteří dosáhli méně než 0,2 bodu. Naopak maximálního bodového hodnocení dosáhli jen 2 dotázaní. V případě této otázky se projevuje přísnost testů normality, které i zde nedosahují potřebných hodnost, přestože středové hodnoty i interval spolehlivosti (95 %) ukazují výsledky přibližující se normální distribuci.



Graf 27 Body za Q5 (nástroje pro pasivní DS)

Problémy, které mohou vycházet ze zneužití digitálních stop, sledovala šestá otázka. Volby odpovědí byly velmi různorodé, jak je patrné z grafu 28.

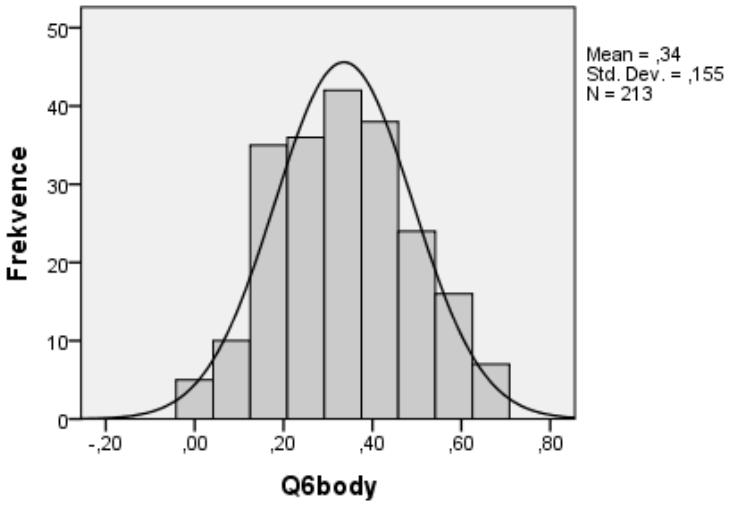


Graf 28 Upotřebení digitálních stop v hrozbách

Nejvýraznější výsledek získala varianta *podporuje* v případě vydírání, přestože to v prostředí internetu musí být spojeno se znalostí informace, která je předmětem tohoto typu útoku. I při vydírání vyhrožováním musí být přítomna informace, která by vedla k doložení oprávněnosti pohrůžky. Těsných výsledků s rozdílem méně než 3 %, ale se slabou převahou správné varianty, dosáhly oblasti kybergrooming a phishing. Větší rozdíl s převahou správné odpovědi (o 7,51 - 15,96 %) byl zaznamenán u krádeže identity, kyberšikany, kyberstalkingu, malwaru a scamu. Spam a hoax byly mezi varianty zařazeny jako distraktory, vzhledem k tomu, že z podstaty nejsou zacílené a jediná možnost, kdy by je bylo možné vztáhnout za útoky využívající digitálních stop, je odkaz na jejich zaslání pomocí e-mailové adresy, je do určité míry odůvodnitelné jejich přiřazení k jiným variantám než *bez vlivu*, která je ale vzhledem k výše uvedenému hodnocena jako správná odpověď. Jednoznačně špatné jsou silně převažující varianty u sextingu a prolamování hesel. Základní charakteristikou sextingu je šíření materiálů zobrazujících subjekt se sexuálním podtextem, tj. digitálních stop, že je ale tento typ útoku vyžaduje, zvolilo jen 17,37 % respondentů. Vzhledem k závažnosti tohoto problému se jedná o výsledek, který by měl být reflektován v dalším vzdělávání cílové skupiny. Naopak digitální stopy jen podporují prolamování hesel, i bez jejich použití je možné prolomení hesla útokem hrubou silou, proto 50,70 % respondentů volbou *vyžaduje* označilo chybnou odpověď.

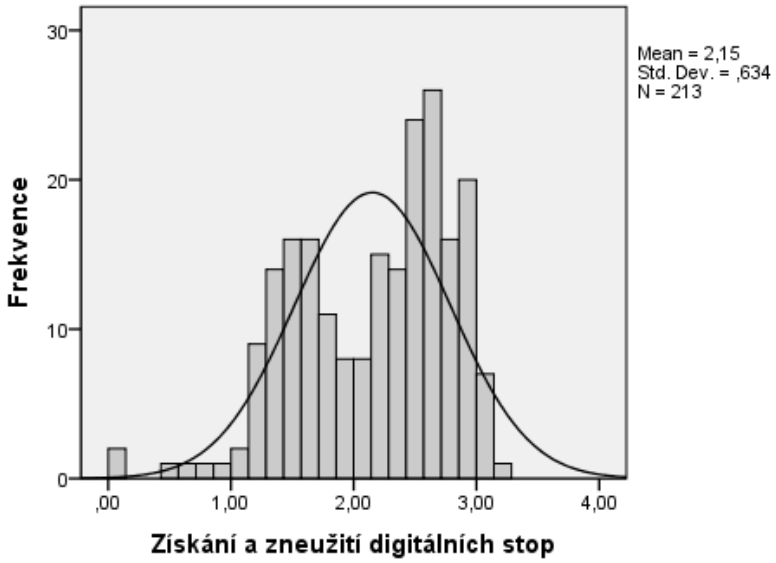
Sexting vyplynul jako téma pro další vzdělávání také z nenormovaných odpovědí, protože u něj zvolilo variantu *nevím* 26,29 % respondentů. Podobného výsledku dosáhly i malware a phishing, což je překvapivé vzhledem k tomu, že tyto problémy jsou poměrně často řešeny i v médiích a bylo tedy předpokládané vysoké povědomí o jejich fungování. Výsledky ukazují, že navzdory předpokladu je vhodné jim věnovat pozornost při dalším vzdělávání cílové skupiny výzkumu. Ještě méně rozšířená znalost byla zjištěna u kybergroomingu (37,56 %) a scamů (60,26 %), což vzhledem k možným důsledkům těchto problémů podporuje důraz na osvětu mezi cílovou skupinou. Hodnoty u scamu, kybergroomingu a malwaru mohou být mírně ovlivněny terminologií, přestože problémy jsou pod jiným označením respondentům známé. Jsou ale natolik vysoké, že i tento aspekt nesnižuje potřebu hlubší osvěty spojené s těmito typy internetových útoků.

Jak naznačovalo množství nenormovaných a chybných odpovědí popsaných výše, bodové hodnocení této otázky bylo dosti slabé (průměr i medián o hodnotě 0,33), ale poměrně jednotné, protože 69,80 % respondentů se pohybuje v bodovém intervalu o velikosti 0,25 bodu. Respondenti tedy prokázali určitou znalost v této problematice, rozhodně ji ale není možné považovat za dostatečnou. Normalita opět nebyla statisticky prokázána (graf 29).



Graf 29 Body za Q6 (útoky zneužívající DS)

Přestože bodová hodnocení otázek navázaných na vznik digitálních stop a jejich zneužití se pohybují kolem průměrné úrovně, graf 30 ukazuje, že se formují dvě skupiny respondentů, a to s podprůměrnými a nadprůměrnými bodovými hodnoceními, pochopitelně proto ani zde není normální distribuce. Předmětem dalšího hodnocení po deskripci zbývajících otázek bude proto zjištění, zda tyto skupiny odpovídají odlišnému zájmu či absolvovanému organizovanému vzdělání v oblasti internetové bezpečnosti.

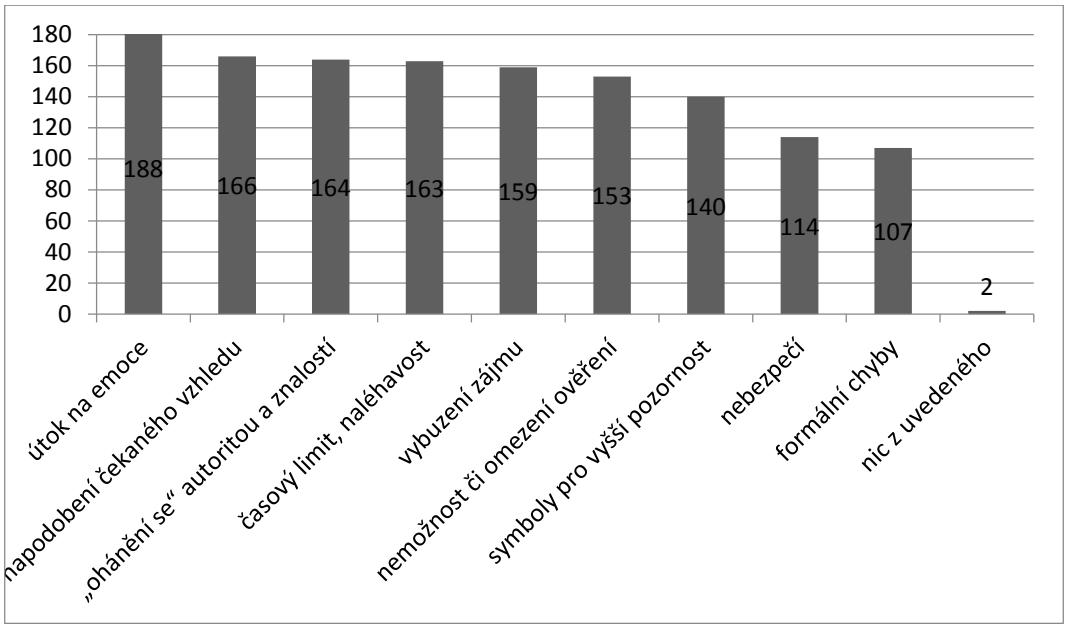


Graf 30 Body za Q3-6 (získání a zneužití DS)

7.4.3.3 Deskripce odpovědí pro ochranu digitálních stop

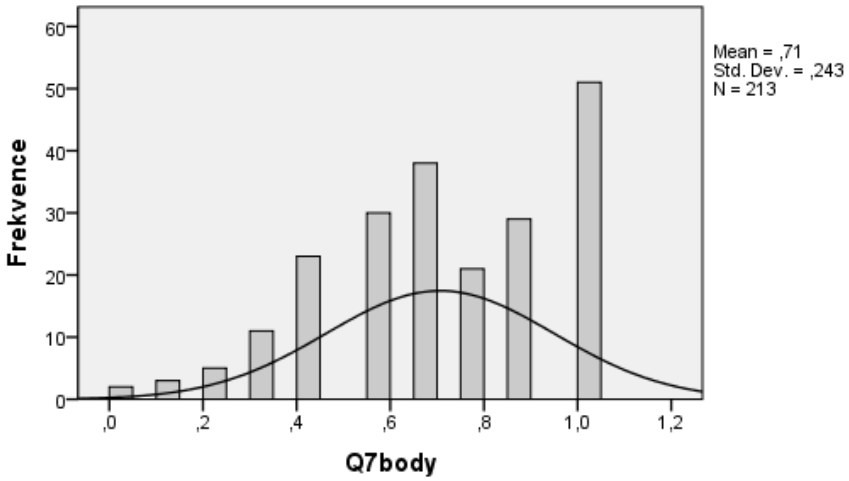
Poslední série znalostních otázek se zaměřovala na možná opatření, která mají chránit subjekt před zneužitím jeho digitálních stop. Klíčové je bezpečné chování reflektující znalost problémů pro jejich včasné rozpoznání, které by mělo být podpořeno technickými nástroji. V případě úspěšného útoku na subjekt lze pak použít legislativní možnosti, o kterých je nutné mít představu, aby si subjekt uvědomil možnost obrany.

Jak bylo popsáno v teoretické části, se zlepšujícími se technickými bezpečnostními prvky, ale stabilním lidským chováním je stále častěji při internetových útocích využíváno prvků sociálního inženýrství. Rozpoznání jeho základních možných projevů bylo předmětem sedmé otázky testu (v grafu 31 jsou pro přehlednost vynechány příklady, které měly usnadnit pochopení nabízené odpovědi, plné znění je uvedeno v příloze 1.3). Otázka obsahovala jediný distraktor (*nic z uvedeného*), který zvolili jen 2 respondenti. Každá varianta byla zvolena více než 50 % respondentů, nejčastější odpověď *útok na emoce* (88,26 %) do určité míry svou obecností pokrývá i ostatní nabídnuté konkrétní postupy. Podobně jako v případě první otázky je toto neomezení na konkrétní přístup, ale otevřenost variacím odpovídajícím obecnému vymezení pozitivním zjištěním.



Graf 31 Varovné signály manipulace

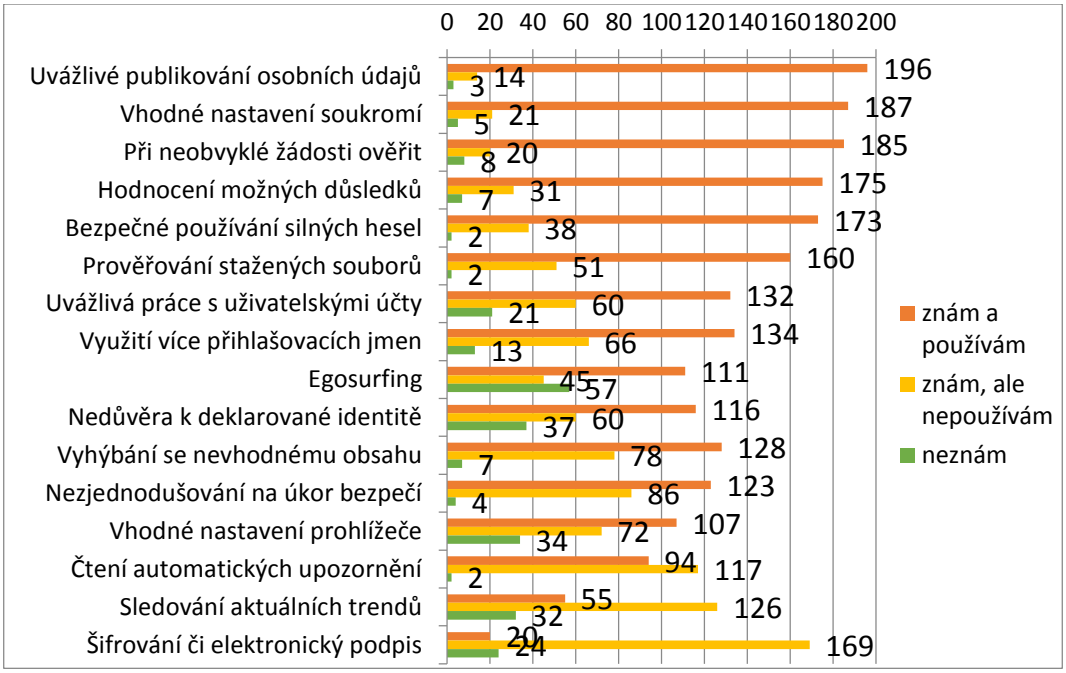
Dobrou znalost problematiky pokrývající tuto otázku dokládá i bodové hodnocení v grafu 32. Průměrné hodnocení je 0,71 bodu, nejvíce respondentů dosáhlo maxima bodů za tuto otázku a hodnota horního kvartilu je na 0,889 bodu (opět ne normální rozložení).



Graf 32 Body za Q7 (varování při manipulaci)

Osmá otázka byla sebehodnotící a snažila se nejen o zjištění znalostí, ale také reálného využívání na internetu. Jak ilustruje graf 33 (odpovědi opět byly zkráceny pro lepší zobrazení), respondenti deklarují u většiny možností, že ji nejen znají, ale i používají. Jedná se o postupy chování (např. uvážlivé publikování

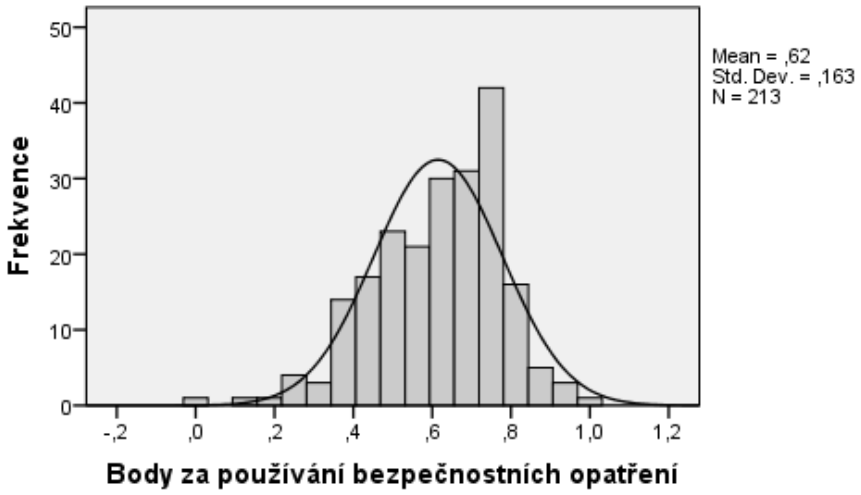
fotografií), odpovědné reakce při znalosti problémů (např. silný hesla) a použití bezpečnostních nástrojů (např. prověřování aplikacemi typu antivir všeho staženého z internetu). Výrazně nižšího počtu deklarovaného použití dosáhly dvě varianty, a to sledování aktuálních problémů a bezpečnostních řešení a šifrování či elektronický podpis, které kladou na subjekt vyšší nároky. Kromě těchto dvou možností ještě v případě čtení upozornění více respondentů zvolilo, že možnost znají, ale nepoužívají. I ta je náročnější, ale ne tolik na schopnosti subjektu, ale spíše na jeho čas, zejména v případě licenčních podmínek.



Graf 33 Znalost a použití preventivních opatření ve vlastním chování

Při analýze nenormovaných odpovědí přesáhl hranici 20 % jen egosurfing. Přestože se nejedná o náročný postup, který může ukázat mnoho problémů a pomoci si uvědomit, jaké digitální stopy jsou snadno dostupné komukoli a dle toho upravit vlastní chování, 26,76 % respondentů uvedlo, že toto opatření nezná. Hranici 10 % překročily také varianty nedůvěra k deklarované identitě, vhodné nastavení prohlížeče, sledování aktuálních problémů a bezpečnostních řešení a šifrování či elektronický podpis, velmi se k ní přiblížila také možnost uvážlivá práce s uživatelskými účty. Jak již bylo uvedeno, některé z nich kladou vyšší požadavky na subjekt, jiné jsou ale poměrně jednoduché, pokud si jich je člověk vědom. Opět tedy z výsledků vyplývají oblasti pro další rozvoj respondentů.

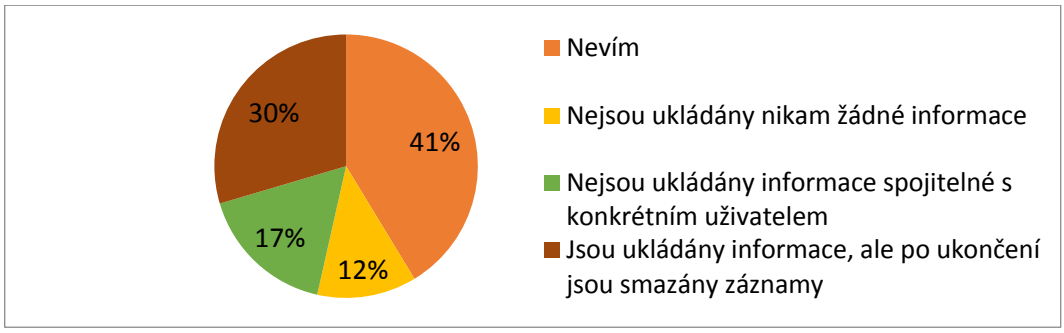
Pokud hodnotíme výsledky dle sebehodnocení znalosti bezpečnostních opatření, dosahuje maximálního počtu bodů 51,2 % respondentů a 91,2 % respondentů získalo více než 0,8 bodu, průměrné bodové hodnocení se tak dostává na hodnotu 0,92. Mnohem nižší úroveň je vykázána, pokud by bylo hodnoceno jen praktické užívání daného opatření s průměrnou hodnotou 0,615, jak ukazuje graf 34. Přesto i zde je patrné pravostranné zešikmení narušující normální distribuci. Protože je šetření položeno především jako didaktický test, pro další vyhodnocování je pracováno s výsledky reflektujícími znalost, ne použití jednotlivých opatření.



Graf 34 Body za Q8 (použití bezpečnostních opatření)

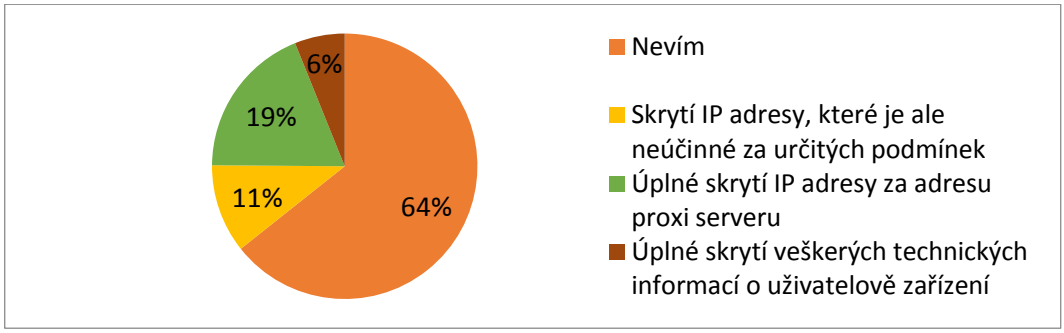
Další série otázek se zaměřila na znalosti technických možností ochrany. Všechny měly více než 70 % špatných odpovědí a distraktory byly velmi funkční, většina nulových ohodnocení byla udělena vlivem označení odpovědi *nevím*.

V případě 9. otázky o fungování anonymního prohlížení ještě 29,6 % respondentů zvolilo správnou odpověď (ukládání informací se smazáním při zavření prohlížeče), pro některou z nesprávných se rozhodlo 29,1 % dotázaných, oba distraktory získaly vyrovnaný počet voleb. Přesto i u této ne výrazně technicky náročné otázky 41,3 % dotázaných zvolilo variantu *nevím* (viz graf 35).



Graf 35 Funkce anonymního módu v prohlížeči

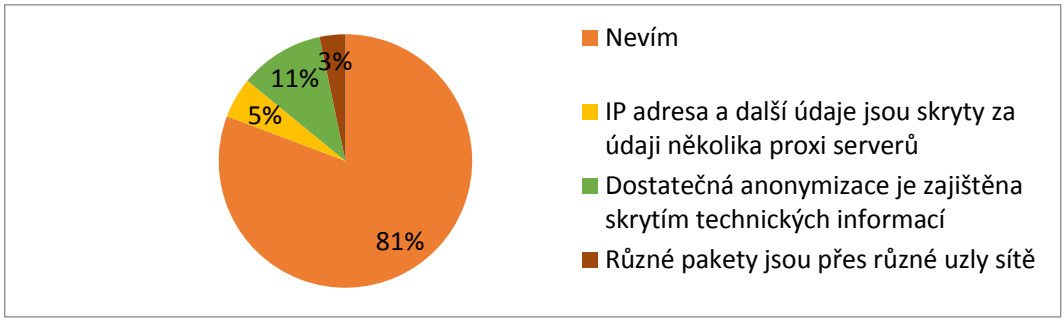
V případě těžší otázky na proxy servery bylo jen 10,8 % správných odpovědí, které patřily k variantě „*Skrytí IP adresy, které je ale neúčinné, pokud nejsou blokovány HTTP hlavičky nebo není důvěryhodný správce*“. Z 24,9 % chybných vymezení patřilo 18,8 % k variantě „*Úplné skrytí IP adresy za adresu proxy serveru, o zařízení uživatele mohou weby zjistit jen obecné technické informace (např. rozlišení obrazovky pro správné zobrazení)*“, ukazuje se neoprávněná převaha důvěry při využití technických opatření. V případě této otázky překročila hranice nevalidních odpovědí polovinu (viz graf 36).



Graf 36 Anonymizace webovými proxy servery

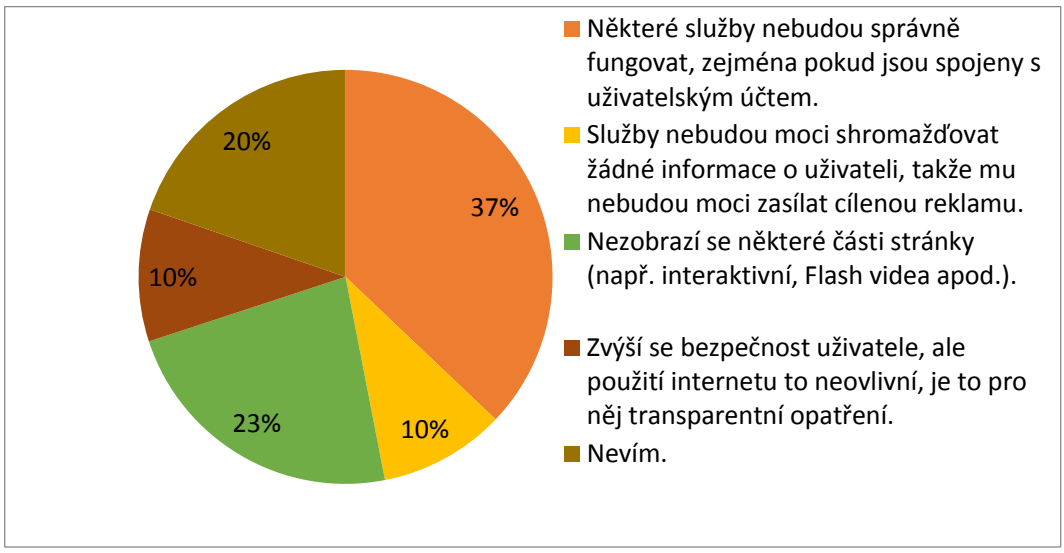
Nejtěžší otázka k anonymizaci prohlížení internetu (viz graf 37) vedla jen k 5,2 % správných odpovědí (skrytí údajů za několik proxi serverů). 14,1 % špatně zvolených vymezení směřovalo 10,8 % na variantu „*Dostatečná anonymizace je zajištěna skrytím veškerých technických informací o uživatelově zařízení několikanásobným zašifrováním (jako vrstvy cibule), jiné funkce by službu jen zpomalovaly*“, kde název řešení a odkaz na cibuli zřejmě vedly k závěru, že se jedná o správnou variantu. Distraktor tedy fungoval velmi dobře. Nevalidních odpovědí bylo zaznamenáno více než tři čtvrtiny, což je několikanásobné překročení hranice

20 % pro hlubší úvahu. Otázka tedy neposkytla mnoho podnětů k existujícím znalostem, podpořila ale přesvědčení, že respondenti opravdu netipovali, ale označovali jen odpovědi, u kterých byli přesvědčeni o jejich správnosti.



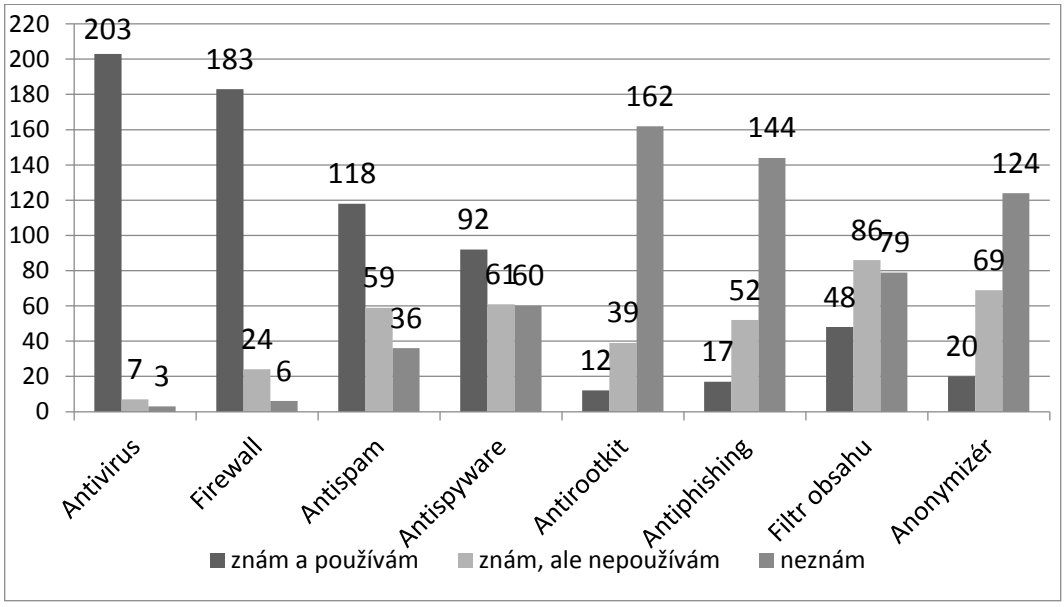
Graf 37 Funkce služeb typu onion routing

Následující odpověď směřovala na znalost omezení technických bezpečnostních opatření, které jsou často jmenovány při řešení internetové bezpečnosti. Problémy spojené s Cookies si dle výsledků 5. otázky uvědomuje většina respondentů, jejich řešení jednoduchým blokováním je sice možné, ale má své negativní důsledky. Právě na ně směřovalo ověření znalostí pomocí této otázky a nejvyšší frekvenci odpovědí získala správná odpověď. Všechny distraktory se projevily jako funkční. Problematickou hranici v této otázce ale překročil počet nenormovaných odpovědí, což ukazuje, že je zde stále prostor na zlepšování, přestože výsledky v tomto směru jsou poměrně pozitivní.



Graf 38 Důsledky zablokování cookies

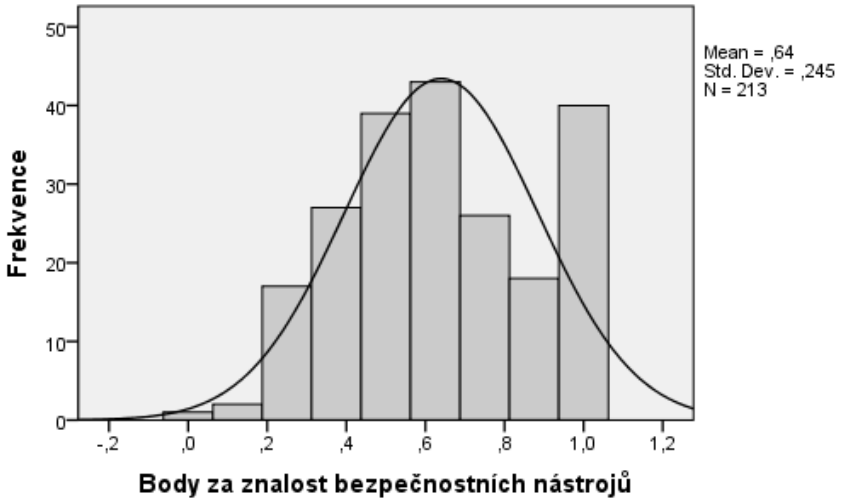
Podobně jako u bezpečnostních opatření v chování, i v případě technických nástrojů bylo sledováno nejen to, jaké z nich respondenti deklarují jako známé, ale také které uvádějí jako používané při vlastní práci s internetem (viz graf 39). Jednoznačně zde převazuje použití antivirů a firewallů, otázkou zůstává, zda si jsou respondenti vědomi toho, proti čemu je tyto nástroje chrání. Aplikace typu antispam a antispyware ještě vykazují užití poměrně vysokým množstvím respondentů, zejména u antispywaru je ale není možné označit za dostatečné, přitom právě tento nástroj patří mezi uvedenými k těm, které mají nejbližší spojitost s ochranou digitálních stop. U filtrů obsahu se již pořadí odpovědí mění, nejvíce respondentů uvedlo, že sice možnost znají, ale nepoužívají. Ostatní tři typy nástrojů zná již méně než polovina respondentů, většina z nich je pak nepoužívá.



Graf 39 Nástroje proti vytváření a využití DS

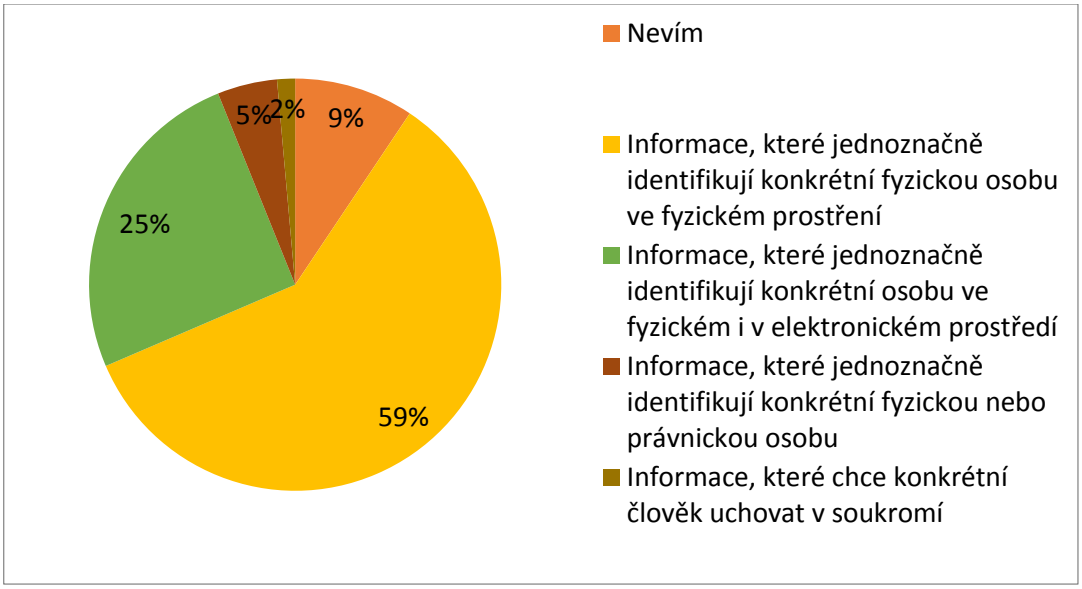
Technické nástroje mají omezené možnosti, ale při vhodném nastavení mohou dlouhodobě omezovat množství útoků a tvoří klíčový doplněk chování pro zajištění bezpečnosti. Při analýze nenormovaných odpovědí překročily 20% hranici všechny typy nástrojů kromě antiviru, firewallu a antispamu. To ukazuje silnou nedostatečnost znalostí, kterou je nezbytné reflektovat při dalším vzdělávání. Dokládá ji také bodové hodnocení za sebehodnocené znalosti znázorněné grafem 40. Při vyhodnocení bodů v případě užití nástrojů by průměrná hodnota

byla 0,41 a 74,7 % respondentů by se pohybovalo v hodnocení 0,25-0,5 bodu. Dále bude opět pracováno s body za sebehodnocení znalosti nástrojů.



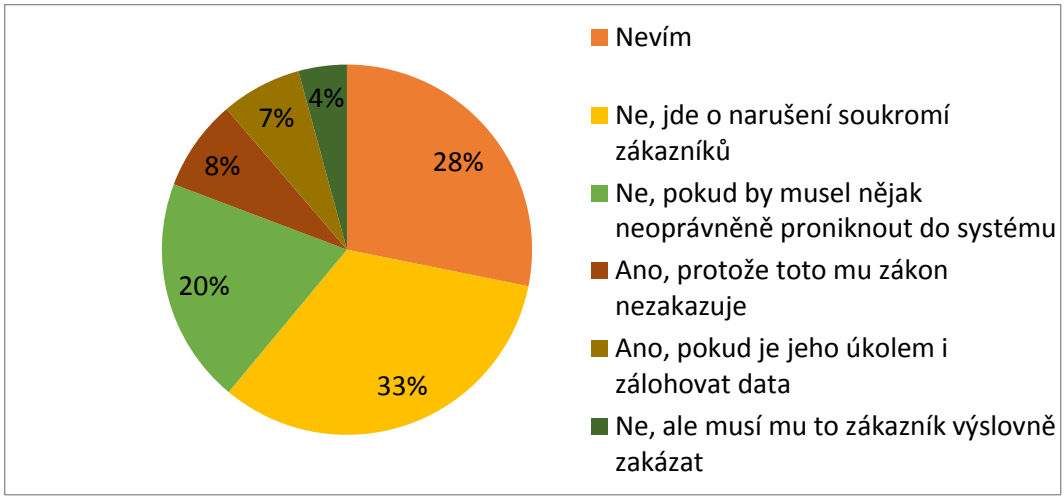
Graf 40 Body za Q13 (znalost bezpečnostních nástrojů)

Závěrečná část otázek pokrývala právní opatření pro ochranu digitálních stop. První směřovala k uvědomění si klíčového pojmu pro ochranu zákonem (viz graf 41). 59,2 % respondentů zvolilo správnou variantu vymezení osobních údajů, dva distraktory byly pravděpodobně příliš snadno odhalitelné, protože společně získaly jen 6,1 % odpovědí, zbývající se ale ukázal jako funkční (25,4 %).



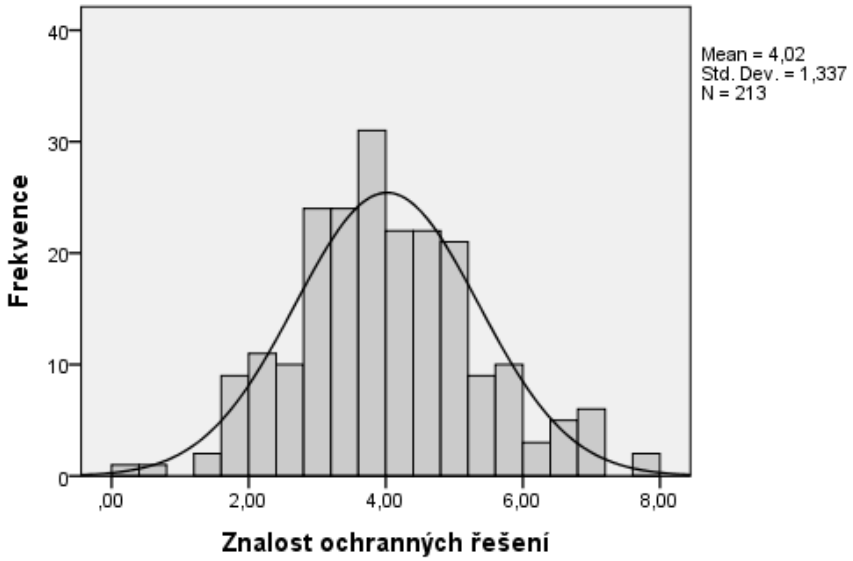
Graf 41 Vymezení osobních údajů dle zákona

Poslední znalostní otázka směřovala na aplikaci zákona do praxe a výsledkem bylo nižší množství správných odpovědí (32,9 %). Ostatní distraktory byly voleny rovnoměrně s výjimkou varianty „*Ne, pokud by musel nějak neoprávněně proniknout do systému (uhodnout heslo, využít bezpečnostní mezery informačního systému atp.); v opačném případě ano*", která svou délkou a snahou vysvětlit aspekty mohla vyvolávat dojem, že ji lze odhadnout za správnou.



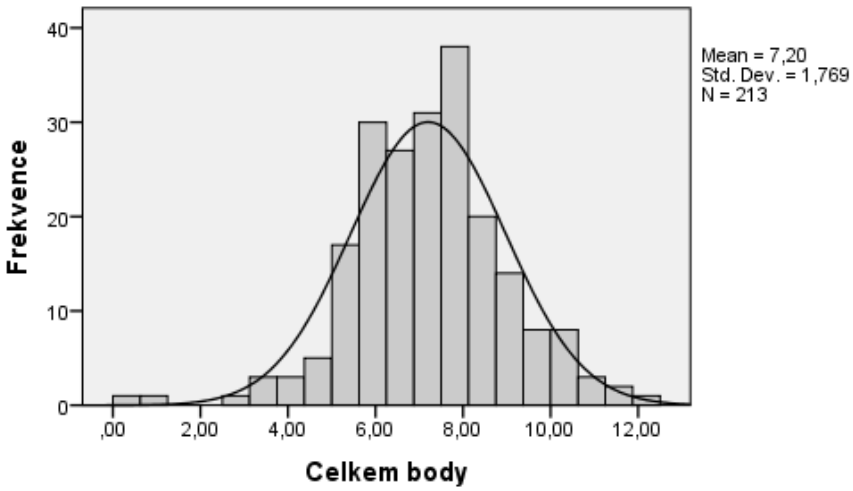
Graf 42 Legálnost prohlížení dat v opravovaném počítači

Při podobném spojení výsledků, jako bylo u problémů s digitálními stopami, je vytvořen přehled bodového hodnocení za všechny otázky k ochraně proti těmto problémům. V něm je rozložení odlišné, jak ukazuje graf 43. Průměrný počet bodů je pod polovinou maximálního počtu. Nejsou ale patrné podobně oddělené skupiny jako v případě předchozí série otázek. Naopak v tomto případě již Kolmogorov-Smirnovův test vykazuje normální rozložení (signifikance 0,2 představuje spodní hranici významnosti), Shapiro-Wilkův test ale ještě nedosahuje kritických hodnot (signifikance 0,299), právě druhý uvedený test je z hlediska počtu respondentů reprezentativnější.



Graf 43 Body za Q7-Q15 (ochrana DS)

V celkovém hodnocení není patrné členění na více vrcholů, projevuje se ale menší množství velmi slabých výsledků a naopak výrazný počet respondentů se pohybuje okolo průměrného bodového hodnocení, které je velmi slabě nad polovinou maxima bodů (graf 44). Hodnota průměru (7,202) a mediánu (7,218) jsou téměř totožné a interval spolehlivosti je poměrně úzký <6,9631; 7,4409>. I zde testy normality vychází podobně jako v případě série otázek na bezpečnostní řešení, hodnoty ale již splňují kritéria normality (Kolmogorov-Smirnov test s významností 0,200 a Shapiro-Wilkův test s hodnotou 0,002). Celkové bodové hodnocení samo o sobě není natolik zásadní z hlediska cíle šetření, jako distribuce hodnocení dle demografických otázek, kterým je věnována následující část práce.



Graf 44 Body za Q1-Q15 (celkové hodnocení)

7.4.3.4 Vlastnosti testových úloh pro třídění 2. stupně

Vzhledem k tomu, že test proběhl jednorázově, nebylo možné provést optimalizaci. Je ale vhodné pro interpretaci výsledků a další testy zohlednit vlastnosti jednotlivých úloh. Proto byly analyzovány obtížnost a citlivost testových úloh (viz tabulka 5) a nenormované odpovědi, které byly popsány výše při deskripci odpovědí na jednotlivé otázky.

Tabulka 5 Obtížnost a citlivost testových úloh

Otázka č.	Q1	Q	d	r_{tet}	$_{b}r_{bis}$
1	5,16*	61,03	,330	-,4737*	,3943
2	1,41*	18,31**	,226	-,7375*	,4577
3*	1,88*	6,10*	,085*	-,2768*	,4008
4	38,50	38,50	,264	-,4175*	,3467
5	4,69*	35,68	,377	-,5923*	,4674
6	2,35*	77,93	,198	,8291	,3202
7	,94*	20,66	,585	-,4866*	,4032
8	,47*	,94*	,981	1,0000	,3576
9	70,42	70,42	,330	-,9948*	,3912
10	89,20*	89,20*	,142**	-,9862*	,3398
11*	94,84*	94,84*	,085*	-,5818*	,2821
12	62,91	62,91	,340	,9724	,3968
13	,47*	22,07	,274	-,2714*	,4922
14*	40,85	40,85	,123*	-,9987*	,2135
15	67,14	67,14	,151**	,6912	,2434

(* označuje nevyhovující koeficienty, ** značí hodnoty blížící se kritické hodnotě koeficientu)

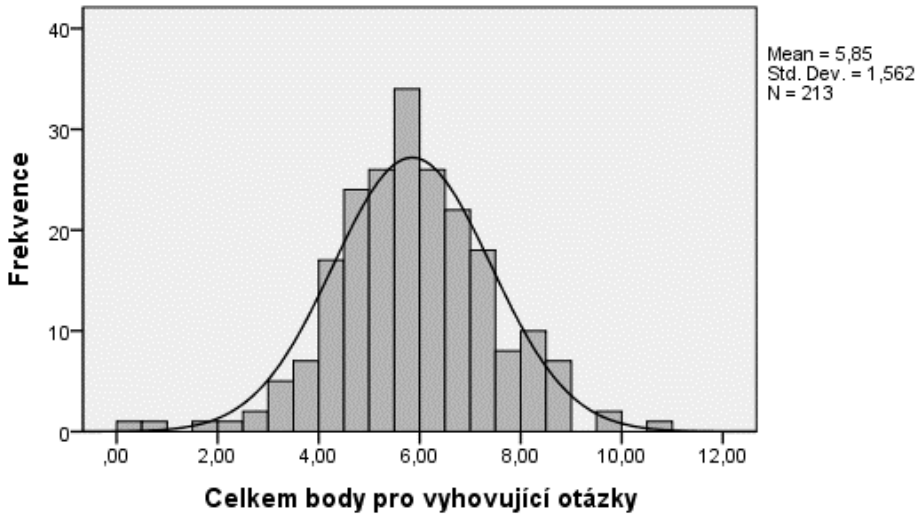
Vzhledem k tomu, že v testu byly otázky často složeny z dílčích složek a s možností více odpovědí, bylo očekávané, že hodnota obtížnosti při výpočtu z otázek, které byly zodpovězeny zcela špatně, bude velmi nízký, což se také potvrdilo (viz hodnota Q1 v tabulce 5). V testu z toho důvodu nebylo hodnoceno postupem *všechno a nic*, ale byla přidělována poměrová část při částečně správné odpovědi. Proto pro hodnocení testových otázek byla hodnota obtížnosti stanovena na základě počtu odpovědí, kde respondenti dosáhli minimálně 0,5 bodu (viz hodnota Q v tabulce 5). Tím se snížil počet nevyhovujících otázek kvůli nízké hodnotě obtížnosti[351] z osmi na tři, z nichž jedna se blíží ke stanovené hodnotě. Dvě otázky v obou přístupech byly vyhodnoceny naopak jako velmi obtížné, jedná se o technické možnosti anonymního prohlížení internetu. Vzhledem k hodnocení

[351] Otázky příliš snadné mají hodnotu Q > 20, velmi obtížné Q < 80 (CHRÁSTKA 1999, s. 47)

obtížnosti pro respondenty je vhodné tato témata akcentovat při dalším vzdělávání respondentů. Hodnoty obtížnosti mimo doporučenou úroveň nejsou překážkou pro zařazení otázek do testu, pokud jich není příliš mnoho, jednoduché otázky totiž odbourávají obavy dotazovaných, příliš obtížné otázky naopak ukazují, kde je přibližně hranice znalostí respondentů a že celý test není příliš povrchní.

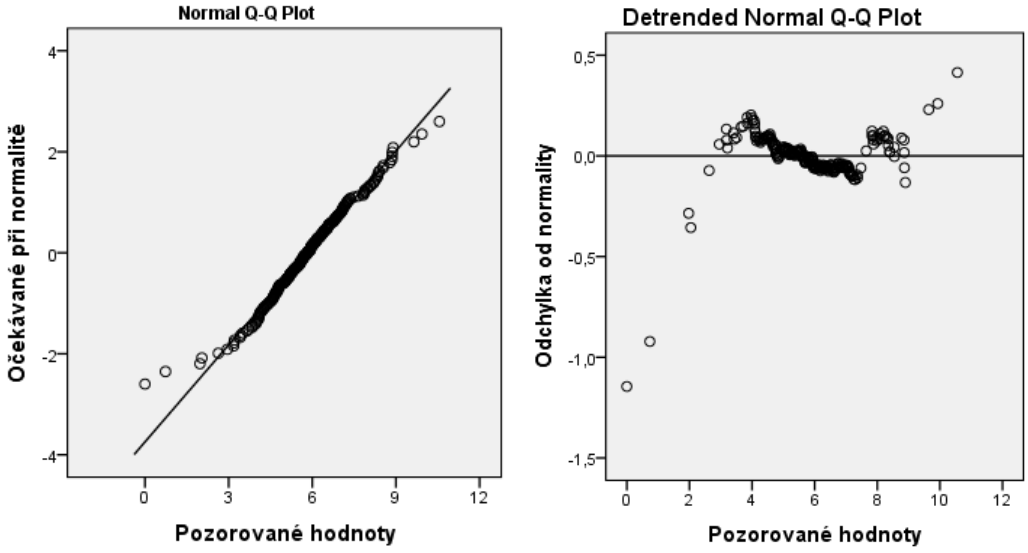
Zásadní pro ponechání otázek v testu je hodnota citlivosti, tj. schopnost rozlišit dotazovaného s vyššími znalostmi od toho s nižšími znalostmi. Vzhledem k lichému počtu respondentů byla citlivost počítána z 50 % nejhorších a nejlepších s vynecháním jedince přímo ve středu dle bodového hodnocení. Chráska[352] pro hodnocení citlivosti doporučuje tři typy koeficientů: koeficient ULI (upper-lower-index, v tabulce 5 označovaný d), tetrachorický koeficient (r_{tet}) a bodově biseriální koeficient ($_br_{bis}$). Přestože všechny mohou nabývat hodnot <-1; 1> se stejnou interpretací, i když s odlišnými kritickými hodnotami, je patrné, že výsledky hodnocení citlivosti jsou různé. Zatímco bodově biseriální koeficient citlivosti vyšel u všech úloh jako vyhovující (kritická hodnota 0,20), naopak tetrachorický koeficient nabýval u 11 z 15 otázek nevyhovujících hodnot (pod 0,15). Proto bylo pro rozlišení úloh o nevyhovující citlivosti využito zbývajícího koeficientu ULI (kritické hodnoty pro Q = <30; 70> ULI ≥ 0,25 a Q = <20; 30> ∪ <70; 80> ULI ≥ 0,15) a za nevyhovující byly hodnoceny otázky 3 (škálování informací podle úrovně zneužitelnosti), 11 (Onion Routing) a 14 (definice osobního údaje). Především u otázek 3 a 14 se jednalo o překvapivé zjištění, v obou případech byly hodnoty kladné, ale nedostatečné, nedochází však stále ke zvýhodnění slabých studentů, jak by ukazovaly záporné hodnoty. Otázky 10 a 15 sice také nevyhovují kritériím, jejich hodnoty jsou ale blízké hraničním, proto byly ponechány pro další testování hodnot. Z citlivosti vyplynulo problematické postavení otázek spojených s právními postupy. Možným důvodem je, že tyto otázky jsou řešeny respondenty i mimo oblast internetové bezpečnosti, a to i v rámci jejich formálního a dalšího vzdělávání, proto tato oblast neodpovídá citlivosti hodnocení otázek blíže spojených s řešenou problematikou. Otázky s nevyhovující citlivostí byly z dalších analýz vyřazeny. Změnu ve výsledném bodovém hodnocení prezentuje graf 45, patrná je výraznější distribuce hodnot.

[352] CHRÁSTKA 1999, s. 49-51



Graf 45 Výsledné bodové hodnocení vyhovujících otázek

Vzhledem k hodnocení dalších charakteristik respondentů a jejich vlivu na bodové hodnocení je pro statistické testy nezbytné ověření normality rozložení celkového hodnocení za vyhovující otázky. Shapiro-Wilkův test sice neukazuje statistickou významnost, Kolmogorov-Smirnovův test ale ano, byť na spodní hranici významnosti. Vzhledem ke grafu 46 je možné rozložení označit za normální s odlehlými pozorováními na obou koncích[353] a pro další testování lze použít i parametrické testy.



Graf 46 Normalita vyhovujících otázek

[353] HENDL 2006, s. 149

Dalším zásadním testem při vyhodnocování charakteristik znalostních otázek je jejich interkorelace, jejíž pomocí lze ověřit, do jaké míry testují stejnou oblast. Není nezbytné, aby interkorelace byly silné mezi všemi otázkami, ale alespoň v rámci stanovených kategorií by měl být vztah průkazný, aby bylo možné konstatovat správné nastavení znalostních otázek. Z tabulky 6 je patrné, že korelace se vyskytují jen v několika málo případech, a to vždy jen na úrovni nízkého stupně korelační závislosti. Mezi kategoriemi se neobjevují vyšší závilosti. To ukazuje na problémy ve stanovení testových otázek, které během přípravy nebylo možné odhalit, znemožňují však test posunout ke standardizaci. Pozitivním zjištěním však je, že negativní korelační hodnoty nikdy nepřekročily hodnotu, aby bylo možné pozorovat opačnou závislost, tedy kdyby byly otázky nastaveny zcela špatně.

Tabulka 6 Interkorelace znalostních otázek

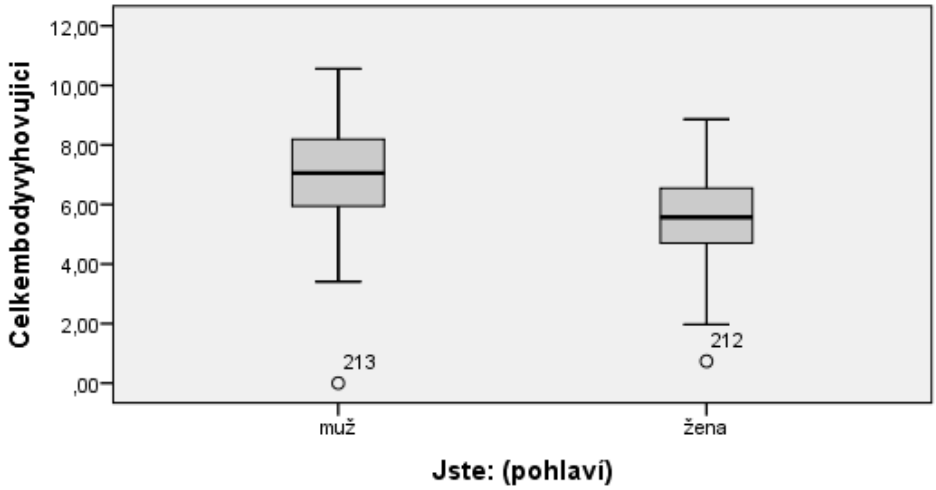
	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**	**Q13**	**Q14**	**Q15**
Q1		,272	,142	-,042	*,303**	,113	,161	,145	,092	,118	,072	,022	,118	-,006	-,059
Q2			,266	,069	,195	,155	,272	*,446**	,115	,102	,049	,140	*,333**	-,024	-,018
Q3				,025	,188	,140	,183	*,308**	,127	-,021	,034	,166	,217	,025	-,099
Q4					,091	,105	,112	,203	,132	,058	,054	-,032	,171	-,088	,040
Q5						,016	,198	,209	,090	,159	,263	,076	,232	,031	,030
Q6							,053	,281	,129	,003	,054	,135	*,321**	,049	,054
Q7								*,300**	,059	,054	,156	,124	,219	-,009	-,069
Q8									,113	,116	,113	,154	*,531**	,092	,009
Q9										,106	,081	,141	,224	,015	-,125
Q10											,192	,077	,266	-,019	,046
Q11												,128	,192	,021	,063
Q12													,248	,084	-,020
Q13														-,028	,101
Q14															,073
Q15															

* Průkazná korelační závislost

7.4.3.5 Vliv pohlaví a přesvědčení o smyslu problematiky

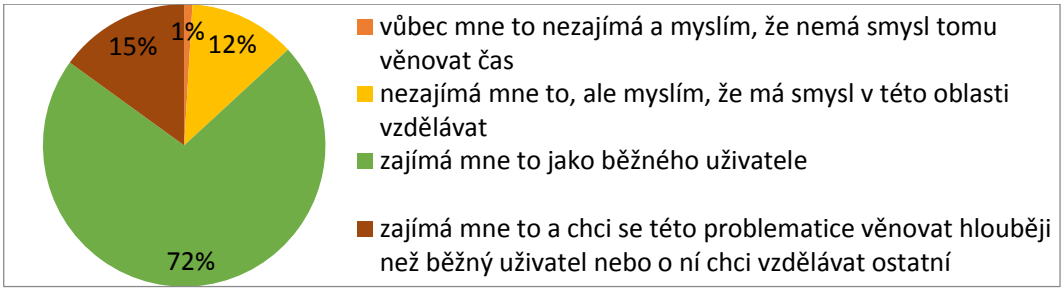
Zbývající otázky v dotazníku nebyly určeny ke zjišťování znalostí, ale charakteristik respondentů, vzdělání a názorů na vzdělávání o digitálních stopách. Jediná demografická otázka cílila na pohlaví respondentů. Výsledný poměr 172 žen ku 41 mužům ukazuje nevyváženost zastoupení ve vzorku, výsledek je ale

nepochybně ovlivněn tím, že v cílové skupině respondentů, ať už mezi studenty ISK nebo pracovníky knihoven, je zastoupeno více žen než mužů. Při srovnání bodového hodnocení dle pohlaví jsou patrné lepší výsledky mužů než žen (graf 47), pokud dále srovnáme průměrné bodové hodnocení v otázkách více technických (otázky č. 4, 5, 9, 10, 12, 13) a více zaměřených na chování uživatele (otázky č. 1, 2, 6, 7, 8, 15), v případě prvního jmenovaného typu je výrazně větší rozdíl mezi pohlavími (rozdíl průměrů 0,1708) než u otázek k chování (rozdíl průměrů 0,0419). Rozdíly jsou tedy dány především technicky zaměřenými otázkami, které jsou obecně častěji doménou mužů. Poměrně zajímavým poznatkem je, že v oblastech vymezení a problémů s digitálními stopami se výsledky dle pohlaví téměř neliší, ale u ochranných možností mají muži výrazně lepší výsledky (r = 0,5) proti ženám (r = 0,3125), bez překrytí 95 % intervalu spolehlivosti.



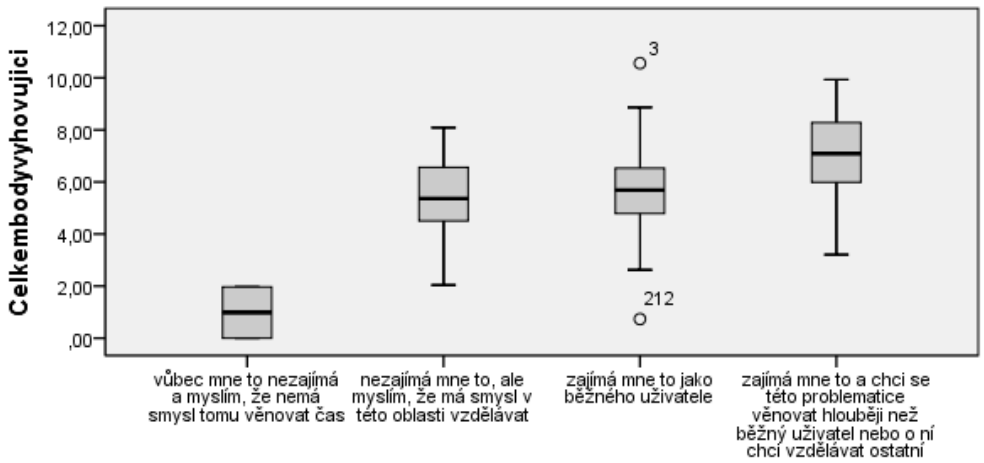
Graf 47 Celkové bodové hodnocení dle pohlaví

Podstatnou proměnnou pro hodnocení bylo podle předpokladu, jaký zájem pociťuje respondent o řešenou problematiku. Jasně převažovala se 71,8 % varianta zájmu z pozice běžného uživatele, pozitivní je ale zjištění 15 % respondentů, kteří by danou problematiku chtěli prohlubovat u sebe či ostatních, což je základní předpoklad pro rozvoj řešené problematiky v praxi i pro smysluplnost dále navržené metodiky vzdělávání.



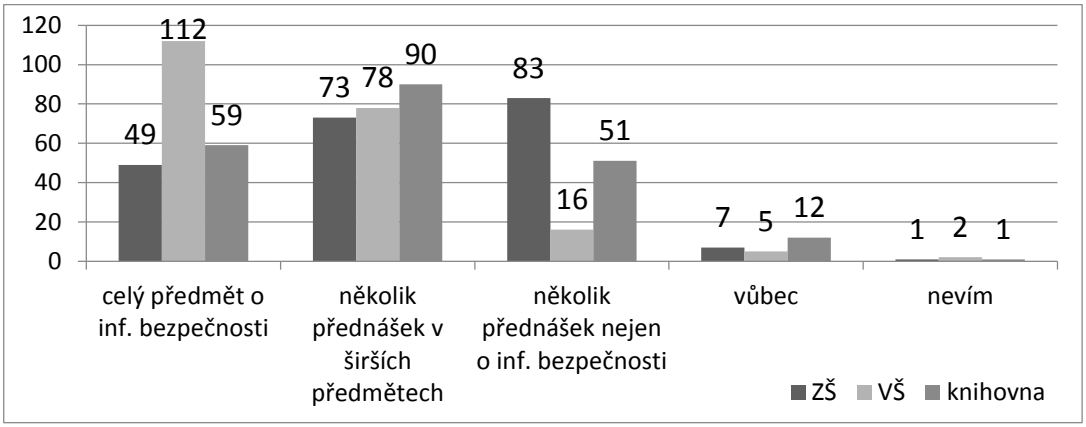
Graf 48 Sebehodnocení zájmu o téma digitálních stop

V souladu s očekáváním se při hodnocení dle zájmu o téma (viz graf 49) objevily rozdíly, výsledky skupiny bez přesvědčení o jeho smyslu jsou limitovány malým zastoupením. Nicméně ostatní skupiny jsou zastoupeny dostatečně, lze proto brát v úvahu blízkost výsledků bežných uživatelů a nezajímajících se o téma, kteří ale vidí jeho smysl, a naopak lepší výsledky nejvíce zaujaté skupiny (rozdíl průměrů u zaujatých proti běžným uživatelům je 1,2429 bodu). Při dalším hodnocení rozdílů dle charakteristiky zájmu v rámci bodového zisku v dílčích kategoriích otázek se projevuje rozdíl v oblastech techničtěji zaměřených otázek proti těm směřujícím k chování uživatelů. Podle témat nebyly prokázány rozdíly proti celkovému hodnocení v žádné z kategorií, jen oblast užití digitálních stop vykazuje výrazně širší intervaly bodových zisků s minimálními rozdíly průměrů. Z toho lze vyvodit, že hlubší zájmem o problematiku vede respondenty k rozvoji techničtěji zaměřených oblastí problematiky, zatímco ty spojené s lidským užitím technologií jsou u respondentů poměrně srovnatelně známé.



Graf 49 Celkové hodnocení dle zájmu o digitální stopy

Související charakteristiku respondentů představují názory na vzdělávání o digitálních stopách v různých institucích. Výsledek (graf 50) ukazuje převahu přesvědčení o smyslu vzdělávání v této oblasti. Že by se o ní vzdělávat nemělo, bylo nejčastěji uváděno u knihoven, ale i zde jen v 5,63 % případů. Co se týká pozitivních reakcí, v případě základního školství převažuje varianta několika málo přednášek jen souvisejících s informační bezpečností. Jen o 4,70 % méně respondentů se přiklonilo k zahrnutí tématu do šířeji pojatého předmětu. Obě tyto varianty jsou reálné v prostředí současného základního školství více, než samostatný předmět o informační bezpečnosti, ke kterému se přiklání 23,00 % dotázaných. Pro středovou úroveň vzdělávání z nabízených variant se rozhodlo nejvíce respondentů v případě knihoven (42,25 %), vyšší i nižší pojetí bylo srovnatelné (kolem 25 %). Nejjasnější přesvědčení bylo vyjádřeno u vysokých škol, kde se pro samostatný předmět o informační bezpečnosti rozhodlo 52,58 % dotázaných. Dotázaní projevili silné přesvědčení o tom, že by se mělo o digitálních stopách vzdělávat ve všech sledovaných institucích, i když na různé úrovni rozsahu, z čehož je patrné, jak silný význam této problematice přikládají.

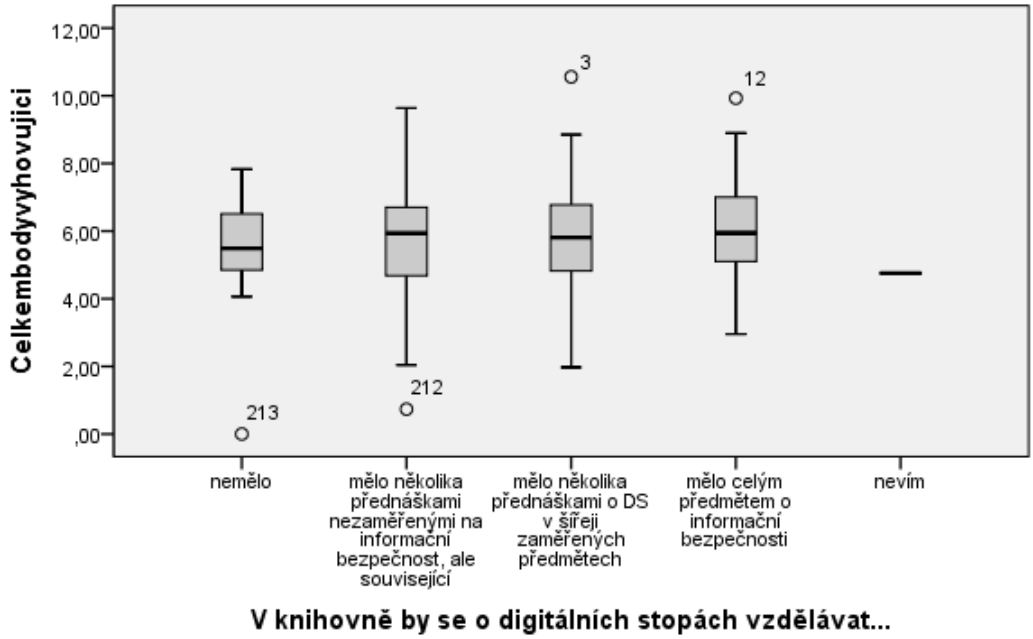


Graf 50 Názory na vzdělávání o DS na různých úrovních

Na druhou stranu je nutné zohlednit, že výběrem respondentů je zájem ovlivněn, protože odpovědi na dotazník se při použitém způsobu oslovení z velké části rozhodnou zanechat lidé, kteří mají o řešenou problematiku zájem. Výsledky negativního přístupu ke vzdělávání v této oblasti jsou ale zastoupeny natolik

minimálně, že je pravděpodobné, že by při reprezentativním vzorku byl pozitivní přístup opět převažující, i když ne natolik výrazně.

V hodnocení podle přesvědčení o úrovni vzdělávání nejsou významné rozdíly. Proto nejsou uvedeny všechny tři grafy distribuce výsledků, které jsou podobné. Vzhledem k cíli šetření je uveden jen graf 51 Celkové hodnocení dle názoru na vzdělávání v knihovnách. Nevybočuje ani varianta *nemělo* od výsledků pozitivních názorů. Obecný názor na vzdělávání o digitálních stopách tedy nemá pro výsledky takový vliv, jako osobní zájem respondenta. Přestože obě jmenované otázky směřují k zájmu o vzdělávání k této problematice, jeden na úrovni osobní pro knihovníka, druhá na zprostředkované uživatelům knihovny, bodové výsledky se liší. Test nezávislosti proměnných Chí-Kvadrát (po vyloučení nedostatečně zastoupených proměnných *nevím* a *nemá smysl*) ukázal nejvýraznější nezávislost mezi osobním zájmem o problematiku a názorem na vzdělávání v knihovnách ($p = 0{,}787$), naopak k závislosti na 5 % hladině významnosti se blíží u názoru na vzdělávání na vysoké škole ($p = 0{,}59$).



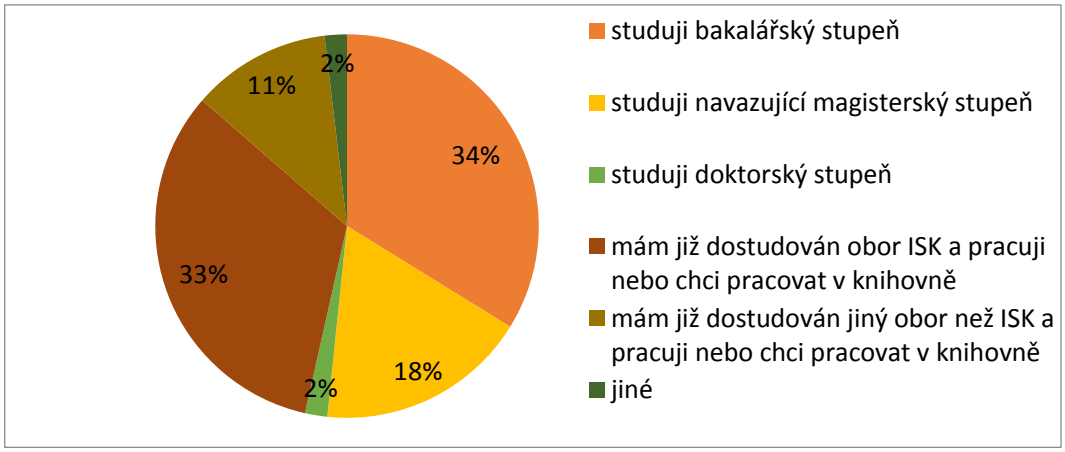
Graf 51 Celkové hodnocení dle názoru na vzdělávání v knihovnách

Rozdíl v bodovém hodnocení je ve prospěch většího rozdílu u osobního zájmu. Současně je ale patrné, že pro rozvoj znalostí nestačí přesvědčení o podstatnosti problematiky, dokud si ji nespojí se svou osobou. Je tedy nezbytné,

aby nebyli jen přesvědčováni o tom, že má smysl zabývat se digitálními stopami, např. kvůli možným důsledkům v podobě jejich zneužití, ale spíše se zaměřit na to, proč by právě knihovníci měli zasáhnout více do této oblasti, a to jak vzděláváním seba sama, tak i uživatelů knihovny.

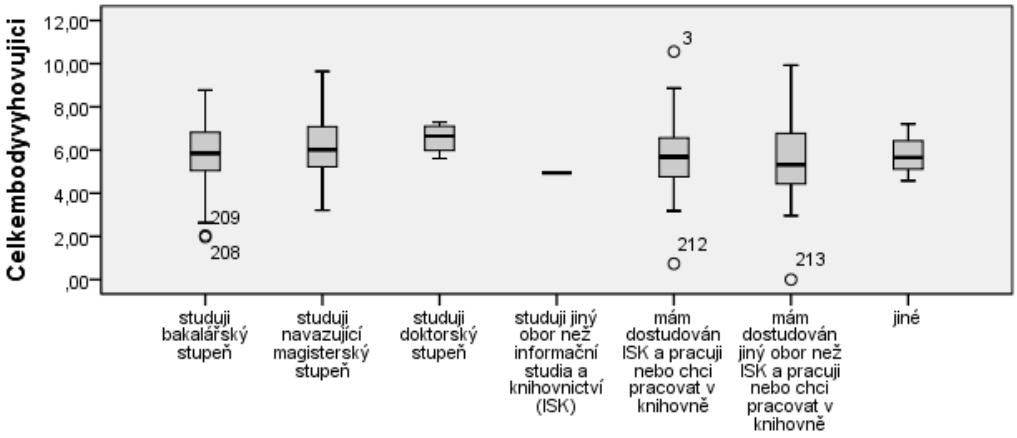
7.4.3.6 Vzdělání respondentů ve vztahu k bodovým hodnocením

Ostatní dotazované charakteristiky se vztahovaly k vzdělání respondentů, a to jak z hlediska pozice v systému školství, tak s ohledem na absolované vzdělání k problematice digitálních stop, příp. širší informační bezpečnosti (viz graf 52). Ve vzorku bylo zastoupeno podobné množství studentů a knihovníků z praxe. Vzhledem k velikosti skupin má smysl věnovat se bodovým hodnocením všech skupin mimo doktorandy a nevalidní hodnotu jiné (tyto dvě skupiny nejsou dále zahrnuty do testování statistické významnosti).



Graf 52 Pozice respondentů v systému školství a knihovnictví

Rozdíly hodnocení dle pozice v systému školství jsou minimální (graf 53), jen slabě lepší výsledky lze najít u doktorských studentů proti vyrovnaným bakalářským a navazujícím magisterským, podobné jsou i hodnoty knihovníků po absolvování ISK proti ostatním v praxi. Žádná z dílčích kategorií se nevymyká.

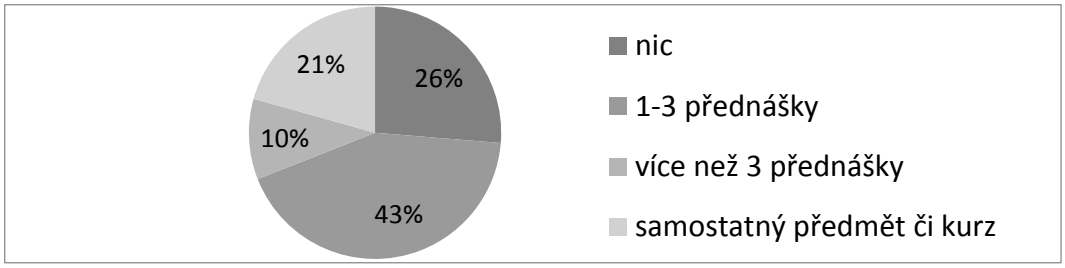


Graf 53 Bodové hodnocení dle aktuální pozice ve školství a knihovnictví

Body v jednotlivých otázkách i skupinách otázek byly dále hodnoceny pomocí Kruskal-Wallisova testu pro zjištění rozdílů mezi současnými a bývalými studenty vysoké školy vzhledem k předpokladu, že studenti budou celkově dosahovat lepších výsledků než lidé, kteří se pohybují v praxi a neprocházejí tedy vzděláváním v aktuálních tématech, mezi které digitální stopy patří. Rozdíl ale nebyl statisticky prokázán v celkovém hodnocení ($p = 0{,}148$), pouze v některých dílčích otázkách byly zjištěny statistické rozdíly (na hladině významnosti 5 % to byly otázky č. 6, 12 a 13). Zajímavé jsou rozdíly respondentů v tomto dělení při hodnocení dalších charakteristik. Projevily se statistické rozdíly na hladině významnosti 1 % v nejvyšším rozsahu vzdělání před vysokou školou, na ní a po ní v rámci ISK, v počtu etap bez vzdělání o digitálních stopách a v počtu etap se samostatným seminářem a nakonec i v nejvyšším rozsahu vzdělání o digitálních stopách. Je překvapivé, že i přes tyto rozdíly ve vstupních charakteristikách se neprojevily do rozdílů ve znalostech problematiky digitálních stop.

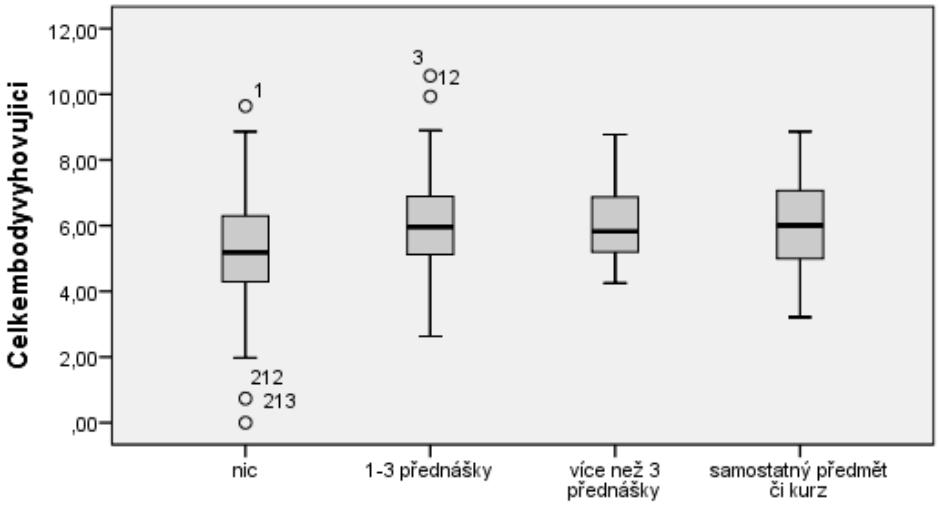
Zbývající otázka sledovala absolvované formální vzdělávání o tématu digitálních stop. Zjišťovala jednak jeho rozsah, jednak také instituci, která ho organizovala. Jak ukazuje graf 54, v případě nejvyššího rozsahu vzdělávání o digitálních stopách je modus i medián varianta 1-3 přednášky, která je platná pro 42,7 % respondentů. Nejvyšší možnost v podobě samostatného kurzu uvedlo 20,7 %, naopak žádné vzdělávání v tomto směru deklarovalo 26,3 % dotázaných. Vzhledem k výsledkům zájmu o téma (viz graf 48 na s. 160) existuje možnost, že

respondenti z nějakého důvodu nemají možnost využít organizovaného vzdělávání v tomto směru, příp. upřednostňují informální vzdělávání.



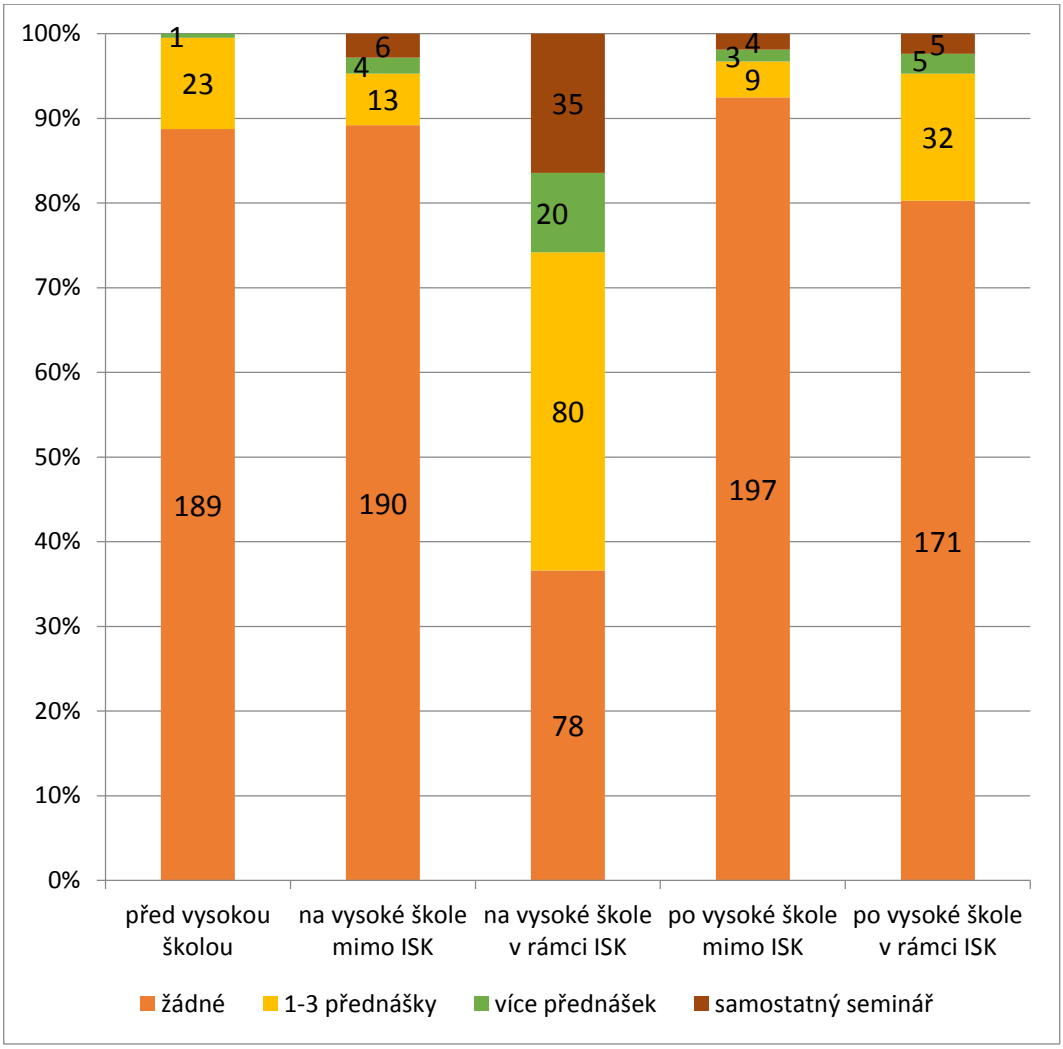
Graf 54 Nejvyšší rozsah vzdělání o digitálních stopách

Výsledky rozsahu vzdělávání o problematice nezahrnují informaci, v kolika etapách byl rozsah opakován. Protože v případě samostatného kurzu a více přednášek se jedná téměř výhradně o variantu v jedné etapě (více bylo zastoupeno u méně než 3 %), je tato informace zajímavá jen ve variantě 1-3 přednášky, které na dvou různých úrovních absolovalo 13,6 % a na třech 1,9 % dotázaných. Protože nesouvisející přednášky mají malý rozsah, nelze očekávat hlubší vliv, což potvrzují bodové výsledky. Rozdíly v bodovém hodnocení se ale neprojevily ani v závislosti na absolvovaném vzdělání dle maximálního rozsahu, jak znázorňuje graf 55.



Graf 55 Celkové hodnocení dle nejvyššího rozsahu vzdělání o problematice

Kde a v jakém rozsahu absolvovali dotazovaní vzdělávání o digitálních stopách, ukazuje graf 56. Ze sledovaných stupňů se vymyká vzdělávání o digitálních stopách na vysoké škole v rámci ISK, kde výrazně více respondentů prošlo větším množstvím přednášek nebo dokonce samostatným předmětem.



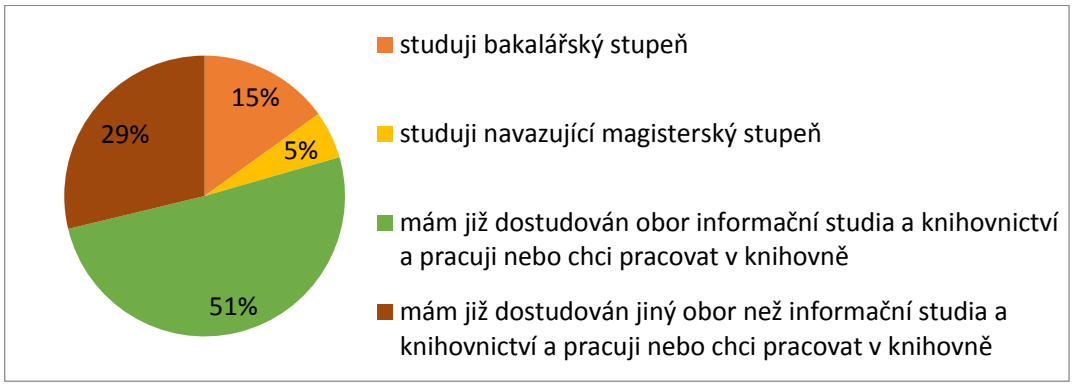
Graf 56 Absolvovaný rozsah vzdělávání na různých stupních vzhledem k ISK

Na všech ostatních sledovaných stupních je vzdělávání v jakémkoli rozsahu zastoupeno spíše výjimečně, nejvíce je to po vysoké škole v rámci ISK. Roli hraje to, že mezi respondenty jsou významně zastoupeni lidé, kteří ještě neabsolvovali vysokou školu, a proto nemohou zvolit jinou možnost než *žádné*. I pokud se ale omezíme na respondenty, kteří již v knihovně pracují nebo by chtěli pracovat, alespoň jednu přednášku k problematice po vysoké škole mimo IS absolvovalo jen 11,6 % a v rámci ISK 33,7 %. To ukazuje nedostatečné pokrytí dalšího vzdělávání

knihovníků v této oblasti. Pomoci by mohl vytvořený e-learningový otevřený kurz o informační bezpečnosti pro knihovníky[354], v rámci kterého je problematice digitálních stop věnována významná část, ale byl zveřejněn až po sběru a vyhodnocení dat v rámci zde popisovaného didaktického testování. Forma kurzu byla zvolena pro co největší redukci bariér, které by mohly ovlivnit další vzdělávání knihovníků (především finanční, časové a geografické).

Po i v rámci vysokoškolského vzdělávání mimo ISK vzhledem k vymezení výzkumného vzorku je očekávaně nízké zastoupení vzdělávání k této problematice. Není ale zcela zanedbatelné, což ukazuje, že pokud není nabídnuta vyhovující podoba vzdělávání o digitálních stopách cílená přímo na studenty ISK a knihovníky, je využito nabídky určené primárně pro jinou skupinu osob.

Žádným vzděláním na tomto stupni neprošlo jen 36,62 % respondentů. Další přiblížení této skupiny podle toho, v jaké úrovni vzdělávání se nacházejí, ukazuje graf 57 (vynechány jsou málo zastoupené skupiny doktorandů a *jiné*), ze kterého je patrný rozdíl mezi aktuálními studenty, kterých tímto vzděláním neprošlo 15,3 % na bakalářském, resp. 10,5 % na magisterském stupni, a lidmi z praxe, kterých bylo v případě absolventů ISK 52,9 % a absolventů jiných oborů dokonce 84 %. Je proto pravděpodobné, že s tím, jak se studenti ISK budou postupně dostávat do praxe, bude se situace v tomto směru měnit.

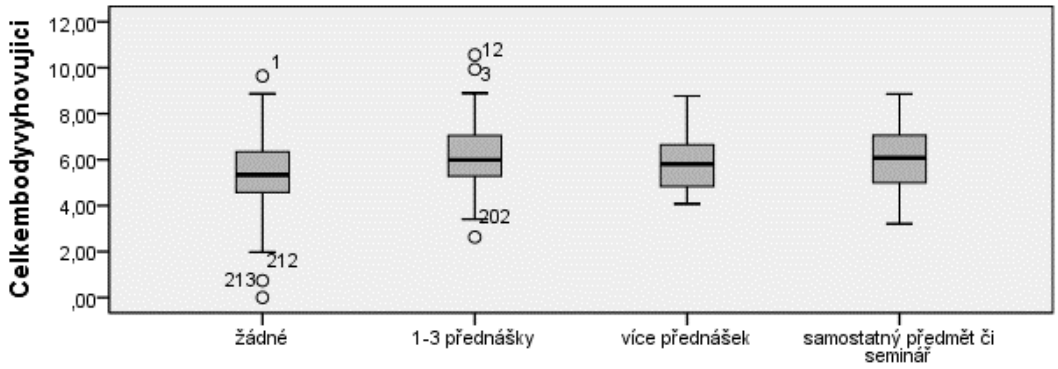


Graf 57 Neabsolvované vzdělání o digitálních stopách na VŠ v rámci ISK

Vzhledem k velikostem skupin je pro srovnání rozdílů v bodovém hodnocení na všech stupních hodnoceno jen zda respondent prošel či neprošel

[354] Tento kurz byl vytvořen v rámci programu VISK 2 a je dostupný na portálu Kurzy.knihovna.cz.

v dané úrovni nějakým vzděláváním, výsledky jsou u všech srovnatelné. Dle rozsahu bylo přikročeno ke srovnání jen v případě vzdělávání na VŠ v rámci ISK (graf 58). Z výsledků je patrné, že není zřetelný rozdíl ve znalostech v závislosti na vzdělání na žádném ze sledovaných stupňů, po absolvování vzdělání na každém z nich jsou ale výsledky s menší variační šíří, ale ne výrazně odlišným mezikvartilovým rozpětím. Přestože tedy není jasný vliv na zlepšení znalostí po absolvování vzdělání, dochází alespoň ke stabilizaci úrovně, kterou lze ve znalostech očekávat. Bez formálního vzdělávání mohou být bodová hodnocení ovlivněna informálním vzděláváním, příp. náhodou, které mohou posouvat hodnoty do vyšších úrovní, ale také rozšiřovat rozptyl. I z toho lze vyvozovat pozitivní vliv vzdělávání, přestože ne na úrovni, která byla očekávána.



Graf 58 Celkové hodnocení dle nejvyššího rozsahu vzdělání o DS na VŠ v ISK

7.4.3.7 Statistické testování vlivů na znalosti a průkaznosti testu

V předchozích dvou kapitolách bylo popsáno, v jaké míře se sledované charakteristiky vyskytují u respondentů a jejich vliv na celkové i dílčí bodové hodnocení. Nebyla v nich však řešena statistická průkaznost. Důvodem je především přísnost testů, proto byly nejdříve případné rozdíly hodnoceny na libovolné úrovni a až následovně je popsána signifikance. Při ANOVA testu celkového hodnocení s faktory danými charakteristikami respondentů (viz tabulka 7) totiž statisticky průkazné rozdíly byly zjištěny jen u některých sledovaných charakteristik, ne vždy u všech na stejné úrovni. V případě pohlaví a osobního zájmu o problematiku digitálních stop je třeba nulovou hypotézu o rovnosti rozptylů zamítnout, protože Sig. 0,000 < 0,05. Tato hodnota významnosti byla zjištěna právě jen u těchto proměnných. Z hlediska názoru na vzdělávání

o digitálních stopách je statisticky rozdílný rozptyl při hodnocení prostředí základních škol, pro vysoké školy a knihovny rozdíl průkazný není.

Na hladině významnosti 1 % se ještě pohybuje proměnná *nejvyšší rozsah vzdělání na vysoké škole v rámci ISK*, u ostatních úrovní nelze nulovou hypotézu zamítnout, což může být způsobeno nízkým zastoupením kategorií rozsahu mimo žádné vzdělání. Při hodnocení počtu etap o určitém rozsahu je statistický rozdíl v rozptylu jen u žádného vzdělání, k hranici 5 % hladiny významnosti se blíží také hodnota u 1-3 přednášky, naopak rozptyly nejsou statisticky odlišné při větším počtu přednášek. Dle vzdělání respondentů se statistický rozdíl rozptylů projevil také u nejvyššího rozsahu vzdělání v problematice. Z těchto hodnot je možné vyvodit odpovídající minimální potřebný rozsah vzdělávání pro plošné zlepšení znalostí knihovníků, aby mohli dále rozvíjet řešenou problematiku. Ideální je proto na jedné úrovni postihnout téma digitálních stop o 3 a více přednáškách, příp. samostatném semináři, nejlépe na vysoké škole v rámci oboru informační studia a knihovnictví s tím, že je u vzdělávaných vzbuzen osobní zájem o tuto problematiku.

Tabulka 7 ANOVA test pro celkové bodové hodnocení

			Sum of Squares	df	Mean Square	F	Sig.
Pohlaví		Mezi sk.	53,922	1	53,922	24,539	,000*
		Uvnitř skupin	463,655	211	2,197		
		Celkem	517,577	212			
Fáze vzdělávání		Mezi sk.	8,107	6	1,351	,546	,772
		Uvnitř skupin	509,470	206	2,473		
		Celkem	517,577	212			
Osobní zájem o digitální stopy		Mezi sk.	94,359	3	31,453	15,533	,000*
		Uvnitř skupin	423,218	209	2,025		
		Celkem	517,577	212			
Názor na vzdělávání o digitálních stopách	na ZŠ	Mezi sk.	36,009	4	9,002	3,888	,005*
		Uvnitř skupin	481,568	208	2,315		
		Celkem	517,577	212			
	na VŠ	Mezi sk.	10,242	4	2,560	1,050	,383
		Uvnitř skupin	507,335	208	2,439		
		Celkem	517,577	212			
	v knihovnách	Mezi sk.	10,178	4	2,545	1,043	,386
		Uvnitř skupin	507,399	208	2,439		
		Celkem	517,577	212			
Nejvyšší rozsah vzdělání	před vysokou školou	Mezi sk.	5,192	2	2,596	1,064	,347
		Uvnitř skupin	512,385	210	2,440		
		Celkem	517,577	212			
	na vysoké škole mimo ISK	Mezi sk.	3,326	3	1,109	,451	,717
		Uvnitř skupin	514,250	209	2,461		
		Celkem	517,577	212			
	na vysoké škole v rámci ISK	Mezi sk.	28,140	3	9,380	4,005	,008*
		Uvnitř skupin	489,437	209	2,342		
		Celkem	517,577	212			
	po vysoké škole mimo ISK	Mezi sk.	14,133	3	4,711	1,956	,122
		Uvnitř skupin	503,444	209	2,409		
		Celkem	517,577	212			
	po vysoké škole v rámci ISK	Mezi sk.	12,335	3	4,112	1,701	,168
		Uvnitř skupin	505,242	209	2,417		
		Celkem	517,577	212			
Počet etap vzdělání o digitálních stopách	bez vzdělání	Mezi sk.	49,996	5	9,999	4,427	,001*
		Uvnitř skupin	467,581	207	2,259		
		Celkem	517,577	212			
	s 1-3 přednášky	Mezi sk.	18,747	3	6,249	2,618	,052
		Uvnitř skupin	498,830	209	2,387		
		Celkem	517,577	212			
	více než 3 přednášky	Mezi sk.	4,442	3	1,481	,603	,614
		Uvnitř skupin	513,135	209	2,455		
		Celkem	517,577	212			
	samostatný seminář	Mezi sk.	8,956	3	2,985	1,227	,301
		Uvnitř skupin	508,621	209	2,434		
		Celkem	517,577	212			
Nejvyšší rozsah vzdělání o digitálních stopách		Mezi sk.	27,818	3	9,273	3,957	,009*
		Uvnitř skupin	489,759	209	2,343		
		Celkem	517,577	212			

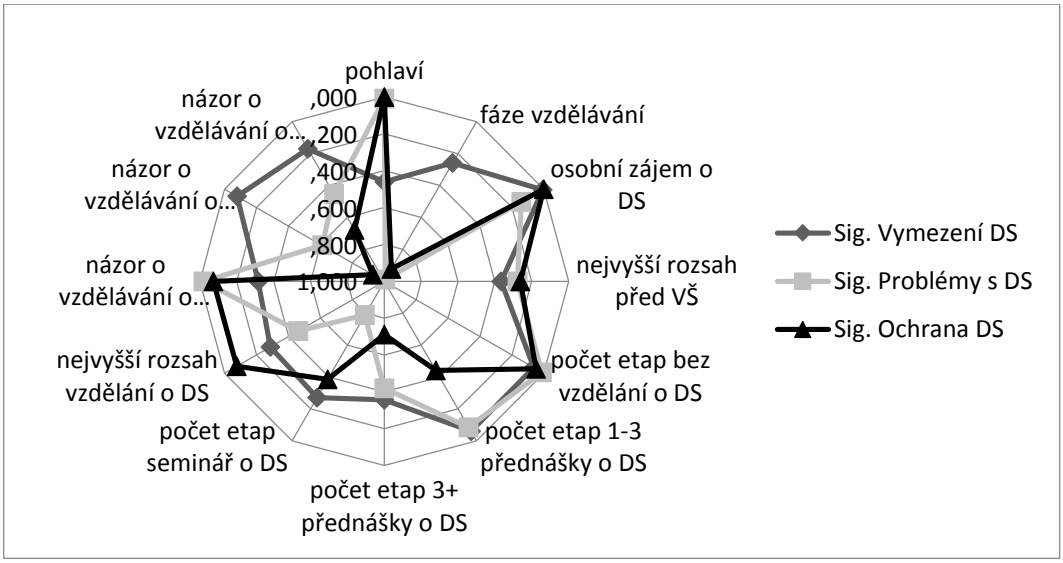
Protože celkové bodové hodnocení může být ovlivněno nerovnoměrnými znalostmi v dílčích tématech, byly sledovány výsledky ve dvou různých kategorizacích. Dělení vycházelo z tematického zaměření (vymezení digitálních stop, jejich užití a ochrana), druhý přístup dělil otázky na technické (možnosti softwaru a hardwaru) a uživatelské, resp. založené na chování uživatele. V tomto případě bylo použito pro srovnání výsledků korelace pro zjištění závislosti získaných bodů v jednotlivých typech otázek.

V případě dělení na otázky zaměřené na technickou stránku (č. 4, 5, 9, 10, 12, 13) a chování (č. 1, 2, 6, 7, 8, 15) byl zjištěn Pearsonův korelační koeficient 0,295, který je statisticky významný na hladině 1 % při jednostranném testu. Protože technické otázky měly výrazně nižší průměr bodového zisku v otázkách ($r = 0,4204$) proti otázkám směřujícím k chování ($r = 0,5547$) a nedošlo k překrytí intervalů spolehlivosti, lze prohlásit, že respondenti vykázali vyšší znalosti ve druhé uvedené oblasti. Dotazovaní více znalí problematiky vykazují lepší výsledky v obou oblastech (byla prokázána závislost mezi výsledky v obou směrech), ale v oblasti chování jsou na tom prokazatelně lépe.

Druhé dělení odpovídá složení testu, kategorie jsou různě rozsáhlé dle významnosti (vymezení tématu zahrnuje jen dvě otázky, zbývající kategorie vždy pět). I zde byly zjištěny statistické závislosti mezi proměnnými ($r = 0,169$ mezi vymezením tématu a ochranou, $r = 0,268$ mezi vymezením a užitím digitálních stop a $r = 0,273$mezi užitím a ochranou; všechny statisticky významné na hladině 1 % při jednostranném testu). Stejně jako v předchozím případě byly srovnány kategorie pomocí t-testu, který prokázal rozdíly mezi proměnnými bez překrytí intervalů spolehlivosti, kdy vymezení problematiky vykazovalo u v průměrném bodovém zisku otázky $r = 0,5165$ bodu, užití digitálních stop $r = 0,6149$ a ochrana $r = 0,3486$. Je tedy možné podobné konstatování jako v předchozím případě, kdy nejslabší znalosti byly zjištěny u ochrany digitálních stop, přestože právě ta je důvodem, proč by měly být známy i předchozí dvě řešené oblasti.

Charakteristiky byly řešeny i k dílčím tématům v testu. Kvůli nesplnění podmínky normality rozložení nemohl být využit ANOVA test, ale jen méně přísný Kruskal-Wallisův test. Zde již není nutné uvádět všechny hodnoty pro určení významnosti rozdílů jako v případě celkového hodnocení, k zjištění klíčových vztahů pro srovnání tematických oblastí postačí hodnoty významnosti u všech

proměnných zobrazené v grafu 59 Signifikance tematických oblastí v Kruskal-Wallisově testu. V rámci sledování těchto rozdílů nejsou řešeny kategorie nejvyššího rozsahu na dílčích stupních vzdělání, protože nebyly zastoupeny v dostatečném množství pro provedení testu.

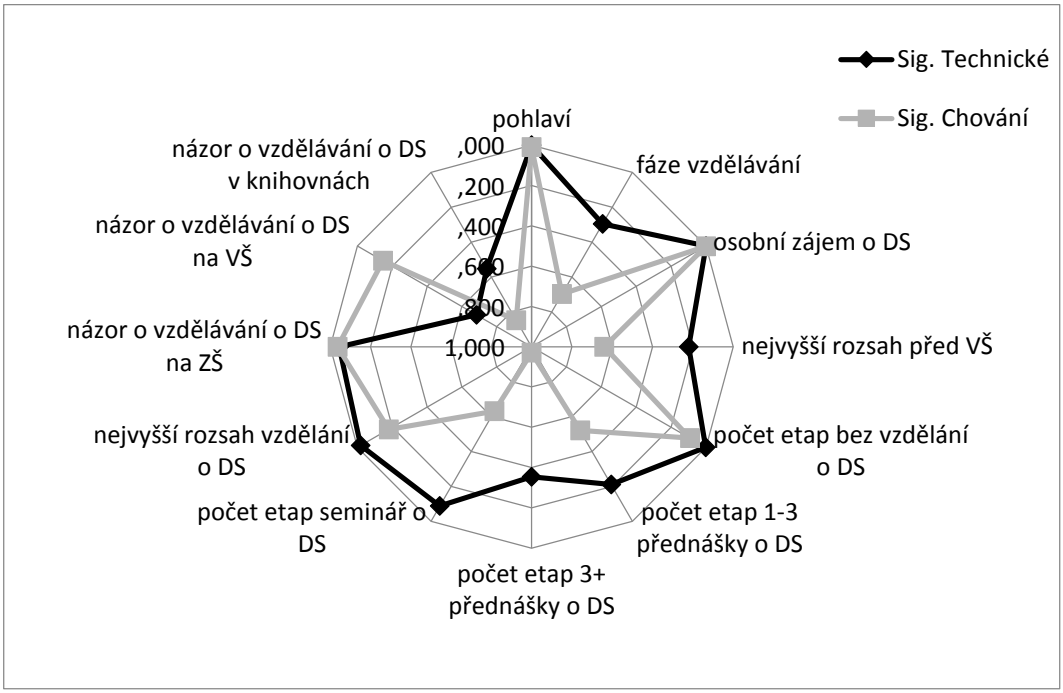


Graf 59 Signifikance tematických oblastí v Kruskal-Wallisově testu

Z grafu je možné pozorovat vliv osobního zájmu o téma, také se objevuje u všech tematických okruhů kromě užití digitálních stop jako statistiky významný (hodnoceno na hladině 5 %), což odpovídá také celkovému hodnocení, interpretace již byla uvedena při deskriptivním hodnocení. Pohlaví, tedy druhá proměnná s nejvyšší významností diferenciace znalostí v celkovém hodnocení, se neprojevila dostatečně u vymezení digitálních stop, ale u zbývajících témat ano, průkazný vliv na stejné oblasti má také počet etap bez vzdělání o digitálních stopách. To ukazuje, že pokud nedochází k žádnému vzdělávání v tomto směru, má to vliv na znalosti v problémech s digitálními stopami i jejich ochraně, což je poměrně očekávaný výsledek, význam rozsahu v žádném intervalu se ale prokázat nepodařilo. Poslední signifikantní výsledek byl zjištěn u užití digitálních stop při faktoru názor na vzdělávání o digitálních stopách na základní škole.

Mírně odlišné výsledky ukazuje graf 60 Signifikance techničnosti zaměření v Kruskal-Wallisově testu, kde se objevují jako statisticky významné totožné proměnné, v obou zaměřeních to je pohlaví, osobní zájem o téma a názor na

vzdělávání o digitálních stopách na základní škole. Rozdíly jsou u počtu etap bez vzdělání o vysokých školách a nejvyššího rozsahu vzdělání o digitálních stopách (tento faktor se v předchozím testu jako signifikantní neukázal), kterě se projevily jako diferencující u techničtěji zaměřených otázek ve všech tématech. Otázky směřující do oblasti chování člověka s ohledem na digitální stopy diferencující signifikanci v žádné další oblasti neprokázaly.



Graf 60 Signifikance techničnosti zaměření v Kruskal-Wallisově testu

Pro kategorizaci respondentů vzhledem k znalostem problematiky bylo využito logistické regrese. Identifikovala charakteristiky nejvíce přispívající pravděpodobnosti, že respondent bude mít dostatečnou úroveň znalostí digitálních stop. Aby bylo možné logistickou regresi realizovat, bylo nutné stanovit požadovanou úroveň. Bodové hodnocení uvedené výše nereflektuje, že některé otázky představují nezbytný základ znalostí a další již zjišťují hloubku znalostí, která jde nad nutný základ. Těmto dvěma kategoriím byly přiřazeny otázky:

- Nezbytný základ: 1, 5, 8, 9
- Prohlubující otázky: 2, 4, 6, 7, 10, 12, 13, 15
- Z důvodu nízké citlivosti vyřazeny: 3, 11, 14

Pro test jsou nutné vstupy s binárními hodnotami. V charakteristikách respondentů proto vznikly rozlišující hodnoty: pohlaví, studenti/absolventi (kategorie *jiné* byla odfiltrována), osobní zájem/nezájem o téma, nejvyšší rozsah vzdělání před vysokou školou (ostatní etapy byly z výše uvedeného důvodu nehodnoceny) i počet etap s určitou velikostí vzdělání s rozlišením na žádné a absolvované (bez ohledu na rozsah) a přesvědčení o smyslu či nesmyslu vzdělávání o digitálních stopách na dané úrovni. Výsledné hodnoty testu zobrazuje tabulka 8, kdy pro úspěšnost v testu bylo nutné správně odpovědět na všechny základní otázky a min. polovinu prohlubujících.

Tabulka 8 Logická regrese charakteristik pro úspěšnost v testu

	Sig.	**Exp(B)**	**95% C.I.for EXP(B)**	
			Lower	**Upper**
Bi_pohlaví	,007	2,589	1,294	5,182
Bi_praxe	,289	1,332	,784	2,262
Bi_zajem	,011	2,935	1,282	6,723
Bi_před	,234	1,659	,720	3,819
Bi_nic	,838	1,221	,180	8,268
Bi_málo	,474	1,214	,714	2,064
Bi_víc	,339	1,446	,679	3,080
Bi_celý	,030	2,068	1,072	3,988
Bi_zš	,309	2,126	,498	9,089
Bi_vš	,819	1,222	,220	6,792
Bi_knihovna	,718	1,231	,398	3,800

Z hodnoty Odds Ratio vyplývá, že k úspěšnosti přispívá postupně od nejsilnějšího vlivu: osobní zájem, pohlaví, názor na vzdělávání o digitálních stopách na základní škole, absolvování celého semináře k problematice, vzdělání o digitálních stopách před vysokou školou, více než tři přednášky k tématu a zda je respondent student či člověk již pracující nebo zajímající se o práci v knihovně. I ostatní čtyři proměnné přispívají k výsledku, hodnoty se ale již dosti blíží k hraniční hodnotě vlivu. Vedle této hodnoty je ještě nezbytné uvážit velikosti intervalů spolehlivosti. Ten se celý pohybuje nad hraniční hodnotou jen u zájmu respondenta, jeho pohlaví a absolvovaného celého semináře, proto u těchto tří proměnných je vliv nezpochybnitelný. Naopak u názoru na vzdělávání o digitálních stopách na základní a vysoké škole a u neabsolvovaného vzdělání k této problematice jsou intervaly spolehlivosti velmi široké, proto i prokázaný pozitivní vliv je nutné brát

s tímto omezením silně rozptýlených hodnot, vliv tedy statisticky existuje, ale u poměrně širokého vzorku respondentů se neprojevuje.

7.4.3.8 Vyhodnocení testů hypotéz

Výše uvedené výsledky postupně popisují výzkumná zjištění, která vychází ze stanovených hypotéz. V návaznosti na deskriptivní i explorativní vyhodnocení je proto možné vyhodnotit stanovené hypotézy. Podrobnější údaje k výsledkům statistických testů uvedeným u hypotéz jsou předmětem kap. 7.4.3.7.

H1: Většina respondentů dosahuje 40-60 % bodů ve znalostním testu na téma digitální stopy.

Pokud hodnotíme všechny testové otázky, v intervalu 40-60 % bodů se nachází 66,2 % všech výsledků (viz s. 154), při omezení otázek na vyhovující dle citlivosti se počet snížil na 58,2 % výsledků (viz s. 157). I tak je ale hypotéza potvrzena, většina respondentů vykazuje určité znalosti problematiky, ale ne zcela dostatečné. Lze proto navázat a prohloubit orientaci knihovníků v oblasti digitálních stop, směry rozvoje jsou předmětem podhypotéz h2 a h3 (viz níže).

h1: Více než 50 % respondentů dosáhne méně než 50 % maxima bodů.

První dílčí hypotéza vyjadřovala přesvědčení, že znalosti respondentů se budou pohybovat spíše ve spodní polovině výsledné škály, protože problematika stále není plošně příliš řešena. Zatímco v případě celkového hodnocení se ve spodní polovině škály nacházelo jen 15 % respondentů (viz s. 154), při omezení na vyhovující otázky to je již 55,9 % dotázaných (viz s. 157). Proto i tuto hypotézu lze považovat za potvrzenou. Výsledek ukazuje, že znalosti se sice pohybují z výrazné části ve středové části, ale jsou spíše slabší než naopak, což prohlubuje smysl vzdělávání knihovníků o digitálních stopách vyvozený již v H1.

h2: Průměrný počet bodů je vyšší u otázek k chování lidí než k technické stránce.

Průměrný počet bodů v případě otázek zaměřených na chování uživatelů internetu byl 0,55, což je poměrně výrazně více než u technických otázek, kde byl průměrný bodový zisk na otázku 0,42 bodu, 95 % intervaly spolehlivosti se nepřekrývaly, ale kvalita znalostí v obou oblastech byla pomocí Perasonova

korelačního koeficientu prokávána jako závislá (podrobněji viz s. 171). Hypotéza tedy opět byla prokázána, potvrzuje, že studentům ISK a knihovníkům je výrazně bližší informační chování v oblasti bezpečnosti než technické nástroje pro práci s digitálními stopami. Jejich zaměření se proto doplňuje s technickou podporou v oblasti, která je blíže právě cílové populaci výzkumu proti informatikům.

h3: Průměrný počet bodů v jednotlivých tematických oblastech se liší.

Jiný pohled na kategorizaci otázek představovalo rozdělení na vymezení digitálních stop (průměr pro otázku 0,52 bodu), problémy jimi způsobené (průměr 0,61 bodu) a ochrana digitálních stop (průměr 0,34). Z toho vyplývá, že nejméně známá jsou řešení problémů, které může zneužití digitálních stop způsobit, oproti chápání, co vše mezi digitální stopy patří a jakými postupy je lze využít či zneužít. Stejně jako u předchozí hypotézy byly prokázány statisticky významné rozdíly mezi průměry t-testem na hladině významnosti 1 % (viz s. 171). Hypotéza se tedy potvrdila. Výsledky pak vedou k tomu, že je nutné se při dalším vzdělávání zaměřit na řešení digitálních stop, protože ostatní dvě oblasti podporují bezpečnost uživatele, ale jejich znalost bez orientace v řešeních má výrazně slabší vliv na bezpečnost uživatelů, než kdyby byly znalosti prokázány opačně.

h4: Respondenti s větším zájmem o téma digitálních stop dosahují více bodů.

Hypotéza, která měla spojit hodnocení s vnitřní motivací jako základem znalostí, se zaměřila na jednu ze sledovaných charakteristik respondentů. Tato proměnná se prokázala jako vlivná v ANOVA testu (pro celkové hodnocení $p = 0{,}000$; viz s. 170) i specifičtěji zaměřených Kruskal-Wallisových testech (vymezení digitálních stop $p = 0{,}007$, problémy s digitálními stopami $p = 0{,}035$, ochrana digitálních stop $p = 0{,}000$; technick zaměřené otázky $p = 0{,}000$, otázky zaměřené na chování $p = 0{,}002$; viz s. 168-173). Hypotéza tedy byla potvrzena.

h5: Respondenti s vyšším počtem bodů jsou častěji přesvědčeni o smyslu vzdělávání o tématu digitálních stop.

Tuto hypotézu není možné vyhodnotit, protože jen dva respondenti uvedli, že podle jejich názoru nemá vzdělávání o problematice digitálních stop smysl (viz

s. 160). Jejich bodové hodnocení bylo velmi nízké (v jednom případě 0 bodů, v druhém 3,239, resp. 1,97 bodu při omezení na vyhovující otázky). Při takto malém zastoupení ale není možné učinit z výsledku oprávněný závěr, není totiž možné statistické testování.

H2: Respondenti, kteří absolvovali rozsáhlejší organizované vzdělávání o digitálních stopách, dosahují vyššího bodového hodnocení v testu.

Druhá hlavní hypotéza již směřovala k statistickým testům, kdy byl hodnocen vliv vzdělávání. Průkazný rozdíl byl zjištěn při srovnání maximálního rozsahu vzdělání bez ohledu na stupeň, kdy k němu došlo ($p = 0{,}009$). Při hodnocení v rámci jednotlivých sledovaných stupňů byl signifikantní rozdíl jen v případě nejvyššího rozsahu vzdělání na vysoké škole v rámci ISK ($p = 0{,}008$; viz h8 níže), u ostatních stupňů vzdělávání není možné hypotézu potvrdit z důvodu malého zastoupení hodnot mimo žádné vzdělání. Hypotézu je tedy možné s uvědoměním si omezení málo zastoupených kategorií přijmout.

h6: Současní studenti oboru ISK dosahují vyššího počtu bodů než současní knihovníci a zájemci o práci v knihovně.

Vzhledem k tomu, že problematika je v oboru ISK řešena poměrně nedlouho, bylo očekáváno, že ti, kteří si aktuálně procházejí vzděláváním reflektujícím aktuální vývoj v oboru, budou vykazovat lepší znalosti i ve sledované problematice. Tato hypotéza se ale statisticky neprokázala ($p = 0{,}148$, více viz s. 164). Jedná se o poměrně překvapivé zjištění, nicméně obě skupiny jsou vzdělávány v případě zájmu v řešené problematice volitelnými semináři, ani jedna skupina téma plošně řešené nemá, což může být důvod neprokazatelného výsledku této hypotézy.

h7: Min. 75 % bodů dosahují respondenti, kteří absolvovali více než 3 přednášky nebo samostatný předmět či kurz.

Jak bylo uvedeno při vyhodnocení H1, výrazná většina respondentů se pohybuje kolem středového bodového hodnocení a pouze 1,4 % respondentů překročilo 75 % celkového bodového hodnocení u vyhovujících otázek (viz s. 157;

2,8 % respondentů při všech otázkách viz s. 154). Jakýkoli výsledek kvůli nízkému zastoupení není průkazný a hypotézu není možné potvrdit, ani vyvrátit. Tito tři nejúspěšnější respondenti neuvedli žádné rozsáhlejší (více než tři přednášky) absolvované organizované vzdělání.

h8: Vyššího počtu bodů dosahují studenti, kteří prošli organizovaným vzděláváním na vysoké škole, než ti, kteří vzděláním prošli na jiné úrovni.

Statisticky významný rozdíl byl zjištěn u bodového hodnocení respondentů dle nejvyššího vzdělání na vysoké škole v rámci ISK ($p = 0{,}008$), ne však při vzdělání na vysoké škole mimo tento obor ($p = 0, 717$). Při sloučení oborů vysokoškolského vzdělání a vyhodnocení rozdílů byl zjištěn statisticky významný rozdíl na hladině 5 %, k překrytí intervalů spolehlivosti na této hladině nedošlo ani částečně. Hypotéza tedy byla potvrzena, čímž je prokázán smysl vzdělávat o problematice digitálních stop na vysoké škole.

h9: Respondenti, kteří prošli organizovaným vzděláváním, jsou častěji přesvědčeni o smyslu vzdělávání o tématu digitálních stop.

Stejně jako h5, ani tuto hypotézu není možné vyhodnotit z důvodu nízkého zastoupení respondentů, kteří nevidí smysl problematiky.

7.4.4 Závěry z výzkumu

Cílem testování bylo zmapovat znalosti digitálních stop u lidí pohybujících se v oblasti knihovnictví, a to jak na úrovni praxe, tak i studia, a porovnat je s ohledem na jejich předchozí vzdělání. Tyto znalosti jsou totiž nezbytným předpokladem, aby mohli pomáhat uživatelům knihovny či jiné instituce ve zvýšení bezpečnosti digitálních stop.

Z šetření vyplynulo, že respondenti mají určité znalosti o problematice, ale jsou poměrně nízké, převažující většina dotázaných se pohybuje mírně pod polovinou maximálního počtu bodů. Slabá místa jsou především ve znalostech technických nástrojů pro správu digitálních stop, naopak v chování uživatelů jsou znalosti silnější. Test ale prokázal, že znalosti knihovníků i studentů ISK nejsou

dostatečné a bylo by vhodné dále je rozvíjet v tomto tématu. Vhodné je především nasazení více než tří přednášek k problematice na vysoké škole.

Existují spíše výjimečně jedinci, kteří se v problematice dobře orientují, na celém sledovaném vzorku ale převažuje omezená orientace v problematice, což dokládá i evaluační dotazník semináře realizovaného v roce 2012 v Městské knihovně v Praze[355], kdy knihovníci reflektovali svůj postoj k užitečnosti lekce zaměřené na sociální aspekty informační bezpečnosti pozitivně v 77 %, jen 16 % negativně (ostatní zvolili variantu *nevím*), nikdo nebyl zcela nespokojen. Při negativním hodnocení byly jako důvody uvedeny, buď že se knihovník již problematikou zabývá, a tedy seminář mnoho nového nepřinesl, nebo naopak že danou problematiku ve své práci nevyužije (shodně zastoupeny). 42 % projevilo zájem o navazující lekci a 24 % ne. Z otevřených otázek byly získány informace potvrzující smysluplnost lekce i zájem a překvapení z hlediska škály problémů na internetu i omezených možností knihoven jim předcházet a klíčových prvků pro ochranu knihovny proti zákonným postihům jednáním knihovníků i uživatelů na internetu. Je tedy pravděpodobné, že přijetí tématu jako podstatného nejen v obecném pojetí, ale i pro knihovny, bude nutné pomocí hlubších vzdělávacích akcí pro knihovníky ve fyzickém prostředí, nelze očekávat, že si více z nich dostatečně dostupné materiály v tuto chvíli z vlastního zájmu najde. Současně je nutné téma postavit na konkrétní praxi v místě, přizpůsobit lekci nejen knihovně, ale případně i pobočkám a nevést lekci jako přednášku, ale umožnit interakci.

Nicméně potřebné je zajištění podpory vedení, jak dokládá e-mailová komunikace s knihovnicí z městské knihovny ze dne 18. 7. 2013, která projevila zájem o téma i vzhledem k nedostatečné připravenosti z formálního vzdělávání, nicméně spíše na rovině osobní než pracovní, kde by vzhledem k omezeným časovým a finančním možnostem volila vzdělávání spíše v práci s dětmi nebo přehledu současné literatury. Tato knihovnice také dodává, že didaktický test nedokončila z důvodu přílišné odbornosti otázek na její znalosti s komentářem, že seminář o informační bezpečnosti, který absolvovala v rekvalifikačním kurzu, byl zaměřen „*spíše praktické věci, se kterými se i "běžný smrtelník" může setkat*“. To ukazuje nedostatečnou představu o reálnosti tohoto rizikového jevu.

[355] Využití výsledků evaluace pro tuto práci odsouhlasil Ondřej Hartman z MKP v e-mailové komunikaci z 8. července 2013

Toto posunutí řešení tématu do více cílené, osobnější roviny odpovídá i dalším zjištěním. Základním předpokladem rozvoje znalostí je vnitřní motivace a zájem o problematiku, tento vliv se projevoval ze sledovaných charakteristik nejsilněji. I další sledované faktory posilují zlepšování znalostí v problematice digitálních stop, jejich vliv je ale méně průkazný. Zajímavým zjištěním jsou velké rozptyly výsledků, které ovlivňují třeba i statisticky průkazné vlivy na zjištěné znalosti, především u názorů na vzdělávání na různých úrovních a u respondentů, kteří neprošli žádným organizovaným vzděláním k řešené problematice.

Na základě výzkumu je tedy možné konstatovat, na jaké úrovni a v jakém rozsahu je vhodné hlouběji vzdělávat v problematice digitálních stop a také na jaká témata by měla být zaměřena větší pozornost než doposud. Znalosti totiž rozhodně není možné považovat za dostatečné, byť předmětem šetření byly základy tématu. Prvním krokem je přitom dostatečné vysvětlení respondentům, proč by se právě oni měli v této problematice vzdělávat, protože právě osobní zájem má nejsilnější vliv na zjištěné znalosti. Obecně již problematiku není nutné obhajovat, protože pouze malé výjimky nevidí smysl vzdělávat v tématu digitálních stop, jak potvrdily i předchozí výzkumy (viz kap. 7.1.2.2. a 7.2.2.2).

7.5 Zhodnocení současného stavu

Z dotazování knihovníků a studentů ISK v období 2011-2013 vyplynulo, že při zavádění problematiky digitálních stop do vzdělávání uživatelů knihovny je možné navázat na již realizované aktivity, tento kvantitativně hodnocený výsledek je podpořen i výsledky kvalitativního výzkumu od stolu (viz kap. 4.3). Vzdělávání uživatelů je již v knihovnách poměrně zavedenou aktivitou, přičemž především u dospělých uživatelů je často pozornost věnována i práci s informačními technologiemi, v případě dětí je stále převažující zaměření na čtenářství. Knihovníci deklarují, že do svých vzdělávacích aktivit problematiku informační bezpečnosti zahrnují, ale hlubší pozornost v samostatných lekcích není častá.

Důvodem omezené implementace informační bezpečnosti a konkrétně digitálních stop není nezájem o problematiku nebo její odmítání v prostředí knihoven. Naopak téma je podle respondentů důležité, ale sami často mají problém se v tomto směru rozvíjet. Tento zájem je patrný na individuální úrovni zjištěné

pomocí dotazníků, ale také na plošnější úrovni mapované v kap. 4.3 a tím, že knihovníci na žádost knihoven procházejí semináři zaměřenými na digitální stopy, např. v rámci rekvalifikačního kurzu v Moravské zemské knihovně, dalšího vzdělávání knihovníků Městské knihovny v Praze nebo v rámci mimoškolního vzdělávání knihovníků (VISK 2) v Moravskoslezském kraji. Od klíčových osob v oblasti knihovnictví je tedy zájem dále přenášen různými formami a úrovněmi na další knihovníky ve větších i menších knihovnách.

V současnosti ale znalosti knihovníků, ale také studentů ISK není možné považovat za dostatečné. Tyto znalosti jsou přitom nezbytným předpokladem, aby bylo možné zahrnout téma do lekcí knihoven pro koncepční řešení bezpečnosti digitálních stop. V rámci didaktického testu byla zjištěna forma i obsahové zaměření, které by měly být v tomto směru hlouběji řešeny. V současnosti prokázané znalosti mohou být pro knihovníky bariérou v tom, aby vzdělávali v tomto směru především děti, které bývají někdy označovány jako digitální domorodci[356], jejichž znalosti a frekvence užívání informačních technologií a služeb, kterých by se mělo týkat vzdělávání, jsou nesrovnatelné. Knihovníci proto potřebují získat dostatečnou jistotu ve znalostech, aby se problematikou zabývali. Přitom tyto znalosti nemusí přesahovat ve všech směrech znalosti dětí, protože „*děti jsou často dobře obeznámeny s počítačem a internetem jako zdrojem zábavy, ale nejsou zvyklé je používat jako nástroje.*“[357] Proto je nutné naučit je především kritickému přístupu k tomu, co internet nabízí, a uvědomění si i možných negativních, nejen zábavných důsledků jejich působení na internetu.

I přes limitované znalosti knihovníků lze bez odkladu podpořit zavádění vzdělávání o digitálních stopách do spolupráce knihoven se školami, především základními, kde požadovaná úroveň je bližší prokázaným znalostem řešené problematiky. Odpovídají jí také nastavení lekcí, které jsou představené v metodice vytvořené pro tuto práci v kap. 8.2.

[356] PRENSKY 2001
[357] WOLD 2010, s. 77; CHANG 2010, s. 526

8 Možné vzdělávání v knihovně o bezpečnosti digitálních stop

V teoretické části byla rozebrána problematika digitálních stop a důvody, proč by ji knihovny měly zařadit do své vzdělávací nabídky. Zásadní specifika knihoven a z části i jiných institucí neformálního vzdělávání, které je staví do pozice vhodných subjektů pro rozvíjení schopností zejména dětí pohybovat se bezpečně na internetu, byly rozebrány v kap. 4.3. Knihovny mohou tuto výzvu přijmout, jsou na to připraveny, jak bylo dokázáno v první polovině výzkumné části a částečně již řeší buď konkrétně tuto problematiku, nebo její širší témata.

Informační technologie jsou nástroj jako každý jiný, proto mohou být využity i zneužity. Knihovny by neměly omezovat vzdělávací nabídku na poměrně rozšířené výhody, které informační technologie nabízejí, ale měly by se zaměřit i na problémy, které je mohou doprovázet. Nemá smysl duplikovat činnost škol, ale působení by mělo být dlouhodobé. Především v případě dětí (které se, stejně jako jejich používání internetu, vyvíjejí) by měly být reflektovány aktuálně využívané služby internetu a způsob práce na internetu. Je proto vhodné nastavit celou koncepci, která by postupně rozvíjela znalosti a dovednosti žáků dle jejich aktuální úrovně poznání a současně by budovala postavení knihovny jako instituce, která zprostředkovává přístup k informacím i s využitím internetu, a to způsobem, který je komplexní a bezpečný. Kvalifikovaný knihovník přitom dokáže poradit i nabídnout možnosti dalšího rozvoje. Knihovny by přitom měly využít možností, které se váží na neformální vzdělávání a tím zaujaly svou pozici v systému, kde budou doplňovat instituce formálního vzdělávání.

Dále jsou představena teoretická východiska neformálního vzdělávání a aktivního učení, které knihovny mohou snadno zavést a odpovídají moderním výukovým principům. Jsou aplikovány do návrhu ucelené koncepce vzdělávání o bezpečnosti digitálních stop pro žáky na základní škole. Její část byla podrobena akčnímu výzkumu v případové studii lekce pro 4. – 5. třídu Masarykovy základní školy v Poličce v knihovně. Částečně její evaluací a částečně zhodnocením názorů zástupců různých klíčových subjektů na vzdělávání o bezpečnosti digitálních stop v knihovnách přinesly rozhovory se šesti dotazovanými, a to po dvou z prostředí školy, knihovny a rodiny. Tím je uzavřen teoretický i praktický pohled na možné pojetí vzdělávání v knihovně o bezpečnosti digitálních stop.

Všechny popsané postupy jsou podstatné pro dosažení druhého cíle této dizertační práce v podobě vytvoření metodiky vzdělávání o digitálních stopách na základních školách a jejího ověření výzkumy. Tak je komplexně popsána možná realizace vzdělávání v této problematice i její přijetí a pozitivní důsledky pro všechny zúčastněné strany. Knihovny tím získávají ověřený nástroj, který mohou použít pro zvýšení informační bezpečnosti svých dětských uživatelů a sekundárně pak pro zlepšení své role v komunitě tím, že budou přispívat k řešení stále silněji pociťovaného společenského problému, který je v současnosti především mimo velká města řešen spíše nahodile nebo vůbec.

8.1 Specifika formy vzdělávání v knihovnách

Přestože knihovny jsou příslušností k ministerstvu kulturní, ne vzdělávací instituce, osvětová činnost k nim patří. I pokud bude jejich role omezena na tradiční zpřístupňování zdrojů, využití této nabídky uživateli je pro vzdělávání, příp. zábavu. Knihovnu však kromě fondu definují i služby, které nespočívají jen v administraci výpůjček, ale i k osvětě při práci s informacemi (např. referenční služby). Jak ale bylo doloženo v kap. 4, přímé vzdělávání je, a v budoucnu pravděpodobně stále více bude, jednou ze základních služeb knihoven.

Knihovny jako vzdělávací instituce se výrazně liší od škol všech úrovní. Nabízí totiž vzdělávací akce všem zájemcům na dobrovolné úrovni a uživatele vzdělává obvykle bez udělení uznávaného certifikátu, spíše pro odpověď na jeho zájmy či potřebu v osobním, ne profesním rozvoji. Jen výjimečně knihovny nabízí i certifikované kurzy (např. Kurz první pomoci záchrany života[358]). Tato forma odpovídá typu vzdělávání označovanému jako neformální. S tím jsou sice spojeny limity využitelnosti, na druhou stranu může být efektivnější, protože reflektuje oblast, ve které je vzdělávaný motivovaný se rozvíjet[359]. V neformálním vzdělávání jsou snadno využitelné postupy, které vzhledem k dlouhodobosti a pevným výukovým cílům to formální limitují. Mezi tyto postupy patří aktivní učení, které

[358] Kurz první pomoci záchrany života 2013
[359] STASIUNAITIENE 2009

staví na moderních konstruktivistických přístupech ve výuce a podle výzkumů je výrazně efektivnější než tradiční frontální výuka.

Specifika neformálního vzdělávání a aktivního učení by měly knihovny využívat pro zvýšení efektivity svých lekcí i odlišení se od institucí neformálního vzdělávání, které nemusí každému vyhovovat. Knihovny tak mohou pro vzdělávání v klíčových oblastech být alternativou, kde tradiční postupy nefungují. Knihovny by si měly být svého postavení ve vzdělávacím systému vědomy, protože jen tak budou plnit roli, která je jim stanovena a nebudou jen omezenými možnostmi opakovat činnosti, které již zastává škola.

8.1.1 Neformální vzdělávání

Ze strategických dokumentů v oblasti vzdělávání, které vytváří státy i mezinárodní organizace, je patrný důraz na celoživotní vzdělávání formálně, neformálně a informálně ve spojení, a to už více než 15 let. Za klíčové při prosazování neformálního vzdělávání lze považovat především snahy, které deklarovalo UNESCO[360] a Evropská komise[361], jejich vývoj stále pokračuje[362]. Neformální učení lze definovat jako „*nezávislý učební proces, ke kterému dochází v rozdílných prostředích, ale je charakterizováno plánovanou povahou, má své vlastní cíle a je limitováno časem*“[363]. Oproti formálnímu typicky nevede k certifikaci. Informální vzdělávání je také nezávislé a v různých prostředích, ale není organizované. Z toho důvodu mu dále není věnována pozornost, protože se objevuje neplánovaně, tudíž na jeho výskyt není možné spoléhat.

Propojení forem vzdělávání má přinést spojení jejich výhod s omezením limitů. To je ale možné jen v případě, že si strany budou důvěřovat a vzájemně se podporovat[364]. Toho lze dosáhnout kvalitou vzdělávání a komunikací klíčových osob, jejichž vzdělávací snahy se budou propojovat ve spolupráci, budou respektovat práci ostatních, ne ji degradovat na nižší. Že to je možné, ukazuje i případová studie v kap. 9. Protože se jedná o systém založený na důvěře, spolupráce přestává být funkční, pokud se důvěra ukáže jako nepodložená (např. kvůli

[360] DELORS 1996
[361] Communication from the Commission of the European communities 2001
[362] Viz např. Commission staff working paper impact assessment 2012
[363] STASIUNAITIENE 2009
[364] HARRIS 2012

nekvalitní výuce), pak je náročné její získání zpět. Není možné, aby se spolupráce omezovala na tolerování se, je nutné najít vazby mezi formálním a neformálním vzděláváním, na což upozorňuje i Asociace evropských univerzit[365].

Přestože role neformálního vzdělávání je uznávána již poměrně dlouho, v praxi není dostatečně rozvíjeno. Nový impulz se objevil s tzv. MOOC (Massive Open Online Course), kdy se zájemci mohou často zdarma přes internet učit od expertů bez ohledu na geografickou vzdálenost, jen ze zájmu, bez získání uznatelného certifikátu. Pozitiva a negativa těchto kurzů jsou ale stále diskutována[366]. Obecně se neformální vzdělávání stává stále populárnější, i vzhledem k rostoucí kritice nastavení současného formálního vzdělávání[367]. Právě neformálnost totiž umožňuje snazší reflektování proměn ve společnosti, a to jak na úrovni formy vzdělávání (viz následující kapitola), tak i v obsahu.

Neformální vzdělávání je významné s ohledem na svoje charakteristiky nejen pro profesní rozvoj, ale často více pro rozvoj osobní a občanský. Dává prostor vzdělávat se v oblastech, které aktuálně člověk pociťuje jako potřebné, čímž se neformální vzdělávání přibližuje potřebám pro celoživotní učení, jehož význam vychází ze změn ve společnosti, které vyžadují nové dovednosti od občanů. Neformální vzdělávání přitom dává jedinci větší prostor vytvořit si vlastní cestu pro učení, která odpovídá právě jeho osobním potřebám[368]. Tento rozvoj se pak často neodráží v profesním uplatnění, jako spíše v sebevědomí jedince a spokojenosti se schopností udržet si svou roli ve společnosti[369].

Role knihoven v neformálním vzdělávání je dána jeho vymezením odpovídajícím aktuálním činnostem a roli knihoven (viz kap. 4.1). Nedeklarují to ale jen samy instituce. Při výzkumu vzdělávaných, jaké preferují místo pro učení (bez ohledu na to, zda formální či neformální), se knihovny objevily na 5. místě, jako preferované je označilo 6,9 % respondentů[370]. Další výzkumy vzdělávání v knihovnách (se zaměřením na prostředí ČR) byly již popsány v kap. 6.3.

[365] BJØRNÅVOLD 2008
[366] Např. MACKNESS 2010
[367] TERESEVIČIENĖ 2008
[368] JANSSEN 2011
[369] TERESEVIČIENĖ 2008
[370] TUOMAITE 2008

8.1.2 Aktivní učení a model E-U-R

Jedna z výhod neformálního vzdělávání je možnost většího prostoru pro aktivní učení[371]. Škola je často omezena počtem lekcí, dlouhodobými studijními cíli, autoritou učitele udržet ticho a pořádek během výuky. Samozřejmě tato omezení jsou různě silná ve školách či ve třídách, ale mnoho z nich je nezbytných pro každodenní efektivní formální vzdělávání. Současně jsou však bariérami pro aktivní učení, kde je každý příspěvek vítaný a kde se více jedná o učení pomocí dělání. Není kladen důraz jen na znalosti, ale také na vytváření dovedností a postojů[372], což odpovídá současným snahám na mezinárodním poli vzdělávání i v českých koncepcích, např. formalizovaných do Rámcových vzdělávacích programů různých úrovní[373].

Aktivní učení je založeno na zapojení vzdělávaných do výuky pomocí různých aktivit, přičemž probíhá interakce mezi vzdělávanými i směrem k vzdělávajícímu, častá je proto skupinová práce a diskuze v různých formách. Aktivity staví na reálných situacích, které vzdělávaní znají nebo si je snadno dokáží představit. Zapojení vzdělávaných vede ke zvýšení motivace se učit a také ke zvýšení retence získaných znalostí[374], současně se skrz ně učitel stává facilitátorem znalostí a vzdělávaní získávají pozici, kdy kvalita výuky je dána jejich vlastní činností, což vede k větší zodpovědnosti za výuku i její výsledky, ale také vzdělávané více baví. To vše reflektuje charakteristiky připisované především mladším generacím (od Generace Y)[375]. Aktivní učení také posouvá poznání od pouhého přenosu informací, vede mnohem více k zapojení vyšších úrovní Bloomovy taxonomie výukových cílů. Odpovědnost a nadšení vzdělávaného také značně zvyšuje pravděpodobnost přenesení získaných znalostí po lekci do jeho širšího okolí[376], což by v případě informační bezpečnosti bylo velmi pozitivní vzhledem k stále nevyřešenému způsobu zaujetí dospělých v produktivním věku pro tuto problematiku.

Tím, že je výuka založena na aktivitách pro jednotlivce a malé skupiny, je kladen důraz na podobnou charakteristiku jako u neformálního vzdělávání, tj. že

[371] GRECMANOVÁ 2000
[372] HANSEN ČECHOVÁ 2006, s. 10
[373] Rámcové vzdělávací programy © 2013 – 2014
[374] POLING 2009
[375] HARRIS 2010
[376] PETRESS 2008

vzdělávaný si učení přizpůsobuje svým potřebám a aktuální situaci, vč. předchozích znalostí a zkušeností. „*Přednostmi tohoto učení jsou silné podněty, rychlé vnímání plné zájmu, spontánní aha-efekty a prožitky úspěchu a rovněž snadno vybavitelné uložení v paměti.*“[377] Princip vychází ze současných trendů učení založených na konstruktivistickém přístupu[378], kdy je důraz kladen právě na individualitu vzdělávaných, kterou je nutné reflektovat i při výuce tříd, tedy větších skupin. Přestože se jedná o poměrně nový a stále se prosazující přístup ke vzdělávání, jeho kořeny je možné pozorovat již v 80. letech 20. století[379].

S aktivním učením souvisí příbuzné konstruktivistické přístupy, které akcentují charakteristiky jmenované výše. Důraz na interakci mezi účastníky lekce klade tzv. kooperativní učení. Vychází ze způsobu řešení neznalosti v běžném životě zeptáním se na odpověď. Ne vždy je odpovídající expert, někdy je i přínosnější se zeptat známého, kterému člověk důvěřuje a který sdělí potřebné způsobem, který je pro oba přijatelný, byť ne z odborného hlediska zcela přesný. Pozitiva vzdělávání dětí touto formou uvádí Kasíková: „*U dětí se projeví v úrovni začlenění do procesů učení, v kvalitě myšlenkových operací, v rozsahu a úrovni řeči, v kvalitě dokončené práce, vyšší míře samostatnosti a nezávislosti na vzorech, vyšším sebevědomí a sebedůvěře.*“[380] Tak je rozvíjena znalost tématu, ale i tzv. klíčové kompetence (také kompetence pro 21. století apod.), které zvyšují uplatnitelnost člověka v kolektivu, ale vedou také k návykům pro celoživotní učení[381]. Vedle pozitiv k vlastní osobě Kasíková[382] upozorňuje i na změny vůči okolí: učení se postojům, hodnotám, dovednostem a znalostem od vrstevníků nápodobou těch, kteří vlastní uznanou kvalitu, učení se pomoci a sdílení, budování schopnosti pohlížet na problém nejen z vlastního úhlu pohledu, budování autonomie osobnosti, přijetí odlišnosti vlastní i ostatních, zvýšení výkonu motivací, když je viděna práce ostatních ve skupině a současně odbourána obava z chyby. Obava z chyby je odbourávána první kontrolou ve skupině před prezentací ostatním, ale i při jejím výskytu je nutné k ní přistupovat odlišně než v tradiční výuce, měla by představovat stimul pro další učení.

[377] BELZ 2001, s. 65
[378] SMART 2012
[379] HARRIS 2012
[380] KASÍKOVÁ 1997, s. 8
[381] BELZ 2001
[382] KASÍKOVÁ 1997, s. 35-37

Aktivní učení se silně vyvíjí podle vzdělávaných, je tedy výrazně náročnější pro vzdělávajícího. Ten musí být dobře připraven znalostmi, tak na změny formy vzdělávání, pokud se některá z plánovaných aktivit ukáže jako nevhodná pro danou skupinu nebo se vyvíjí odlišně, než bylo plánováno (např. její provedení trvá déle, takže bude nutné zkrátit jinou aktivitu). Další výraznou změnou proti tradiční výuce je silný nárůst hlučnosti vzdělávaných a vyšší nároky na obnovu pozornosti k vzdělávajícímu, což je logický důsledek toho, že interakce mezi vzdělávanými a také zaujetí pro aktivitu je základem aktivního učení. Jinou změnou, kterou je také nutné akceptovat při aktivním učení, je zmenšení šířky probraného učiva, což je cenou za to, že se naopak jde do hloubky. Protože vzdělávaní ovlivňují směr výuky, je zásadní, aby byli dobře seznámeni na začátku lekce s výukovými cíli a byli také schopni zhodnotit jejich dosažení[383].

Aktivní učení se již osvědčilo i v knihovnách, dokonce i akademických, např. knihovna Pennsylvania State University ho využila formou hry při rozvoji informační gramotnosti studentů, jiná hra pro stejný účel vznikla na University of North Carolina[384]. V ČR je využíváno spíše v základních knihovnách, prosazují jej zejména zástupkyně IVU SDRUK Lenka Navrátilová (Městská knihovna Polička) a Veronika Peslerová (Krajská knihovna Vysočiny). Spojení aktivního učení a informační gramotnosti vidí Grecmanová tak silné, že by mělo být začleněno jako přístup k celému učebnímu obsahu[385].

Aktivní učení, jak bylo řečeno, vychází z konstruktivizmu, ovšem může mít různé výukové rámce. V návaznosti na Piagetovu teorii patří mezi nejčastěji užívané rozdělení do tří fází: evokace, uvědomění a reflexe[386]. Každá fáze má svou roli a vychází z někdy intuitivně používaných postupů ve vzdělávání.

Evokace má vzdělávanému připomenout jeho již dříve nabyté poznatky k tématu, což podporuje motivaci, protože navazuje na známé a představitelné pro využití ve vlastním reálném životě. Nestačí, že tyto poznatky existují, je nutné je aktivitou zapojit do lekce, uvědomit si různé související znalosti k tématu. „*Cílem této fáze je tedy žáky aktivizovat, motivovat, vzbudit v nich vnitřní zájem problém řešit.*“[387] V tradiční výuce lze evokaci přirovnat k opakování učiva.

[383] PIHT 2012
[384] HARRIS 2010
[385] GRECMANOVÁ 2000, s. 9
[386] PIHT 2012
[387] HANSEN ČECHOVÁ 2006, s. 30

Uvědomění si významu je druhou fází vzdělávacího rámce, kdy dochází k předání nových poznatků. I zde může být využito vzdělávací aktivity, ale může se jednat také o tradiční frontální výuku[388], pokud je vhodná pro téma lekce a skupinu vzdělávaných. I v tomto případě je vhodné proložení drobnými aktivizačními metodami pro udržení pozornosti vzdělávaných. Není možné lekci omezit na tuto fázi a počítat s tím, že ostatní vzdělávaný zvládne sám bez vedení.

Závěrečnou fázi představuje reflexe, která slouží ke zhodnocení získaných zkušeností a poznatků, ověření, že došlo k správnému pochopení, k hlubšímu zakotvení informací ve znalostní struktuře. V tradiční výuce si tuto fázi lze z části přiblížit zkoušením, které také slouží oběma stranám ve výuce k ověření, že došlo k správnému přenosu poznatků. V případě reflexe je toto zjištění pouze informativní a je nezbytné tuto fázi realizovat ihned po fázi uvědomění, protože slouží k upevnění poznání před zapomenutím. Známky a produkt učení se při reflexi stávají sekundárními, vzdělávaní často dochází k uvědomění, že důležitější je pro ně proces učení, kdy získává zpětnou vazbu od ostatních, ne od vzdělávajícího[389]. Klíčové přitom je, aby se při reflexi dostala vzdělávanému také zpětná vazba od vzdělávajícího, nestačí sebehodnocení vlastního výkonu.[390] Cílem reflexe je také motivovat k dalšímu učení v řešené problematice tím, že student bude zaujat aktivitami a také si bude vědom dosažení výukových cílů, projeví se tedy pozitivní emoce v podobě spokojenosti s vlastním výkonem.[391]

Z vymezení aktivního učení v této kapitole vyplývá, že pro knihovny může být tento postup jednodušeji využitelný než u institucí formálního vzdělávání. Současně představené výhody mohou posílit vzdělávací roli knihovny a zaujmout nejen pro předmět lekce, ale také budovat pozitivní vztah vzdělávaného k samotné instituci. Nevýhody přístupu mohou být v knihovně tolerovány vzhledem k tomu, že se jedná o neformální vzdělávání. Proto jsou aktivní učení i struktura evokace – uvědomění – reflexe využity v dále popsané koncepci vzdělávání v knihovně o bezpečnosti digitálních stop.

[388] GRECMANOVÁ 2000, s. 27
[389] KASÍKOVÁ 1997, s. 91
[390] PIHT 2012
[391] PIHT 2012

8.2 Metodika lekcí v knihovně o bezpečnosti digitálních stop

Podobně jako v běžné výuce je nutné nastavit předávané informace podle jejich příjemce[392]. Vzhledem k tomu, že tato dizertační práce navrhuje nové, ne rozšiřující řešení, navržená koncepce je jen prvním stupněm komplexní nabídky vzdělávání o digitálních stopách, které mohou zprostředkovat knihovny. Lekce je propojena se základním vzděláváním, je zde tedy potenciál oslovit celou populaci, pro kterou je určena. Vzhledem k výukovým cílům[393] v první a druhé třídě základní školy je koncepce nastavena až od následujícího ročníku. Mimo první lekci jsou návrhy vždy doporučeny pro dva po sobě následující ročníky, tato varianta byla zvolena s ohledem na omezené možnosti výuky v knihovně, především na 2. stupni základní školy. Téma informační bezpečnosti není pro knihovnu jediné, které by měla žákům předávat, v návrhu je proto prostor pro proložení lekcí dalšími tématy, uvažován je jiný přístup k informační bezpečnosti v podobě autorství a důvěryhodnosti informací na internetu. V případě nadané třídy je také možnost nasazení lekce pro nižší ročník, než je doporučení, příp. pro méně nadanou třídu naopak, protože doporučení se vztahuje spíše k průměrným znalostem a dovednostem žáků v daném vývojovém období.

Pro správné předávání poznatků je vždy nezbytná znalost základních pojmů, aby nedošlo k mylnému spojení informací s něčím, čeho se zcela netýkají. Proto je tématem první lekce (pro 3. třídu) řešení základních pojmů a funkcí souvisejících s internetem. Po tomto ujasnění je již možné s 4. a 5. třídou zaměřit se na základní principy bezpečné komunikace přes internet, především při kontaktu s člověkem neznámým z fyzického prostředí. Pro 6. a 7. třídu je nabídnuta problematizace předchozího tématu v tom, že jsou žáci upozorněni na využití sociálního inženýrství a krádeže identity, které jsou v prostředí internetu snadné a využívané. Současně s tím dostanou bližší tipy k užívání bezpečných hesel, která patří mezi zásadní prvky internetové bezpečnosti a přispívají i v ochraně proti problémům v této lekci. Závěrečným tématem koncepce vzdělávání o internetové bezpečnosti pro základní školy jsou typy útoků, se kterými se mohou setkat při zneužití digitálních stop. Přiblížením přes informace zanechávané na silně

[392] ČÁP 1993; FONTANA 1997; VÁGNEROVÁ 2005
[393] Rámcový vzdělávací program pro základní vzdělávání 2007

využívané sociální síti Facebook[394] jsou děti seznámeni s povídkami vycházejícími z reálných útoků na děti při zneužití jejich digitálních stop. Snahou je přitom upozornit je nejen na typické prvky průběhu daného typu útoku, ale také umožnit jim uvědomit si možnost vlastního ohrožení přes podobné chování. Na tuto základní aktivitu navazuje rozbor různých možností nastavení soukromí na příkladu aktuální nabídky Facebooku.

Lekce na sebe navazují v oblasti náročnosti znalostí, lze je ale realizovat také samostatně, pokud žáci mají dostatečné znalosti pro zvládnutí problematiky. Metodika v následujících kapitolách je určena především knihovníkům, kteří lekce budou realizovat ve své knihovně, čemuž odpovídá forma a obsah návrhu. Nejdříve jsou vždy uvedeny předpoklady pro realizaci lekce, následně jsou popsány jednotlivé aktivity a jejich význam pro lekci, pracovní materiály k nim jsou obsahem přílohy 2. Na závěr je odkázáno na zkušenosti z realizace lekce a na doporučené zdroje pro lektora, kde je možné najít další informace k řešené problematice a které byly také z části použity pro tvorbu návrhu lekce.

Dále představená koncepce byla prezentována na seminářích pro knihovníky[395], na základě toho byla vyžádána pro nasazení ve vlastních aktivitách knihovnami (řazeno abecedně):

- Jihočeská vědecká knihovna v Českých Budějovicích
- Knihovna Jiřího Mahena v Brně
- Krajská knihovna Františka Bartoše
- Krajská knihovna v Pardubicích
- Městská knihovna a infocentrum Dolní Bousov
- Městská knihovna Český Těšín
- Městská knihovna Havířov
- Městská knihovna Orlová
- Městská knihovna Pelhřimov

[394] PEMI 2012

[395] Kdo je za monitorem a mnoholičný lektvar (Workshop Informační vzdělávání v knihovnách – Jak na to kreativně 2013), Bezpečná internetová komunikace akademika s dětmi v městské knihovně (Národní seminář informačního vzdělávání 2013), Bezpečnost dětí na internetu v knihovnách (Nebezpečný internet v KJM 2013), Kdo je za monitorem? (Seminář Informační vzdělávání uživatelů ve veřejných knihovnách 2014)

- Městská knihovna Rožnov pod Radhoštěm
- Městská knihovna Třinec
- Městská knihovna v Praze
- Městská knihovna v Jaroměři
- Severočeská vědecká knihovna Ústí nad Labem

Od knihovníků byla při sdílení žádána zpětná vazba, jejímž smyslem je upravení koncepce pro srozumitelnost i na základě zkušeností z různých prostředí. Veškeré reakce knihovníků i žáků byly pozitivní, ukázalo se ale, že nezbytnou součástí metodiky je vymezení neformálního vzdělávání, aktivního učení a rámce evokace – uvědomění – reflexe (viz kap. 8.1), protože někdy nebyla dodržena didaktická pravidla a tím byl omezen vzdělávací efekt lekce. Materiály lze šířit při uvedení autorky, lze je i upravit, další šíření ale musí obsahovat i původní verzi.

Společné charakteristiky lekcí:

- Jedna třída, tj. 20-30 dětí;
- Časová dotace 90 minut (dvě vyučovací hodiny), zahrnuje 10 min. rezervu pro přesuny, v případě nepotřebnosti jí lze prodloužit fázi uvědomění; časová náročnost je popsána vždy u jednotlivých aktivit v osnově lekcí;
- Struktura lekce E-U-R (evokace – uvědomění – reflexe);
- Na konci každé osnovy je *5 otázek s dospělými*, které by každé dítě mělo po lekci dostat pro diskuzi s rodiči v nejbližších dnech a následně pro diskuzi s učitelem přibližně do týdne od lekce, otázky slouží pro zahájení diskuze o problematice mezi dítětem a dospělým, ideálně rodičem, příp. učitelem; cílem je uvědomění si, jak se dítě chová na internetu z hlediska bezpečnosti, co zná a co skutečně dělá, na druhé straně pro dítě může sloužit pro ujištění, že dospělý je to pro něj k dispozici i pro řešení problémů na internetu;
- Součástí metodiky každé lekce je také krátký seznam doporučených zdrojů, jejichž obsah odpovídá požadovaným znalostem lektora, pro potřeby dizertační práce není zařazen v textu metodiky, ale pro přehlednost je umístěn až za seznamem použitých zdrojů pro tuto práci;
- Odkazované pracovní materiály jsou obsaženy v příloze 2.

8.2.1 Terminologie a základní funkce internetu

Správné pochopení tématu musí být založeno na porozumění pojmům. Libovolné vzdělávání dětí o internetu tedy musí navazovat na lekci, která jim pomůže zažít si základní odborné pojmy, které jsou dále aplikovány pro objasnění funkcí internetu, jeho principů i negativ využití. Obsah je naplněn praktickými a herními aktivitami k udržení pozornosti dětí při nezbytném uvedení termínů.

Předpoklady a cíle lekce

Cílová skupina

- Žáci 3. třídy základní školy.
- Stačí základní povědomí o internetu, nejsou nutné zvláštní znalosti.

Očekávané výstupy

- Zlepšení komunikačních a sociálních kompetencí (vlastní názor, prezentační dovednosti, práce ve skupině, naslouchání, sebereflexe).
- Orientace a správné užívání odborných pojmů souvisejících se základními postupy při využití počítače a internetu.
- Dovednosti pro praktické využití vybraných funkcí internetu, především v oblasti vyhledávání informací a materiálů různé formy.

Materiální zajištění

- Tabule, papíry a psací potřeby, stoly či podložky pro psaní
- Šest počítačů, notebooků, tabletů nebo podobných zařízení, min. jeden bez a jeden s nainstalovaným Skype
- Rozstříhaný text materiálu *Funkce internetu* bez očíslovaných odstavců, vždy díly jedné funkce promíchané vložené do jedné obálky
- Pracovní listy: pracovní materiál *Pětilístek* (pro každého žáka)

Zkušenosti lektora

Jedná se o úvodní lekci k tématu internetu. Nároky na lektora proto nejsou vysoké, měl by mít znalosti o základech fungování internetu a měl by dokázat vysvětlit základní odborné pojmy, které se týkají práce s počítačem a internetem, především v oblasti vyhledávání informací v různých formách (textové, obrazové,

videa). Lektor pro potřeby asistence žákům by měl vědět, jak vytvořit a používat tzv. desetiminutový e-mail, vedle toho by měl mít zkušenosti se všemi činnostmi, které budou realizovat žáci, aby s nimi mohl sdílet zkušenosti.

Cílem lekce je, aby si děti zažily odborné pojmy spojené s internetem a počítačem. Všechny aktivity se tedy úmyslně týkají této jediné oblasti, protože je nezbytná pro efektivní práci v lekcích o internetu. Současně si přes pojmy ujasní některé principy fungování internetu. Činnosti ve fázi uvědomění lze měnit a doplňovat, vždy by se ale mělo jednat o funkce, které děti mohou používat ve svém věku, nemá tedy smysl zařazovat např. nakupování přes internet.

Osnova lekce *K čemu je internet?*

Šibenice na odborné pojmy spojené s internetem a počítačem (15 minut)

Lekce je dle struktury E-U-R zahájena aktivizační činností, která by měla dětem ukázat atraktivnost lekce a podpořit v zapojení do aktivit zbavením obavy díky práci s tím, co už znají. K tomu je využita hra šibenice. Aby byla zapojena celá třída a aktivita nebyla příliš časově náročná, děti jsou rozděleny na třetiny do týmů podle místa, kde sedí, celý tým sedí proti své třetině tabule. Děti vidí počet písmen ve slově znázorněný čárkami. Po domluvě tipují písmeno a snaží se uhádnout skryté slovo, týmy se střídají po jednom tipnutém písmenu. Při každém špatném tipu je dokreslena další část šibenice, pokud je obrázek kompletní (po 12 neúspěšných tipech), tým prohrál. Slova jsou použita z materiálu Funkce internetu (zvýrazněna tučně), volba záleží na lektorovi, ale pro zjednodušení je vhodné volit delší slova a mít podobnou obtížnost pro stejná kola, např.:

1. kolo: monitor, Facebook, klávesa;
2. kolo: prohlížeč, vyhledávač, software;
3. kolo: profil, soubor, ikona.

Aktivita je podána jako soutěž, protože vítěz získá výhodu do další aktivity tak, že si děti z vítězného týmu první losují své *puzzle* (viz další aktivita).

Puzzle na funkce internetu

50 minut:

- max. 5 minut vysvětlení postupu aktivity

- 15 min. skládání částí a vyzkoušení výsledku
- 30 minut prezentace

Pro fázi uvědomění je využito aktivity typu skládání puzzle. Cílem je správně sestavit postup pro využití funkce internetu z rozstříhaného návodu po odstavcích. V něm jsou tučně označeny termíny, odstavce ale nejsou řádkovány. Každá funkce internetu má všechny své části v jedné obálce, týmy obálky losují. Týmy jsou vytvořeny z třetin žáků v evokační fázi, které jsou rozděleny na poloviny. Tím vznikne šest týmů, je tedy možné vyřadit aktivitu z pracovního listu, která je technicky v knihovně problém. Obálky jsou označeny čísly, která odpovídají číslům napsaným u pracovních stanic, u kterých celá aktivita probíhá. Ta správná stanice není ukázána lektorem, ale děti ji mají hledat, což by mělo zvýšit zábavnost. Týmy mohou u zařízení skládat návod z puzzle a současně si správnost ověřovat zkoušením. Pokud něco neodpovídá, zkouší sestavení znovu. Je na každém týmu, aby si práci zorganizoval. Jak bude výsledek sestaven, záleží na dětech, lektor do jejich činnosti nezasahuje, jen sleduje čas a upozorňuje děti na jeho postup, je k dispozici, když něco není jasné. Jinak děti pouze sleduje, aby v diskuzi mohl navazovat na to, co viděl.

K některé činnosti jsou specifické pokyny, které je by měly být dětem řečeny při vysvětlování aktivity. Dopředu jsou upozorněny, že při registraci nemají zadávat svůj e-mail, ale mají zavolat lektora, který pro skupinu vytvoří 10minutový e-mail. Heslo pro registraci je dětem zadáno, mělo by být silné (např. „Moje!hes10.“, kde je využita podobnost dvou posledních písmen a číslic, zadání je zdůvodněno tím, aby omylem nesdílely to, co reálně používají, protože to by neměly nikomu říkat). Zadáním se omezí dohady, vysvětlení problematiky silných hesel je již nad rámec i časové možnosti této lekce. Poslední scénář není losován, je ponechán pro nejrychlejší skupinu jako bonusový. Je výrazně náročnější proti ostatním. Bude skupině podán způsobem, že když jsou tak šikovní, tak pravděpodobně internet dobře znají a lze jim zadat něco opravdu těžkého. Pokud aktivitu zvládnou, zvýší to jejich sebehodnocení, v opačném případě nebudou demotivováni, protože došli alespoň do části postupu.

Poté, co jsou všechny týmy přesvědčeny o správnosti svého výsledku a vyzkoušely si daný postup, příp. pokud vypršel čas, sejdou se k prezentaci výsledků. Nejdříve převyprávíí (z časových důvodů nečtou) skládanku, střídají se

po větě a poté se mohou doplnit. Lektor sleduje správnost, ale nezasahuje. Následuje fáze dotazování, kde již lektor může upozornit na nesprávnou část přes problém v simulaci postupu. I v případě správného výsledku jsou děti povzbuzovány podělit se o zkušenosti z praktické části aktivity, resp. zkušenosti s aktivitou před lekcí a vyjádřit se ke znalosti či neznalosti zvýrazněných pojmů. Neznámé či chybně vysvětlené pojmy lektor vysvětluje v průběhu diskuzní části.

Pětilístek pro vybraný termín (15 minut)

Fáze reflexe je opět navázána na pojmy z předchozí aktivity. Každé dítě si zvolí libovolný pojem ze zvýrazněných ve skládance, které se věnovalo. Doporučen je ten pro ně nejznámější. Následně si doplní pětilístek (viz pracovní materiál *Pětilístek*). Tímto postupem se hlouběji zamyslí nad podstatou, ale také využitím obsahu pojmu. Při dostatku času jsou výsledky představeny na lekci, v opačném případě jsou děti instruovány vystavit si pětilístky ve třídě a seznámit se s ostatními. Fáze reflexe (podobně jako v ostatních lekcích) může být také podkladem pro rozbor ve třídě s pedagogem. Prováží se tak získané znalosti s prostředím školy.

5 otázek s dospělými

1. K čemu používá každý z vás internet?
2. Když něco nevíte, jak to hledáte na internetu?
3. Jak přemýšlíte o tom, jestli tomu, co jste našli, můžete věřit?
4. Jak se bavíte s jinými lidmi přes internet?
5. S kým se tak bavíte?

8.2.2 Ochrana osobních údajů v internetové komunikaci

Komunikace přes internet je běžnou součástí života dospělých, ale mnohem více dětí a dospívajících, pro které se jedná o přirozenost, proto jsou někdy označováni jako *net generation*. Stejně jako v reálném prostředí se i v tom elektronickém seznamují s novými lidmi. S ohledem na malou životní zkušenost ale hůře rozeznávají varovné signály, když s komunikací a novým známým není něco v pořádku. Proto jsou náchylnější k problémům, které mohou zasáhnout

i dospělé. Lekce pomůže s využitím soutěžní aktivity jednotlivých dětí pochopit základní problémy komunikace přes internet s neznámými lidmi. Děti si zažijí klíčové principy, které je možné rozvíjet v navazujících lekcích. Cílem je upozornit na obvyklé postupy pro zjišťování zneužitelných osobních informací, zejména těch, které vedou k identifikaci žáka ve fyzickém prostředí.

Předpoklady a cíle lekce

Cílová skupina

- Žáci 4. – 5. třídy základní školy.
- Běžné uživatelské znalosti v tomto věku, vhodná je orientace v základních pojmech souvisejících s internetem a jeho funkcemi (nejen komunikace).

Očekávané výstupy

- Zlepšení komunikačních a sociálních kompetencí (vlastní názor, prezentační dovednosti, práce ve skupině, naslouchání, sebereflexe).
- Rozpoznání obvyklých postupů pro zjišťování zneužitelných osobních informací v komunikaci na internetu v praxi.
- Identifikace zneužitelných informací, zejména s potenciálem nalezení žáka ve fyzickém prostředí.
- Uvědomění si významu ochrany informací v elektronickém prostředí.
- Postoj odmítnutí sdělit zneužitelnou informaci o sobě či jiném.

Materiální zajištění

- Dvě místnosti (ne vzdálené).
- Tabule v hlavní místnosti, tabule či prostor pro vyvěšení papíru v druhé místnosti, magnety, papíry a psací potřeby, stoly či podložky pro psaní.
- Velké nápisy (čitelné žáky v místnosti) s typy komunikace na internetu – viz pracovní materiál *Mapa komunikace*.
- Pracovní listy: *Tabulka zjištěných identit* (pro polovinu žáků s čísly, pro polovinu s písmeny) a *Když se mě někdo zeptá* (pro skupiny 3-4 žáků).

Zkušenosti lektora

Lektor by se měl orientovat v typech a nejpoužívanějších službách internetové komunikace, zejména v u dětí aktuálně oblíbených online hrách. Hry

a komunikační možnosti populární v době přípravy metodiky jsou uvedeny v materiálu *Mapa komunikace*. Ten je nutné upravovat s vývojem trendů. Pokud nemá lektor možnost zjistit trendy v této oblasti, může se nechat poučit dětmi. Toto poučení nesníží jeho odbornost, pokud projeví zájem a obecnou orientaci.

Zásadní je střízlivý přístup ke zneužitelnosti informací, neměl by být ani příliš striktní, ani benevolentní, aby děti viděly, že bezpečnost v komunikaci lektor bere vážně, ale nesnaží se jim zakázat pro ně nezbytnou součást společenského života, která přispívá k budování jejich postavení v kolektivu a pozitivní digitální stopy. Lektor by měl dále mít přehled o stylu běžné komunikace dětí na internetu, tedy co a komu jsou ochotny sdělit. To lze vysledovat ve veřejné komunikaci dětí, anebo zjistit z výzkumů, např. EU Kids Online nebo e-Bezpečí (viz kap. 11.5 Použité zdroje v navrhované metodice).

Aktivity se mohou zdát příliš jednoduché s ohledem na to, co vše by měly děti znát. S ohledem na časovou dotaci, záživnost a hlubší pochopení je vhodné zůstat na stanovené úrovni a předat sice pouze základy, ale kvalitně. Lekce, zejména soutěž, byla pozitivně hodnocena i 6. třídou speciální základní školy po úpravách a realizaci v Městské knihovně Pelhřimov (dle e-mailové komunikace s Lenkou Havlovou ze dne 19. 2. 2014).

V 5. třídě děti více sledovaly jazykové prohřešky, lze předpokládat, že ve škole by soutěž byla tímto poznamenána více a mohlo tím dojít ke zpomalení komunikace, protože by děti strávily více času přemýšlením nad formou. V knihovně byla soutěž uvolněnější, pomohl tomu také papír A4 bez linek.

Osnova lekce *Kdo je za monitorem?*

Brainstorming

15 minut:

- 5 minut způsoby komunikace na internetu
- 10 minut vyhodnocení

Na začátku lekce jsou děti povzbuzeny, aby se podělily o to, co znají. Uvolní se tak obavy a děti se zapojí do lekce, vytváří si ji do značné míry samy. Je nutné, aby lektor dodržoval pravidla brainstormingu, ale nemusí je vyžadovat po dětech. Poznamenává či dává na tabuli bez komentářů vše, co děti jmenují, že

používají nebo ví, že to někdo v jejich blízkosti používá. Pokud se děti kritizují, lektor komunikaci usměrní a povzbuzuje do jmenování dalších druhů komunikace. Pokud se neobjevují další nápady, dodá nápovědu směřující k připraveným typům (ale nejmenuje je), např. pokud chce slyšet videohovory, tak se zeptá, jestli děti znají něco, pomocí čeho by přes internet s někým mohly mluvit a současně jej vidět. Není nutné, aby se na tabuli objevilo vše připravené, základní kategorie by ale měly být zastoupeny.

Po získání dostatečného množství způsobů komunikace od dětí převezme slovo lektor a pomocí dotazování dětí se snaží vytvořit kategorie na základě barev nápisů tak, že se ptá na specifika dané komunikace a odpovědi upřesní. Děti si touto formou uvědomí, co vše znají, a současně si doplní své názory.

Následně lektor upozorní na paralelu s reálným prostředím, kdy na internetu, stejně jako na ulici či v kroužku, je možné poznávat nové lidí. Většina služeb umožňuje komunikaci lidí, kteří se dříve neznali, a současně se obvykle navzájem nevidí. Podobnou situaci bude simulovat soutěž ve fázi evokace.

Soutěž v odhalování identity internetového známého

35 minut

- max. 5 minut vysvětlení pravidel
- 30 minut soutěž se simulací komunikace na internetu pro poznání druhého člověka

V rámci fáze uvědomění jsou děti po vysvětlení pravidel rozděleny losováním na dvě skupiny. Každé dítě si vylosuje jedno číslo či písmeno, které by nikdo jiný neměl vidět, jedna skupina se přesune do druhé místnosti. Hra spočívá v posílání dotazů a odpovědí mezi jednotlivci z různých skupin, kdy cílem je zjistit identitu co nejvíce dětí z druhé skupiny (za každou správnou získá bod), a současně chránit vlastní identitu před odhalením (za každé odhalení ztratí bod).

Aby hra fungovala, jsou představena pravidla komunikace, která jsou během celé soutěže viditelně napsána v obou místnostech. Děti se označují vylosovaným číslem či písmenem, jsou zakázána veškerá jména, a to nejen dětí samotných. Není možné položit otázku např. na jméno nejlepšího kamaráda. Protože v elektronickém prostředí plní podobnou funkci jako jméno e-mailová

adresa, ze které je navíc často jméno rozeznatelné, jsou zakázány i tyto informace. Další pravidlo je v příkazu, že je nutné odpovídat pravdu, a to na každou otázku. Při nepravdě či neposkytnutí odpovědi by totiž hra neměla smysl, protože by nebylo možné nikoho odhalit.

Aby bylo možné rozlišit, kdo si s kým píše, je každá komunikace nadepsána odpovídajícím číslem a písmenem, např. A1, tedy dítě A si píše s dítětem 1. Pro zjednodušení každé dítě dostane první papír ke komunikaci nadepsaný, čísla píší písmenům na stejné pozici v abecedě, písmena číslům o jedno vyšším. Při zahájení má tedy každé dítě dva komunikační partnery, v případě lichého počtu žáků má jedno dítě tři a jedno jednoho. To se vyrovnává tím, že následně je možné zahájit libovolný počet komunikací. Přitom je nutné upozornit na omezený čas pro soutěž, tedy omezené množství položených otázek, při směřování na mnoho stran zjistí o každém příliš málo informací pro odhalení (ideální jsou 3-4 komunikace během celé soutěže). Zprávy mezi místnostmi přenáší lektor, ideálně s pomocníkem (lze využít učitele). Ti od dveří vyhlašují písmena či čísla, pro která mají zprávu, pohyb dětí usnadňuje práci lektorovi a současně přispívá udržení soustředění dětí. Dítě vždy odpoví na položenou otázku a samo se zeptá na to, co potřebuje pro odhalení identity. Pokud si komunikující myslí, že toho druhého poznali, stále nepíší jméno, ale *znám tě*, komunikace končí, až si toto napíší oba. Aby nezapomněli, koho odhalili pod jakým označením, zapisují si jména do tabulky (viz pracovní materiál *Tabulka zjištěných identit*). Pro zahájení děti dostanou příklady možných otázek, např. *Jsi kluk nebo holka? Jaký je tvůj oblíbený zpěvák? Co hraješ na internetu?*

Během přenášení zpráv je lektor k dispozici jako rádce při nejasnostech. Děti jsou na začátku upozorněny, že soutěží každý za sebe, není jim ale bráněno v komunikaci v rámci skupin. Samy sdílí vhodné otázky a odpovědi, jen při sdílení totožností by měl lektor zasáhnout vysvětlením, že kazí výsledek samy sobě. V průběhu aktivity i bez zásahu lektora pokládají otázky, které znají z internetového prostředí. Také si samy, nebo díky jiným členům skupiny uvědomí, jaké informace je prozradí a jak odpovídat, aby k tomu nedošlo (např. při otázce na bydliště odpoví ČR, ne adresu). Lektor otázky (mimo ukázek), ani odpovědi nenapovídá. Přibližně 5 minut před koncem lektor upozorní, že nese poslední otázky, na které dostanou jejich odesilatelé odpovědi. Po doručení posledních

odpovědí si děti doplní tabulky identity podle svého přesvědčení a sejdou se opět v jedné místnosti.

Vyhodnocení s přednáškou pro komparací s prostředím internetu (15 minut)

Soutěž je vyhodnocena tak, že lektor postupně říká všechna čísla a písmena. Komu patří, ten řekne své jméno. Následně se přihlásí ti, kteří mají v tabulce správné jméno u správného označení, aby bylo jasné, kolik bodů se odečítá za odhalení. Děti se třemi nejvyššími počty bodů získají drobnou odměnu (placky s motivy internetu a IT, např. tablet, zavináč, logo Facebooku).

Po vyhodnocení lektor stručně připomene, jaká byla pravidla pro soutěž a proč. Přitom každé pravidlo postaví do protikladu s internetem, ale i reálným prostředím a upozorní tak děti na to, co poznaly v soutěži jako problém, a jak se mu mohou vyhnout. V souladu s principy aktivního učení jsou podporovány vstupy dětí se sdílením jejich zkušeností ze soutěže i reálného života.

Pravidlo zákazu jmen a e-mailů lze spatřovat v jejich identifikační funkci. V tradičním i internetovém prostředí je s nimi snazší dohledat další informaci či přímo člověka (např. s využitím telefonního seznamu či profilu na Facebooku) nebo se na další informace zeptat (např. jiná reakce na internetu i ve škole bude, pokud se zeptám na jméno nebo pokud se zeptám na přezdívku s tím, že třeba má ráda kočky). Jména a e-mailové adresy propojují profily na různých službách internetu, proto je dobré si dávat pozor, jaké informace je s nimi možné spojit.

Další pravidlo, které spočívalo v nutnosti říkat pravdu, neplatí v tradičním i internetovém prostředí. Současně je na internetu mnoho komunikace veřejné, proto může kdokoli vysledovat způsob komunikace a témata mezi dětmi a s jejich využitím si budovat důvěru a zjišťovat další informace. Proto se nelze spoléhat na pravdu od toho, s kým komunikujeme, zejména pokud jej neznáme z reálného světa. Internet totiž umožňuje mnohem snazší lhaní i v tom, co je ve fyzickém prostředí zjevné, např. věk.

Na závěr je pozitivně ukončeno neplatností posledního pravidla, tedy nutnost odpovídat. Dětem je dobré zdůraznit, že nikdo je nemůže nutit sdělit informaci, kterou poskytnout nechtějí. Současně existují situace, kdy je zjevné, že

něco není v pořádku. Mnoho z nich lze připodobnit k tomu, co je rodiče učí s ohledem na setkání s neznámým člověkem na ulici.

Setkání a ulici a soutěž v lekci by měly dát nápovědu dětem v tom, jakou informaci mohou poskytnout. Pokud se jich internetový známý na něco zeptá, měly by si říct, jestli by je odpověď odhalila v soutěži a jestli by ji poskytly neznámému člověku na ulici. Pozor by si měly dávat především na to, co může pomoci najít je ve fyzickém prostředí, např. adresa školy, jméno učitele, telefonní číslo, fotky, celé jméno, informace o blízkých. Důležité je také si uvědomit, že stejný přístup by měl být zachován, ať je předmětem dotazování člověk sám nebo i jeho známý. Stejně jako na internetu, i v soutěži se známost identity se může rozšířit i k dalším komunikujícím na druhé straně. Aby si rozhodování děti zažily, je na závěr lekce umístěna reflexe poznatků z lekce, kde si děti volbu poskytnutí informace vyzkouší v klidu a bezpečí knihovny.

Pracovní listy Když se mě někdo zeptá s diskuzí (15 minut)

Poslední aktivita uzavírá lekci, je vhodné ji propojit se školou, aby řešení tématu nebylo omezeno na prostředí knihovny. Při nedostatku času může proběhnout ve škole s diskuzí s učitelem místo lektora, vhodnější je ale uskutečnit ji v knihovně a do prostředí školy nechat jen další diskuzi nad výsledky.

Každá skupina po 3-4 dětech dostane jeden pracovní list (pracovní materiál *Když se mě někdo zeptá*). Společně do tabulky udělají šipky od každé otázky v prostředním sloupci ve směru podle toho, jestli danou informaci odmítnou sdělit, nebo ji poskytnou. Lektor by měl vybrat tři otázky pro demonstraci, že na většinu otázek lze odpovědět obecně (např. bydlím na Moravě), ale ne konkrétně (např. adresa). Oproti tomu některé otázky jsou jasně varující (např. Jsi doma sám/sama?).

Pro jednoduchou zpětnou vazbu děti při odchodu umisťují vylosovaná čísla a písmena k obrázkům usměvavého, neutrálního a mračícího se emotikonu, čímž vyjadřují svůj názor na lekci, a zda by chtěly přijít na navazující lekci.

5 otázek s dospělými

1. Jak se bavíte s jinými lidmi přes internet?
2. S kým se tak bavíte?

3. Co chcete, aby o vás hodně lidí vědělo (např. díky zdi na Facebooku)?

4. Jak jste se bavili přes internet s člověkem, kterého jste nikdy neviděli?

5. Když se vám ozve někdo známý s novým profilem (e-mailem, facebookovým profilem, Skype účtem atd.), jak zjistíte, že je to opravdu ten, kdo myslíte?

8.2.3 Sociální inženýrství a silná hesla

Žáci druhého stupně základní školy jsou již často uživateli mnoha služeb internetu, z nichž významnou část tvoří komunikace a služby vázané na osobní profil. S jejich užíváním jsou spojeny různé hrozby, se kterými se mohou setkat a jejichž důsledky mohou být silně negativní. Proto je vhodné vybudovat v nich pomocí lekce zdravou nedůvěru v identitu toho, s kým komunikují na internetu, především s ohledem sociální inženýrství a krádež identity. Pro uvědomění si těchto problémů je zařazena simulace problematické komunikace na internetu. Klíčovou roli v souvislosti s touto problematikou hrají autentizační údaje, především nejčastěji používané ve formě hesel. Žáci by měli dodržovat pravidla bezpečné práce se silnými hesly, která si zažijí pomocí aktivity v rámci této lekce.

Předpoklady a cíle lekce

Cílová skupina

- Žáci základní školy, 6. – 7. třída.
- Běžné uživatelské znalosti v tomto věku, vhodná je orientace v tématech předchozích lekcí.

Očekávané výstupy

- Zlepšení komunikačních a sociálních kompetencí (vlastní názor, prezentační dovednosti, práce ve skupině, naslouchání, sebereflexe).
- Rozpoznání obvyklých postupů krádeže identity a sociálního inženýrství v komunikaci na internetu v praxi.
- Pochopení významu autentizace a znalost různých způsobů autentizace v komunikaci na internetu.
- Uvědomění si významu hesla pro využívání elektronických služeb a znalost pravidel pro bezpečnou práci se silnými hesly.

- Formování postoje zdravé nedůvěry v komunikaci na internetu.

Materiální zajištění

- Dvě místnosti (ne vzdálené).
- Tabule v hlavní místnosti, tabule či prostor pro vyvěšení papíru v druhé místnosti, magnety, papíry a psací potřeby, stoly či podložky pro psaní, anglicko-české a česko-anglické slovníky.
- Lístky pro losování s pojmy označujícími vybrané hrozby v komunikaci na internetu (uvedeny v části evokace v osnově lekce).
- Pracovní listy: pracovní materiál *Tabulka pravosti identit* (pro polovinu žáků s čísly, pro polovinu s písmeny) a *Hesla* (pro každého žáka).

Zkušenosti lektora

Lektor by se měl orientovat v pojmech a vymezení hrozeb na internetu. Měl by být seznámen s výzkumy zaměřenými na používaná hesla na internetu, aby mohl obhájit obsah lekce před žáky. Vhodné je zkontrolovat funkčnost odkazovaných služeb těsně před lekcí (zejména v pracovním listu *Hesla*). Stejně jako v případě předchozí lekce je nutný vyvážený přístup ke sdílení informací, který by měl vést žáky k budování pozitivní digitální stopy a k uvážlivému chování na internetu s uvědomováním si důsledků vlastního chování a snadnosti realizace představených problémů. Vhodné je sledovat aktuální výzkumy v této oblasti, např. EU Kids Online nebo e-Bezpečí (viz kap. 11.5).

Aktivity se mohou zdát jednoduché a nedostatečné s ohledem na to, co vše by měl žáci znát, aby byli v bezpečí. S ohledem na časovou dotaci, záživnost a hlubší pochopení je ale vhodné zůstat na stanovené úrovni a předat sice pouze základy, ale kvalitně.

Pokud budou některé aktivity nahrazeny jinými, je nutné myslet na to, že i přes téma, které žáky zajímá, je lekce poměrně dlouhá a náročná na soustředění. Reflexe zaměřená na hesla je klíčová, autentizace představuje jádro bezpečného užívání elektronických služeb obecně. Je tedy vhodné věnovat jí dostatečný prostor, jak je popsáno výše. Informace jsou ale náročné na zpracování, proto je tato forma vhodná díky odlehčené předchozí aktivitě s pohybovou složkou.

Osnova lekce *Mnoholičný lektvar na internetu*

Týmové definování pojmů označujících hrozby na internetu (15 minut)

Pro zahájení lekce jsou žáci povzbuzeni, aby se podělili o to, co znají. V tomto případě se jedná spíše o ujasnění jejich limitů, protože většina pojmů pro ně bude nová. Touto evokační fází jsou žáci zaujati tím, že lektor jim ukáže slabiny ve znalostech internetu a nabídne jim možnost je zaplnit. S ohledem na obvyklé charakteristiky dospívajících v tomto věku sice nebudou projevovat nadšení jako mladší děti, internet ale chtějí znát, proto se do aktivit zapojí a nebudou projevovat tolik revoltu vůči autoritám, mezi které patří i knihovna, i když mnohem méně než škola.

Po zahájení lekce s představením jejího zaměření na hrozby komunikace na internetu jsou žáci vyzváni rozdělit se do skupin po 3-4 a následně vyslat zástupce pro vylosování jednoho z nabízených papírků přeložených pro skrytí nápisu při volbě. Každá skupina si tak vybere jeden z pojmů: krádež identity, kyberšikana, slovníkový útok, kybergrooming, hacking, kyberstalking, happy slapping, sexting, malware. Pojmy jsou řazeny podle významu pro lekci, do losování je zařazeno tolik pojmů, aby vyšel na každou skupinu jeden. Týmy mají 5 minut na vytvoření definice pojmu, lektor prochází mezi skupinami s anglicko-českým slovníkem, který poskytne skupině pro překlad na vyžádání. Skupiny nemusí znát pojem, ale libovolně mohou odvozovat definici o rozsahu jedné až dvou vět. Následně skupina přednese své vymezení pojmu, které lektor upřesní.

Po vyhodnocení týmových úkolů lektor upozorní na provázání pojmů, zejména uplatnění krádeže identity ve zmíněných hrozbách při komunikaci na internetu, a to s neznámými lidmi, ale i známými, za které se skrytím za monitor může vydávat někdo jiný. Pro simulaci, jak je jednoduché převzít cizí identitu a současně těžké odhalit tuto krádež, je určena následující hra.

Soutěž v odhalování pravosti či krádeže identity

35 minut:

- max. 5 minut vysvětlení pravidel
- 30 minut soutěž se simulací komunikace na internetu pro pochopení principů sociálního inženýrství a krádeže identity

Formát hry je podobný popsanému u lekce pro 4. a 5. třídu, proto zde bude vymezení stručnější. Losováním čísel a písmen, kterými se ve hře označují místo jmen, jsou opět vytvořeny dvě skupiny žáků, které se po vysvětlení pravidel rozdělí do dvou místností, mezi kterými lektor, ideálně s pomocí učitele, přenáší vzkazy žáků. Cílem je zjistit, zda komunikace je pravdivá (s reálnou identitou) či lživá (s ukradenou identitou), a současně zmást toho, s kým je komunikováno. Za každé správné odhalení cizí identity je získán bod, za každé odhalení vlastní ztracen bod.

Pravidla komunikace ve hře jsou viditelně napsána v obou místnostech. Žáci se po rozchodu postaví na vybranou stranu lektora, ten ukáže, ve které ruce měl červený lístek značící falešnou identitu a ve které zelený pro pravou identitu pro průběh celé aktivity. Pravé identity musí psát výhradně pravdu (výjimkou jsou soukromá tajemství), falešní se po celou dobu vydávají za jednoho člověka ze své skupiny, aby nebyli odhaleni už při představení se ukradenou identitou. Jména je možné používat, jen pro označení subjektů komunikace je nutné označení číslem a písmenem, první komunikace je nadepsaná podle stejného klíče jako u předchozí lekce. Opět je možné vést libovolný počet komunikací s podobnými riziky, totožný je i způsob komunikace, kdy je zapsána odpověď a následně položena otázka před odesláním zprávy zpět. Pokud si žák myslí, že poznal identitu druhého, opět použije formulku *už vím*, ale komunikace končí až při jejím zapsání oběma. Pro zaznamenání domnělé identity je použita podobná tabulka jako u předchozí lekce (viz pracovní materiál *Tabulka pravosti identit*). Pro zahájení děti dostanou příklady možných otázek, např. *Jak se jmenuješ? Jaký je tvůj oblíbený zpěvák? Jaký děláš sport?* Lektor opět radí při nejasnostech a zasahuje jen v podobných případech jako u předchozí lekce, opět hlídá čas a 5 minut před koncem dá výzvu k posledním otázkám.

Vyhodnocení soutěže s interaktivní přednáškou (15 minut)

Po ukončení hry se skupiny sejdou v jedné místnosti a vyhodnocení probíhá stejně jako u předchozí lekce. Následně lektor připodobní simulaci ve hře reálnému prostředí a upozorní tak žáky na to, co poznali v soutěži jako problém, a jak se mu mohou vyhnout.

Klíčovým problémem internetu pro komunikaci je snadnost krádeže identity či vytvoření a užívání falešné (pro lekci obě situace označovány

zjednodušeně krádež identity). Nikdo si nemůže být zcela jistý, že komunikuje opravdu s tím, s kým si myslí, pokud toho druhého nezná z fyzického prostředí a nekomunikuje s ním v reálném čase přes webkameru. Tak ale probíhá minimum komunikace přes internet.

Vodítko pro odhalení charakteristik či identity toho druhého nemůže dát ani forma komunikace. Mnoho jí totiž probíhá na internetu veřejně, proto není těžké zjistit si pro konkrétní skupinu uživatelů obvyklou formu i obsah komunikace a napodobit je. V případě krádeže identity může útočník paralelně navázat komunikaci i s tím, za koho se vydává, potom není problém se zeptat na informace, které potřebuje pro komunikaci se zamýšlenou obětí. Při závažnějších problémech, jako je např. grooming, často dochází k dlouhodobému budování důvěry a tzv. zrcadlení, kdy komunikující vyjadřuje stejné zájmy a názory jako ten druhý a tím vyvolává pocit *spřízněné duše*, tedy získává důvěru.

I v případě, že člověk přes internet komunikuje jen s těmi, které zná, nemůže si být jistý, že se nejedná jen o ukradené identity. Lektor vybídne k zamyšlení a vlastnímu vyhodnocení, jak by žák reagoval na popsané situace:

- Když se označím na Facebooku jako Justin Bieber, vyjadřuji se jako on a mám vytvořen profil s informacemi, které odpovídají této osobě, jak zjistíte, že lžu?
- Přišlo by vám divné, kdybych vám poslala zprávu z profilu podobného, jako má vaše kamarádka již zařazená mezi přátele s tím, že toto je nový profil, který jsem si zřídila, aby byl mimo kontrolu matky a že ten starý musím občas používat, aby nepoznala, že mám nějaký bez jejího dohledu, takže ani na ten starý nemůžete nic k novému napsat?
- Jste si zcela jistí, že někdo neuhádl nebo neprolomil heslo vašeho kamaráda k účtu, se kterým komunikujete? Nebo se jen nezapomněl odhlásit či nenechal uložené heslo na počítači, ke kterému má přístup i někdo jiný, třeba v knihovně? Potom byste mluvili s účtem, který máte prověřený, ale se zcela jinou osobou, než myslíte. Přitom tato osoba má přístup i k celé historii komunikace, takže o vás i vašem dorozumívání ví mnoho a dokáže to napodobit.
- Jste si jistí, že znáte dobře všechny vaše přátele na Facebooku a jejich přátele, kteří mají přístup k vašim informacím zveřejněným v této službě?

Reálnost popsaných scénářů je snadno představitelná. Jaké jsou možnosti řešení nebo alespoň omezení těchto situací? A nepřipomínají krádeže identity něco? Zde lektor odkazuje na předposlední a poslední díl série o Harrym Potterovi, kdy smrtijedi používali mnoholičný lektvar právě pro krádež identity, aby narušili odboj proti Voldemortovi. A opět otázka pro žáky: jak se Fénixův řád bránil? I na internetu je jednou z možností (mimo již uvedené ověření webkamerou) využít sdíleného tajemství. Zde je ale nutné pracovat s informací, kterou opravdu nezná nikdo jiný a obě strany ví, že ji nesmí prozrazovat dál, ani když se někdo zeptá a samozřejmě nelze nikde zveřejnit nic, co by ji prozradilo. Jedná se o autentizační údaj, podobně jako heslo. Dále jsou klíčová hesla, jak již naznačil jeden z výše popsaných scénářů. S ohledem na jejich klíčovou funkci je nutné nastavit heslo tak, aby bylo silné. K představení silného hesla slouží poslední fáze lekce.

Brainstorming pravidel pro silná hesla se simulací tvorby hesla (15 minut)

Hesla používají téměř všichni z cílové skupiny, které je určena tato lekce. Reflexe je proto zaměřena na konfrontaci reálně používaných a silných hesel. Metodou brainstormingu žáci společně vytvoří soubor pravidel pro tvorbu, formu a použití hesel, aby byla dostatečně bezpečná. Lektor nezasahuje, pouze zapisuje nápady a ukončí brainstorming, pokud již nepřináší nové myšlenky. Následně dá lektor každému žáku pracovní list *Hesla* a vyzve žáky, aby během tří minut vytvořili ve dvojici bezpečné heslo a zapamatovali si ho. Poté žáci svá hesla napíší. Dvojice se nedorozumívá, slouží pro kontrolu, že heslo je opravdu zapamatováno. Poté, co se všichni vyjádří k tomu, zda heslo splňuje stanovená pravidla, se k bezpečnosti vyjádří i lektor a upozorní na průměrnou rychlost prolomení dané formy podle pracovního listu. Následně lektor uvede možná řešení použití silného hesla bezpečně i k zapamatování:

- Správce hesel je obvykle zvláštní software, do kterého se uživatel přihlásí a program sám za něj doplní heslo pro příslušnou službu, takže nutné je zapamatovat si jen jediné silné heslo pro správce. Příklady programů jsou uvedeny na pracovním listě, takže žáci si je při zájmu mohou snadno najít.
- Několikaúrovňová politika hesel spočívá ve stanovení kategorií důležitosti služeb, které heslo chrání. Podle toho jsou pak hesla silná. Je ale nutné si uvědomit, že jednoduché heslo může být prolomeno, proto by mělo být

použito jen tam, kde uživateli nebude vadit, když dojde ke krádeži profilu, příp. identity přes něj.

- Algoritmus tvorby znamená, že postup je stále stejný, ale generuje vždy jiné a silné heslo. Např. věta „*Toto je moje heslo, které mám na Facebooku v lednu.*“ vytvoří heslo *Tjmh,kmnFv1.* – je použito vždy první písmeno z každého slova, ponechána čárka a tečka ve větě, leden jako první měsíc je nahrazen číslicí 1. Tuto větu lze použít i pro další služby, kdy Facebook je nahrazen jejím názvem, heslo tedy bude odlišné a přitom postup stejný.

Kromě toho lektor upozorní i na služby pro kontrolu bezpečnosti hesla, které jsou opět uvedeny na pracovním listě. Služby jsou jednoduché, ale mění se, proto je dobré se s nimi před lekcí seznámit a stručně je následně představit a doporučit k vyzkoušení. Na závěr jsou žáci opět vyzváni k vytvoření bezpečného hesla, jehož kvalitu si v některé z právě uvedených služeb ověří.

5 otázek s dospělými

1. Jak jste se bavili přes internet s člověkem, kterého jste nikdy neviděli?

2. Když se vám ozve někdo známý s novým profilem (e-mailem, facebookovým profilem, Skype účtem atd.), jak zjistíte, že je to opravdu ten, kdo myslíte?

3. Jak si vytváříte heslo a kde se snažíte, aby bylo co nejbezpečnější?

4. Když s někým komunikujete přes internet, jak si ověřujete, jestli říká pravdu?

5. Dokážete popsat alespoň tři situace, ke kterým by mohlo dojít při komunikaci s člověkem, který chce zneužít internet proti vám?

8.2.4 Typy internetových hrozeb pro dospívající

Žáci blížící se konci základní školní docházky již mají i díky rámcovým vzdělávacím programům jisté seznámení se s možnostmi internetu. Dospívající v tomto věku bývají častými uživateli internetu, mají povědomí o hrozbách s ním spojenými, ne výjimečně, ale na obecné bázi, bez představy o tom, jak by mohla daná situace zasáhnout i je. Pomocí čtení s předvídáním založeného na reálných situacích je žákům zprostředkován právě takový pohled na problematiku. S ohledem na rozšířenost sociální sítě Facebook a možnost jejího zapojení do

ohrožení žáků je v závěrečné fázi lekce pozornost zaměřena na možnosti, které v současnosti Facebook umožňuje v nastavení soukromí jeho uživatelů.

Předpoklady a cíle lekce

Cílová skupina

- Žáci 8. – 9. třídy základní školy.
- Běžné uživatelské znalosti internetu v tomto věku, vhodná je orientace v základech bezpečné komunikace (v rozsahu předchozích lekcí).

Očekávané výstupy

- Zlepšení komunikačních a sociálních kompetencí (vlastní názor, prezentační dovednosti, práce ve skupině, naslouchání, sebereflexe).
- Rozpoznání obvyklých postupů nejčastějších hrozeb v komunikaci přes internet a znalost bezpečnostních opatření proti nim.
- Formování postoje zdravé nedůvěry v komunikaci na internetu.
- Znalost možností nastavení soukromí na sociální síti Facebook a přehled o možných důsledcích jejich využití či nevyužití.

Materiální zajištění

- Psací potřeby, stoly či podložky pro psaní.
- Texty pro čtení s předvídáním (úprava popsána v osnově), pro každého žáka jedna varianta, varianty rovnoměrně využity (podle počtu žáků).
- Pracovní listy: pracovní materiál *Diamant* a *Tabulka pro předvídání* pro každého žáka, materiál *Registrace na Facebook* (pro skupiny 3-4 žáků).
- Učebna s projektorem připojeným k počítači s internetem (lze vynechat).

Zkušenosti lektora

Lektor by se měl orientovat v pojmech a vymezeních hrozeb na internetu. Dále by měl být seznámen s výzkumy zaměřenými na používaná hesla na internetu, aby mohl obhájit obsah lekce před žáky. Lekce je náročnější na znalosti lektora, měl by znát kazuistiky v řešené oblasti a také by měl mít přehled o bezpečnostních opatřeních a důvodech jejich aplikace. Stejně jako u předchozí lekce je nutný vyvážený přístup ke sdílení informací, který by měl vést žáky k budování pozitivní

digitální stopy a k uvážlivému chování na internetu s uvědomováním si důsledků jednání a snadnosti realizace představených problémů. Vhodné je sledovat aktuální výzkumy, např. EU Kids Online nebo e-Bezpečí (viz kap. 11.5).

Popsané doporučení odpovídá i zkušenosti Aleny Srovnalové (Městská knihovna Rožnov pod Radhoštěm, e-mailová komunikace ze dne 18. 6. 2014), kdy žáci vyjadřovali již dostatečné znalosti obecných informací, ale právě doplnění výzkumnými zjištěními a především kazuistikami z českého prostředí přidávalo obsahu na zajímavosti, pro čtení s předvídáním byla upravena tabulka pro snazší vyplnění, pomalí čtenáři četli text bez vyplňování. Metodu diamant bylo někdy problém zahájit, osvědčilo se navést žáky k pozitivním slovesům (3. řádek). Osvědčilo se i video s diskuzí mezi diamantem a čtením, konkrétně *Hnusná držka* (dostupné na YouTube) bez komentářů odborníků. Reflexe byla realizována metodou *poslední slovo patří mně*. Lekce byla hodnocena pozitivně, především pedagogy, podle kterých lekci děti hodnotily a diskutovaly o ní i v následujících dnech, což lze interpretovat splněním cíle v zamyšlení nad řešenými problémy.

Aktivity se mohou zdát příliš jednoduché a nedostatečné s ohledem na to, co vše by měly děti znát, aby byly v bezpečí. S ohledem na časovou dotaci, záživnost a hlubší pochopení je ale vhodné zůstat na stanovené úrovni a předat sice základy, ale kvalitně.

Diamant byl testován na žácích na konci 6. a 7. třídy. Synonymum pro ně byl nejčastěji Facebook, což je dobrým můstkem ke čtení s předvídáním, kde v některých příbězích je Facebook uveden, jinde si lze jeho roli snadno představit.

Osnova lekce *Detektivky na Facebooku*

Diamant pro pozitiva a negativa internetu (15 minut)

V tomto věku je již nepochybné, že všichni žáci na lekci mají poměrně rozsáhlé, i když často jen dílčí zkušenosti s internetem a mají o něm vytvořenou jasnou představu. Současně již není nutné je tolik přesvědčovat o smyslu tématu a uklidňovat jejich sklony k revoltě vůči autoritě v podobě knihovníka. Ten by měl vystupovat v roli partnera a průvodce, nikoliv nezpochybnitelné autority. Pro evokační fázi je tedy možné zařadit diamant na téma internet, kdy si žáci sami uvědomí, nakolik těžké je přemýšlet nad tímto nástrojem nejen ve smyslu využití,

ale i zneužití, kterého si jsou často vědomi na obecné úrovni, ale jen špatně si ho přiřazují ke své osobě.

S pomocí diamantu jsou žáci vedeni k tomu, aby vytvořili na daný počet slov pozitivní i negativní charakteristiky určitého typu (viz pracovní materiál *Diamant*). Obrazec vytváří jednotlivci samostatně, kdy postupují od nejkratších polí střídavě nahoře a dole směrem do středu, čímž se jim spojují pozitiva a negativa na stejných úrovních. Současně by si měli uvědomit, nakolik je pro ně těžké či lehké daný řádek vyplnit. Vyplnění by nemělo přesáhnout 7 minut, po 5. minutě lektor upozorní na blížící se konec. Následně nejdříve přečte vlastní vyplněný diamant a vyzve žáky, aby se také podělili o to, co vytvořili. Pokud žáci nereagují, postupuje se stejně jako při vyplňování, ale žáci nahlas říkají různé varianty pro daná pole.

Lektor by měl diamanty sledovat a najít v nich pojítko na další aktivitu. Obecně lze vždy přejít přes to, že negativa si tolik neuvědomujeme, přestože se s nimi může setkat každý při použití služeb, které jsou s identitami často spojeny, např. pro komunikaci s blízkými lidmi. A právě k problémům, které zahájila komunikace na internetu, se váže aktivita ve fázi uvědomění.

Volitelné uvedení čtení s předvídáním videem Cyber Bullying (10 minut)

Pokud je k dispozici místo, na které lze promítat video z internetu, je vhodné navázat fázi uvědomění videem Let's Fight It Together (dostupné z YouTube), které natočila organizace Childnet International pro ilustraci postupu a možných důsledků kyberšikany. Video je sice v angličtině, mluví se v něm ale minimálně. Přesto je vhodné po zhlédnutí vyzdvihnout základní poznatky o kyberšikaně:

- Začíná obvykle nevinným pošťuchováním, ale graduje do neúnosnosti.
- Terčem se může stát i dříve poměrně oblíbený žák.
- Jsou využívány nejrůznější způsoby komunikace, pomocí kterých je oběť zesměšňována, napadána apod.
- Problém může zahnat oběť na hranici sil, pak jsou i řešení extrémní, v případě videa to bylo zapojení policie, která přišla pro šikanující dívky.

Při zařazení části s videem je nutné myslet na časovou náročnost, i při rychlém komentáři aktivita vyžaduje min. 10 minut. Její použití ale může urychlit fázi vysvětlení pravidel, protože je využito pro ilustraci práce s příběhem.

Čtení s předvídáním k hrozbám komunikace na internetu, přednáška s pokročilejšími doporučeními pro bezpečnou komunikaci

35 minut:

- max. 5 minut vysvětlení pravidel
- 10 minut čtení s předvídáním
- 5 minut shrnutí obsahu ve skupině
- 15 minut závěrečná prezentace příběhů s komentářem lektora

Čtení s předvídáním je založeno na příběhu, který se skládá z více částí, mezi kterými jsou zlomy, kdy se příběh může vyvíjet různým způsobem. Tyto části příběhu jsou odděleny i v materiální podobě, kdy ve zlomech je příběh rozstříhán a jeho části jsou sešity k sobě, takže není možné skákat na další pasáž, pokud se neotočí papír. Žáci si samostatně čtou vždy jednu část příběhu a před otočením na další vyplní jeden řádek tabulky (viz pracovní materiál *Tabulka pro předvídání*). Shrnují, co přečetli a odhadují, jak se bude příběh vyvíjet dál. Poté, co příběh dočtou, se sejdou ve skupinách podle témat a shrnou obsah příběhu. Následně skupiny prezentují svůj příběh, kdy každý ze skupiny řekne jednu větu. Žáci se tak seznámí se všemi příběhy, přitom u každého je aktivita stavěna pro rozvíjejí schopnosti naslouchání i komunikace.

V materiálu *Čtení s předvídáním* je připraveno pět příběhů, každý k jinému tématu, ale všechny spojeny tím, že jsou založeny na hrozbách komunikace na internetu. Příběhy lze libovolně obměňovat, je ale vhodná právě tematická šíře a odkaz na skutečné příběhy. Právě skutečnost by měla být přiblížena žákům po shrnutí obsahu v rámci závěrečné prezentace skupin. Reálný průběh a důsledky konkrétního případu by měly být obohaceny o nejobvyklejší průběh, v tomto věku žáků doplněný i občasným podložením výsledků výzkumů. Důležité je upozornit žáky na prevenci těchto problémů, především v důsledné ochraně soukromí a zdravé nedůvěře v komunikaci s čistě internetovými známými. Pokud žáci dobře reagují, lze návrhy pro preventivní i represivní opatření nechat na jejich brainstormingu.

Simulace registrace a nastavení v sociální síti Facebook s důrazem na vhodnost z hlediska zvýšení soukromí (20 minut)

Z příběhů je patrné, jak silné postavení může mít Facebook nejen pro komunikaci žáků s jejich přáteli, ale také pro hrozby komunikace. Jedním ze základních bezpečnostních opatření je vhodné nastavení soukromí. Facebook umožňuje upravit dostupnost množství informací o uživateli, často se ale stává, že těchto možností není využito. Může se jednat o pohodlnost, ale také neznalost. V obou případech může pomoci reflexní aktivita lekce, která ukáže žákům, jaké možnosti nastavení soukromí Facebook v současnosti umožňuje. I pokud by jich nevyužili, jedná se čistě o jejich rozhodnutí, klíčové je, že si jsou možností vědomi. S ohledem na předchozí aktivitu by si to měli uvědomit ve chvíli, kdy jsou seznámeni s možnými důsledky benevolentního přístupu k soukromí na internetu.

V rámci aktivity si žáci ve skupinách po třech až čtyřek projdou formulář registrace a nastavení soukromí (viz pracovní materiál *Registrace na Facebook*) a vyplní jej pro fiktivní osobu. Podle pokynů by měly být využity možnosti tak, jak by oni poradili svému kamarádovi, aby byl v bezpečí, ale mohl službu dobře využívat. Po 10 minutách lektor vyzve žáky, aby společně prošli jednotlivá pole a možnosti. V případě, že některá skupina bude mít odlišnou reakci nebo jmenované nebudou vhodné, lektor doplní komentář k možným důsledkům jednotlivých variant.

5 otázek s dospělými

1. Když s někým komunikujete přes internet, jak si ověřujete, jestli říká pravdu?
2. Dokážete popsat alespoň tři situace, ke kterým by mohlo dojít při komunikaci s člověkem, který chce zneužít internet proti vám?
3. Slyšeli jste o někom, komu byly zneužity jeho osobní informace zveřejněné na internetu nebo komunikované s internetovým známým?
4. Co děláte pro to, aby se něco podobného nestalo vám?
5. Jak si nastavujete různé internetové služby pro ochranu svého soukromí?

9 Akční výzkum lekce pro 4. - 5. třídu

Pro ověření efektivity navržené metodiky a její zkvalitnění reflektováním názorů osob, kterým je primárně či sekundárně určena, byl zvolen akční výzkum, jehož postup i výsledek odpovídá právě stanovenému výzkumnému cíli. Akční výzkum nepředstavuje výzkumnou metodu, ale spíše přístup, v rámci kterého nacházejí uplatnění nové i tradiční metody sběru a vyhodnocení výzkumných dat, často ve spojení pro triangulaci metod.

Akční výzkum má původ ve 40. letech 20. století, kdy je spojen především s Kurtem Lewinem. Od té doby prošel těžkým vývojem, ovlivněným především kritikami kvůli přílišnému spojení s praxí. Historii akčního výzkumu, stejně jako filozofické základy a směry, které ho ovlivňovaly, podrobně popisují Chevalier a Buckles[396] a dostávají se až k současným aplikacím tohoto přístupu pro doložení uplatnitelnosti a výsledků v oborech, kde si akční výzkum prosadil své místo: organizace, psychologie, zdraví, gramotnost, vzdělání, pracoviště, komunitní rozvoj, zemědělské systémy, meziproduktové technologie, environmentální studia a zapojení veřejnosti (např. v politické sféře). Uplatnění zmiňují i v knihovnách, ale příliš jej nerozvádí, protože se nejedná o prostředí, ve kterém by autoři měli více praktických zkušeností. Uplatnitelnosti akčního výzkumu v knihovnách se ale výrazněji věnuje např. Civallero[397], který ho vidí jako paralelní proces pro knihovnictví založené na důkazu, který je stále silněji diskutován jako potřebný. S tím se shoduje i Pickard, která uvádí, že „*akční výzkum se rychle stává jednou z nejpopulárnějších výzkumných metod v informačním a komunikačním výzkumu mezi lidmi v praxi.*“[398]

Formování akčního výzkumu a vliv filozofických směrů vedly k tomu, že v současnosti je možné identifikovat několik různých přístupů v akčním výzkumu, např. experimentální akční výzkum, induktivní akční výzkum, participační akční výzkum, participační akční výzkumná praxe a dekonstrukční akční výzkum. To vede i k různým definicím. V této dizertační práci je preferován induktivní akční výzkum, kdy je nejdříve identifikován pozorováním problém, po kterém následuje akce a reflexe. Tomuto přístupu stále odpovídá definice Lewina: „*Představuje*

[396] CHEVALIER 2013
[397] CIVALLERO 2007
[398] PICKARD 2013, s. 157

flexibilní, vědecký přístup k plánované změně, která postupuje přes spirálu kroků, z nichž každý se skládá z cyklu plánování, akce a zjišťování faktů o výsledcích akce."[399] Jedná se o spirálovitý proces, který nikdy nekončí, každá výzkumná fáze je následována akcí a evaluací, změna se pak promítá do odlišných výsledků nového cyklu výzkumu, které vedou k novým akcím a evaluacím. I přesto je možné výsledky akčního výzkumu hodnotit, pokud se ukáže efektivita (v tomto případě vzdělávací) akce a její přijatelnost pro všechny dotčené cílové skupiny.

Akční výzkum je ve vzdělávání používán pro profesní vzdělávání učitelů, zkvalitňování kurikula nebo třeba pro zlepšování edukační praxe[400]. Protože cílem je změna praxe v komunitě[401], je nutné, aby komunita přijala výzkumníka i výzkum, je tedy nevyhnutelné zapojení (ne akademický odstup) při řešení výzkumu, při vyhodnocování výzkumu je nutné toto zapojení zohlednit a usilovat o co nejvyšší objektivitu a současně reálnost (ideálně ověřením správnosti pochopení zjištění u zkoumané komunity). Rozdíl přirozeného vývoje a akčního výzkumu je právě v striktním dodržení pravidel výzkumu.

K základním charakteristikám akčního výzkumu patří úzké spojení s praxí, s tím souvisí i typické využití kvalitativního výzkumu[402], proto nelze výsledky zobecňovat, popisuje jen zkoumaný vzorek. Protože k požadavkům na akční výzkum patří publikování výsledků[403], musí být tyto dobře popsány i se specifiky prostředí, kde byl výzkum realizován, aby si následovníci, kteří jej budou chtít aplikovat ve vlastní praxi, mohli zvážit míru společných a odlišných charakteristik a tím také míru přenositelnosti do vlastního prostředí. Z toho důvodu jsou dále podrobně popsány různé vstupy do výzkumu. Další kritéria hodnocení kvality realizovaného akčního výzkumu jsou popsána v jeho závěru.

Prezentovaný akční výzkum představuje explorativní případovou studii. Byl realizován pro přispění k řešení praktických problémů a k ukázce možné změny zahrnutím knihoven do vzdělávání o internetové bezpečnosti v praxi. Cílem výzkumu bylo ukázat specifický přístup ke vzdělávání o bezpečnosti digitálních

[399] LEWIN, K. Resolving Social Conflicts; Selected Papers on Group Dynamics. In: CHEVALIER 2013, s. 11
[400] PICKARD 2013, s. 157-158
[401] HENDL 2008, s. 136
[402] HENDL 2008, s. 136
[403] ZUBER-SKERRITT 2007, s. 415

stop s použitím metod neformálního vzdělávání a aktivního učení s minimem materiálních požadavků a ukázat akceptaci všemi klíčovými osobami. V lekci si děti pomocí aktivního učení samy vytvoří nové poznatky o rizikových formách komunikace, problematických informacích ve formě digitálních stop a možnostech vyhnout se jejich vytváření při komunikaci přes internet, lektorka působí jen jako průvodce dětí aktivitami a upozornění na tyto poznatky.

Výzkumné metody a výsledky jsou popsány chronologicky podle nasazení i logické návaznosti. Vzhledem k cíli lekce byl pro hodnocení efektivity zvolen Kirkpatrickův čtyřúrovňový model[404], který umožňuje sledovat krátkodobý i dlouhodobý vliv, jak z hlediska dojmu z lekce, tak zlepšení znalostí a dovedností.

Nejdříve je pozornost zaměřena na zúčastněné pozorování, v jehož rámci je popsán kompletní průběh lekce pro akční výzkum. Součástí popisu je výsledek jednoduché zpětné vazby od žáků na to, jak se jim lekce líbila, pomocí tzv. smile-sheetů. Tento postup a částečně i zúčastněné pozorování ukazují výsledek na první úrovni Kirkpatrickova modelu, který slouží ke zjištění aktuální reakce na lekci (spokojenost s prostředím, lektorem apod.). Pozorování ale spíše zjišťuje druhou úroveň, tedy studijní výsledky, v tomto směru na ně navazuje dokumentová analýza materiálů vytvořených v rámci fáze uvědomění při lekci. Dokumentová analýza měla za cíl ověřit nejen to, jestli v průběhu aktivity dochází ke změně přístupu k zanechávání digitálních stop, ale také jestli žáci vychází ze zkušeností s obdobnou situací v praktickém použití internetu. S odstupem několika týdnů až měsíců po lekci byly uskutečněny rozhovory, jejichž dílčím cílem bylo zhodnocení dlouhodobého vlivu lekce na chování vzdělávaných, což představuje třetí úroveň Kirkpatrickova modelu. Čtvrtá úroveň modelu je určena k hodnocení přínosů lekce pro okolí (např. při dalším vzdělávání ve firmách), vzhledem k typu hodnocené lekce tato úroveň jako jediná nebyla sledována, jen částečně byla pokryta rozhovory (viz kap. 9.4). Protože se jedná o jeden výzkum, samozřejmě je nezbytné výsledky všech úrovní a metod (všechny použité uvádí Pickard[405] mezi základními pro akční výzkum) propojit a na základě zjištění všech zhodnotit efektivitu navržené lekce. Tento komplexní závěr spojující výsledky výzkumů s navrhovanou koncepcí je rozebrán v kap. 9.6.

[404] KIRKPATRICK 1996
[405] PICKARD 2013, s. 165

V rámci celého šetření byla uvažována etika výzkumu, která je v tom akčním složitější kvůli úzkému spojení s konkrétní praxí, kdy je problematická především anonymita výzkumu. Protože ale bylo do šetření zahrnuto celkem osm tříd v jedné škole, jsou subjekty vzdělávání neidentifikovatelné. Současně měli všichni možnost neúčastnit se lekce, příp. se jí účastnit, ale svým chováním neposkytnout data (pro pozorování mluvení tiše, pro dokumentovou analýzu odnesením svých dokumentů), čehož ale využilo jen několik jednotlivců. Není přesně možné říci, kolik z nich odneslo dokumenty, řád je odvozen podle přítomnosti a nepřítomnosti pseudonymů v dokumentové analýze, v případě pozorování jsou jednotky popsány. V případě vzniku audiozáznamů byli o tomto žáci, jejich rodiče i učitelé dopředu informováni prostřednictvím školy a byl od nich získán souhlas, pokud se jej nepodařilo pro třídu získat, byla data z pozorování zaznamenávána jen pomocí terénních deníků. V rámci rozhovorů bylo s ohledem na nemožnost anonymizace zvoleno neanonymní řešení, se kterým všichni dotázaní souhlasili udělením poučeného souhlasu (viz příloha 3).

9.1 Prostředí výzkumu

Městská knihovna v Poličce byla vybrána jako prostředí výzkumu díky zájmu knihovníků o internetovou bezpečnost[406]. Jednalo se o účelový výběr s využitím extrémního případu, vzhledem k nastavení akčního výzkumu jej totiž není možné realizovat, kde o něj není zájem nebo mezi autorem výzkumu a jeho subjekty není důvěra a společný cíl. Výběr eliminoval problémy s nezájmem knihovny či školy se zachováním reálného (ne laboratorního) prostředí. Smyslem šetření bylo ověřit účinnost navržené lekce s důrazem na uplatnění aktivního učení (viz kap. 8.1.2). Tato první případová studie může sloužit ukázka, jak pozitivní mohou být výsledky zapojení knihovny do vzdělávání o internetové bezpečnosti s aplikací prvků aktivního, neformálního učení a jak pozitivní může být jeho hodnocení různými zúčastněnými stranami. Omezení závěrů případové studie by

[406] Jak již bylo uvedeno u vymezení akčního výzkumu, zájem cílové skupiny o změnu je podstatným předpokladem pro provedení akčního výzkumu, viz např. PICKARD 2013, s. 163

v budoucnu mělo být redukováno aplikací lekce v odlišných prostředích a realizovaných jinými lektory, což ale není součástí této dizertační práce.

Polička je město s asi 9000 obyvateli a dvěma základními školami. Knihovna zprostředkovala kontakt s jednou z nich – Masarykovou základní školou. Tato škola vzdělává žáky z města a blízkých vesnic. Učitelé z obou stupňů školy jsou již několik let zvyklí navštěvovat s třídami lekce v knihovně, a to pravidelně, každoročně. Dosud však měli zkušenost spíše s lekcemi zaměřenými na práci s textem, a to v tradiční i elektronické podobě. Právě v druhém případě se lekce zaměřená na hodnocení informací (2. a 3. třída) často dotýkala problémů internetové komunikace. I z toho důvodu knihovnice pociťovala zájem více téma rozvinout v samostatné lekci. Spolu s ředitelem knihovny proto iniciovali vstup knihovny do případové studie, která je předmětem tohoto šetření.

Po domluvě spolupráce mezi výzkumnicí a knihovnou došlo přes zástupkyni ředitele pro 1. stupeň k zahájení vzdělávací činnosti o internetové bezpečnosti. Knihovnice a zástupkyně školy představují pro výzkum tzv. gatekeepers[407]. Od počátku byl plánován koncepční přístup, kdy budou vzděláváni žáci všech ročníků od poloviny 1. stupně po ukončení základní školní docházky, vždy jednou za rok v tématu internetové bezpečnosti.

Lekcím předcházel kontakt s vyučujícími na 1. stupni, protože ty (v návaznosti na pozitivní přístup zástupkyně) rozhodují, zda se se svou třídou lekce zúčastní a propojí ji se svou působností při formálním vzdělávání. Cílem setkání tedy bylo vybudovat si pozitivní vztah s touto skupinou zahrnutou do akčního výzkumu. Byla diskutována významnost problematiky internetové bezpečnosti a zvláště digitálních stop a také omezené znalosti pedagogů v této oblasti. Obě oblasti měly být zvýšeny spoluprací s knihovnou, a to vzdělávacími lekcemi pro děti v rámci akčního výzkumu, ale také lekcí pro učitele souběžně s prvními cykly pro děti. Seminář pro učitele měl za cíl snížit jejich obavu z jednání s dětmi o řešené problematice. Zájem učitelů o téma byl překvapivě pozitivní, a to při jejich vlastním vzdělávání i ochotě zúčastnit se lekce se svou třídou.

Šetření probíhalo v letech 2013 a 2014, přičemž druhý rok potvrdil saturaci vzorku a možnost uzavřít akční výzkum v této fázi, protože zúčastněné pozorování nepřinášelo nové výsledky, přestože kolektivy tříd byly velmi odlišné a poslední

[407] PELIKÁN 2011, s. 234

lekci realizovala knihovnice, výzkumnice byla přítomna v roli pozorovatele a pomocníka. Na přelomu let 2013 a 2014 došlo ke změně osoby v pozici knihovnice – lektorky, zkušenosti druhé knihovnice se vzděláváním byly omezené, ale lekce proběhla bez výraznějších odchylek, což potvrzuje její přenositelnost. V létě 2013 došlo ke změně pozic i ve spolupracující škole, kde se zástupkyně ředitele pro 1. stupeň (jeden z gatekeeperů) stala ředitelkou školy a učitelka nejsilněji spojená s výzkumem zařazením do rozhovorů ji vystřídala na původním místě. Ke změně došlo přibližně v době rozhovorů, které je tím možné hodnotit více jako reprezentující spolupracující instituci.

Aby se ověřil přístup k formě, obsahu i názorům všech zúčastněných na tuto spolupráci, byla v prvním roce (duben a květen 2013) realizována jen s 1. stupněm lekcí pro všechny 4. a 5. třídy, což představuje 113 žáků rozdělených do pěti tříd. Ročníky odpovídají době, kdy dochází k silné změně využití internetu v příklonu od her ke komunikaci[408]. Po každé lekci byl diskutován její průběh (fáze akce) s knihovnicí zkušenou ve vzdělávání a byly formulovány požadavky na úpravy v návaznosti na pozorované reakce dětí a stručný komentář učitelky po lekci, tyto úpravy byly zavedeny v následujícím běhu. V souladu s postupem akčního výzkumu došlo i k druhému cyklu v roce 2014, vzhledem k nemožnosti opakovat stejnou lekci s bývalou 4. a nově 5. třídou proběhl druhý cyklus jen se všemi třemi 4. třídami školy, zúčastnilo se celkem 61 dětí. Termíny realizace lekcí, počet žáků v nich a zastoupení pohlaví (49,43 % chlapců a 50,57 % dívek) byly:

- 9. dubna 2013: 4.A s 23 žáky (11 chlapců a 12 dívek),
- 9. dubna 2013: 4.B s 22 žáky (12 chlapců a 10 dívek),
- 23. dubna 2013: 5.A s 24 žáky (14 chlapců a 10 dívek),
- 23. dubna 2013: 5.B, s 23 žáky (10 chlapců a 13 dívek),
- 21. května 2013: 5.C s 21 žáky (9 chlapců a 12 dívek),
- 6. května 2014: 4.A s 20 žáky (7 chlapců a 13 dívek),
- 6. května 2014: 4.B s 23 žáky (13 chlapců a 10 dívek),
- 27. května 2014: 4.C s 18 žáky (10 chlapců a 8 dívek).

[408] FINDAHL 2009

V rámci ročních cyklů docházelo k menším etapám v podobě lekcí, protože po každé lekci došlo ke zhodnocení a úpravě na základě zapojování žáků. V rámci dokumentové analýzy došlo k rozšíření souboru dat pro zkvalitnění statistických výsledků, rozhovory již také opakovány nebyly, pouze byly stručně doplněny během kontaktu pro autorizaci přepisů.

9.2 Zúčastněné pozorování lekce

Vzhledem k charakteristikám akčního výzkumu je zúčastněné pozorování často aplikovanou metodou při tomto přístupu. Jeho prostřednictvím dochází ke sledování efektivity zvoleného přístupu a na základě vyhodnocení stavu k úpravám vzdělávacího nástroje. K této výzkumné metodě patří omezená možnost zaznamenání veškerých podnětů, zejména při paralelním výskytu. Proto nebylo v souladu s doporučeními[409] pozorování jedinou aplikovanou metodou hodnocení. Pro triangulaci dat byla spojena zjištění pozorování s výsledky rozhovorů a dokumentové analýzy. Právě dokumentová analýza umožnila vycházet nejen z toho, co bylo žáky řečeno a uděláno, ale také napsáno. Tato klíčová část lekce by zůstala při samotném pozorování skrytá.

Cílem pozorování bylo především ověřit reakce žáků na zvolené metody a současně efektivitu lekce spočívající ve změně reakcí na podněty. Proto byl zaznamenáván a vyhodnocen průběh lekce a reakce žáků vzhledem k využitým vzdělávacím aktivitám.

9.2.1 Metodologie šetření

Kvalitativní výzkum byl realizován lekcí vytvořenou pro tento účel (viz kap. 8.2.2), protože existující lekce jsou určeny primárně pro použití na školách. Proti tomu byl důraz kladen na ukázku možností neformálního vzdělávání založeného na akčním učení, kde učení neprobíhá pouze poslechem nebo mluvením o tématu, ale hlavně vlastní aktivitou, děláním určitých činností, které mohou představovat simulaci reálné komunikace přes internet. Realizace lekce byla

[409] Např. PELIKÁN 2011, s. 209-210

podrobena zúčastněnému pozorování. Jeho cílem bylo potvrzení akceptace neformálního přístupu k učení o digitálních stopách žáky a učiteli. Proto bylo sledováno především to, jak žáci reagují na postupy neformálního vzdělávání i konkrétních typů aktivit a jejich přijetí simulace reálné online komunikace.

Lekce byla vytvořena s výukového rámce E-U-R (evokace, uvědomění a reflexe) pro podporu aktivního učení. Bylo nezbytné založit lekci na znalostech a zkušenostech žáků (fáze evokace), proto jejich zapojení bylo primárním ukazatelem, zda je lekce vhodně postavená. Vzhledem k tomu, že akční výzkum má cyklický průběh a na základě zjištění dochází k úpravám přístupu pro dosažení žádoucího cíle, i v tomto případě byly sledovány především reakce žáků a zda, příp. jak dochází k naplnění cíle lekce. Ten spočívá v tom, že si děti samy, aniž by jim to někdo řekl, uvědomí, při poskytnutí jakých informací je jejich komunikace riziková (fáze uvědomění). To by mělo být přeneseno po lekci do jejich reálné internetové komunikace, kdy se před poskytnutím či zveřejněním osobní informace zastaví a zamyslí se, jaký bude vhodný postup podle toho, jaký byl důsledek jejich reakce v podobné situaci během simulace. Ten si v lekci žáci vyzkouší ve fázi reflexe, jejímž smyslem je ukotvení poznání z předchozí aktivity.

Zásadním výsledkem zúčastněného pozorování tedy bylo ověřit, že děti reagují na aktivity uvedeným způsobem, a to nejen na úrovni znalostí, ale také formou reakcí na postupy aktivního, neformálního vzdělávání. Pokud tomu tak nebylo, v rámci cyklu akčního výzkumu došlo k úpravě lekce a jejímu opakování pro ověření nově nastavených činností. Jejich zaujetí lekcí, která sice byla o internetu, ale nepracovala nejen s ním, ale také s žádným zařízením, které jej může využívat, bylo sledováno a na závěr přímo ověřeno pomocí rychlé zpětné vazby od žáků i učitelek pomocí tzv. smile-sheetů.

Vedle záznamů výsledku zpětné vazby bylo pozorování vyhodnocováno na základě otevřeného kódování terénních poznámek a audiozáznamů lekce. Záznam byl pořízen kamerou snímající přednášející s žáky mimo záběr kamery, při samostatných aktivitách byla otočena, aby nedošlo k záběru žáků. Videokamera sice z počátku vzbudila zájem žáků, její vliv na výslednou lekci ale pravděpodobně nebyl významný s ohledem na rychlý návrat žáků k původnímu způsobu chování a spontánnosti projevů po dočasné změně způsobené zpozorováním záznamového zařízení. Snaha omezit vliv výzkumu na chování subjektů lekce byla také důvodem,

že o probíhajícím výzkumu věděly učitelky, ale žáci měli informaci jen o nezvyklé lektorce, která lekci realizuje v rámci své práce na univerzitě. Vliv změny učitele bude patrný i při běžném nasazení lekce v knihovnách, kdy lekci nevede učitelka, ale knihovnice, tedy osoba, která děti vzdělává výjimečně, čímž je omezen tzv. Hawthornský efekt[410]. Pomocí záznamových technik byly vyhodnocovány kvalitativně výskyty sledovaných jevů, jejich řádová četnost (na úrovni jednotlivce, skupiny jednotlivců a všech přítomných) a okamžik výskytu[411].

V záznamových arších došlo k členění sledovaných jevů do 12 segmentů. Základní kategorie segmentů sloužila k popisu aktivizačního vlivu lekce u žáků:

1. Formální otázka či kontakt

   Do tohoto segmentu patří navazování kontaktu se skupinou či jednotlivci, výzvy k aktivitě bez nového poznatku či informace. „*Napadá vás ještě něco?*“, „*Co si o tom myslíte?*“

2. Aktivní projev bez přímé výzvy

   Tímto segmentem byly označovány vzájemné reakce žáků, bez opakované iniciace aktivity lektorkou.

3. Rada, pomoc studentovi

   Tento segment je blízký přímému stanovení aktivity žáka z omezení aktivního přístupu, v tomto případě ale nedochází k návodnému přesnému pokynu, ale k podnětu, jak přemýšlet nad danou aktivitou.

4. Motivování, podpora k dalšímu aktivnímu přístupu

   „*To je velmi pěkná otázka (odpověď).*“, „*Znáte toho víc, než jsem čekala.*“

5. Přenos zkušenosti z použití internetu do lekce

   Jedná se o komentáře žáků, kdy tlumočí vlastní zkušenost, nejen zprostředkovanou. Patří sem otázky na lektorku, jak řešit situace ve vztahu k tématům v lekci.

6. Vzájemné hodnocení

   Vzájemné hodnocení žáků spolužáky formou diskuze o správnosti, nesprávnosti, přínosu příspěvku apod.

[410] Slovník pedagogické metodologie 2005
[411] Dle PELIKÁN 2011, s. 210 -211

Další nezbytně sledované prvky pro kompletní popis průběhu znamenaly naopak omezení aktivního přístupu pro řízení průběhu lekce v daných limitech:

7. Příkaz, pokyn k usměrnění aktivity lektorem

   „*Rozdělte se do skupin.*“, „*Pojďte si pro desky.*“, „*Soustřeďte se.*“

8. Tlumení iniciativy žáka, odmítnutí aktivity lektorem

   „*Teď se nevěnujeme všem možnostem práce s internetem, ale zaměřujeme se na komunikační služby.*“, „*Nevymýšlejte různé možné odpovědi na otázky, ale soustřeďte se na zhodnocení všech uvedených.*“

9. Přímé stanovení aktivity žáka

   Vyvolávání při chybějící reakci, definice přesného postupu, např. pokud žák neví, jak se vypořádat se zadáním, lektor zadá přesný postup prvního kroku, který má žáka inspirovat k hledání vlastních postupů v aktivitě.

10. Zásah autority

    Lektorka využívala své autority při příliš silné diskuzi, pro předcházení vzájemným útokům nebo při nesprávném vývoji aktivity.

11. Nesouhlas, trest

    „*Neříkejte si navzájem, co jste zjistili.*“, „*Nebavte se.*“, „*Když porušíte pravidlo v soutěži, budete muset odpovědět o otázku navíc.*“

12. Zásah učitelky či vychovatelky k usměrnění chování

    Typickým projevem bylo tišení vykřikování žáků bez vyvolání, pokyn ke sledování výkladu či pokynů lektorky.

Protože segmenty byly hodnoceny zejména kvalitativně, záznamové archy a terénní poznámky, později pak reflexní deníky obsahovaly citace osob v lekci. Frekvence a šíře výskytu byla hodnocena na základě počtu záznamů v daném segmentu. Výskyt v lekci byl hodnocen na základě obsahu a pořadí v poznámkách a záznamech. Výsledek pozorování je v souladu s principy etnografického přístupu prezentován formou analytického interruptu v podobě chronologie[412].

[412] PELIKÁN 2011, s. 234-235

9.2.2 Vzdělávací nástroj pro výzkum

Akční výzkum byl stanoven jako lekce pro žáky 4. a 5. tříd základní školy. Omezením bylo možné návrh přizpůsobit znalostem a schopnostem dětí v tomto věku a jejich ochotě zapojit se do aktivit. Pro mladší děti by mohla představovat problém aktivita založená na písemném projevu, který je pro tyto děti namáhavý a časově náročný, soustředily by se více na psaní než na obsah zpráv. Naopak starší by bylo nutné přesvědčit o kompetenci lektora a o smyslu předmětu lekce, protože téma internetu mohou považovat za zvládnuté, podléhají přesvědčení, že knihovnice jim k tématu nemá co říci. Forma lekce založená na výukovém rámci E-U-R (evokace, uvědomění, reflexe) byla učitelům známá z předchozích výukových akcí v knihovně, nové bylo ale téma základních problémů v komunikaci přes internet s někým neznámým a zpřístupňování zneužitelných osobních informací jako digitálních stop. Cílem lekce bylo naučit děti rozeznávat některé varovné signály před poskytnutím zneužitelných informací.

Lekce trvala 70 minut, což představuje téměř dvě školní vyučovací hodiny. Byla uskutečněna ve všech případech v knihovně v době běžné výuky. Škola se nachází nedaleko knihovny, ale učitelé musí dodržovat časový rozvrh, proto určenou délkou lekce je vyvážen prostor pro předání znalostí více do hloubky, ale současně není narušen celý den výuky. Spojení dvou hodin je na prvním stupni poměrně snadné vzhledem k zajištění výuky jedním učitelem, který si tematickou náplň může snadno přizpůsobovat, mírně problematické by to bylo u druhého stupně, který ale nebyl subjektem této lekce.

I místo výuky se ukázalo jako klíčové. Situováním lekce do knihovny bylo omezeno sledování různých charakteristik projevů, které by omezovaly zaměření na téma lekce, tj. rizikovou internetovou komunikaci, i když starší děti (5. třída), zejména dívky, poměrně často upozorňovaly na jazykové nedostatky v písemných projevech spolužáků. Je nicméně pravděpodobné, že tento trend by byl ve škole silnější. Podobně je tomu s výzvou k uvolnění projevů žáků, které jsou základem aktivního učení. Při něm je vítán jakýkoli příspěvek žáků, třeba i nesprávný, protože může vést k zamyšlení, kde je jeho problém. Již osoba učitelky toto do určité míry omezovala, což bylo patrné i na tom, že před vstupem do místnosti či do knihovny všechny učitelky upozornily žáky, že se mají chovat tiše a mluvit až na vyzvání, což je proti principům aktivního učení. To se v knihovně po krátkém čase vždy

podařilo odbourat, opět je ale pravděpodobné, že ve škole by děti silněji vytrvávaly na zažitých požadovaných stylech chování.

Osoba učitelky se ukázala jako silný faktor pro průběh lekce. Neplánovaně se podařilo, že během realizovaných lekcí se jednou učitelka po předání dětí vzdálila a vrátila se po skončení lekce, v jedné třídě se zapojila do realizovaných aktivit, v jednom případě třídu nedoprovázela vzhledem k absenci učitelka, ale vychovatelka, v ostatních případech učitelka přihlížela lekci. V případě účasti vychovatelky při celé lekci se děti chovaly uvolněně, a to i na úkor pozornosti, také necítily takové zábrany v projevech šikany jedné dívky, která již na lekci přišla s pláčem, že ji spolužák uhodil, a jako jediná žákyně ze všech tříd se nechtěla zapojit do aktivit v lekci. Proti tomu v případě, že učitelka na lekci nebyla přítomná, ale děti na ni přivedla, nebo se dokonce do aktivit zapojila, se děti chovaly srovnatelně jako při pasivní účasti učitelky. V jednom případě došlo k šikaně žáka agresivním útokem ve zprávě v rámci simulace komunikace na internetu, ta ale nebyla vysledovatelná k původci, byla dostatečně skrytá.

Lekce byla zahájena brainstormingem. Cílem bylo upozornit děti, že řešené oblasti vycházejí z toho, co znají a co je součástí jejich života. Současně byl pomocí brainstormingu odbourán odstup, lektor se snažil dětem ukázat, že se staví mezi ně, ne nad ně, a zná způsoby, jakými komunikují, a nezasahuje do nich. Žáci uváděli názvy a typy služeb, které znají ze zkušenosti vlastní nebo zprostředkované jejich příbuznými a známými. Tímto způsobem se děti nemusely bát jmenovat nástroje, u kterých cítí, že by je používat neměly, např. Facebook, kde je věková hranice pro uživatele 13 let, což žáci v případové studii nedosáhli. Během brainstormingu při utišení nápadů lektor místy inicioval další vlnu názorů upozorněním na analogii dosud nejmenované komunikace (např. pro videokonference – „*Pokud si s někým chcete povídat a vidět ho, co můžete použít, abyste se tak bavili přes internet?*“). Při dostatečném množství jmenovaných služeb došlo k jejich kategorizaci a upřesnění komunikačních funkcí, možností a omezení. Po diskuzi o funkcích služeb následoval závěr uvozující následující aktivitu tím, že upozornil na možnost většiny služeb komunikovat s někým neznámým z offline prostředí.

Uvědomění bylo uskutečněno s využitím interaktivní hry. V souladu s postupy této metody[413] jsou reprodukovány situace ze skutečného života dětí pro porozumění a nalezení možných scénářů jednání s ověřením jejich důsledků. Průběh aktivity byl popsán v kap. 8.2.2.

Reflexe pracovala s otázkami, které se mohou objevit v komunikaci na internetu. Žáci se ve skupinách o 3-4 členech rozhodovali, na kterou otázku z nabídky by odpověděli. Po určitém čase byly vybrané otázky diskutovány. Mezi ně patřila např. otázka „*Co dělá tvůj táta?*“ Zde, podobně jako u většiny dalších, lze reagovat způsobem, který poskytne o člověku informaci silně podporující jeho identifikaci v reálném prostředí („*Je učitel v 1. A v Masarykově základní škole v Poličce.*“), ale také naopak s velmi slabým potenciálem identifikace („*Je učitel.*“). Zároveň byly zdůrazněny otázky, které by měly vždy představovat varování, že v komunikaci něco není v pořádku, jako v případě otázky „*Co máš teď na sobě?*“ nebo „*Jsi doma sama?*“. Otázky neřešené v lekci byly ponechány pro diskuzi ve třídě, kterou podle jejich vyjádření učitelky uskutečnily.

Při odchodu dětí z místnosti nechávaly odznaky vylosované před soutěží na obrázcích tzv. smajlíků, které vyjadřovaly hodnocení lekce, tedy zda se jim líbila a doporučily by ji dalším (usměvavý), zda se jim vůbec nelíbila, takže by ji nedoporučily (mračící se), příp. zda je jejich názor někde mezi těmito extrémy (neutrální výraz).

9.2.3 Výsledky pozorování s anketní zpětnou vazbou

9.2.3.1 Fáze evokace

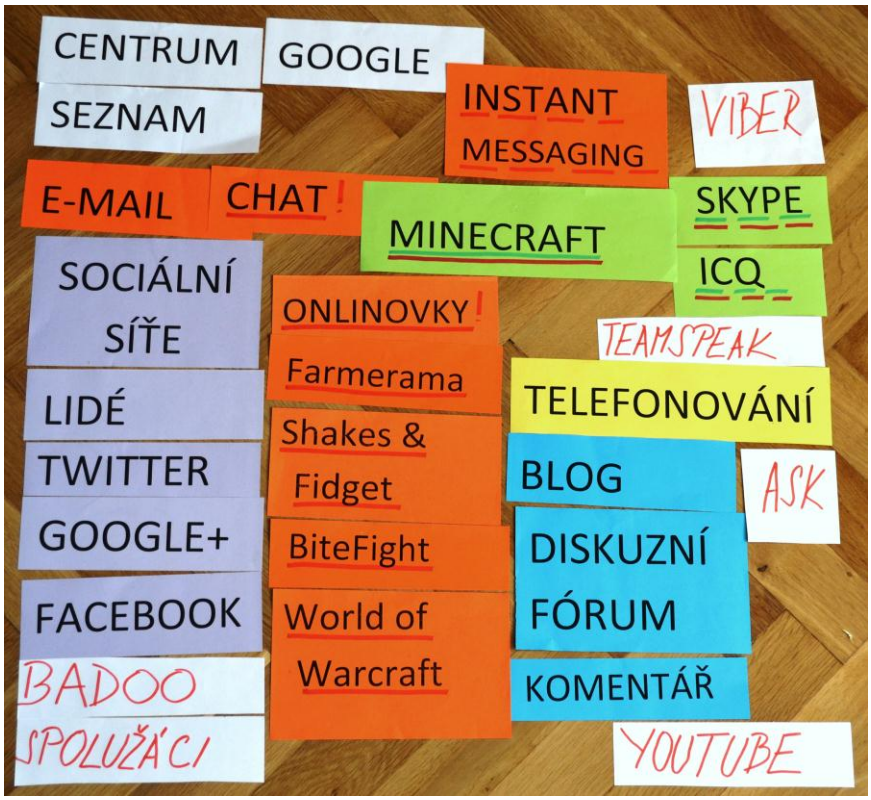
Při zahájení lekce se děti posadily vždy odděleně chlapci a dívky. Na téma lekce reagovaly s nadšením, zejména když jim bylo oznámeno, že v knihovně nebudou číst, ale budou se věnovat internetu. Děti ve všech třídách vnímaly jako přirozené, že do knihovny téma patří, protože vidí, že do ní patří také počítače a internet. Nálada se nezměnila ani v okamžiku uvědomění, že nebudou pracovat se samotným internetem, ale budou se jen o něm bavit a simulovat jej. V rámci brainstormingu děti vykázaly znalost poměrně velkého množství konkrétních nástrojů, často ale měly problém při kategorizaci s jejich obecným označením. Od

[413] BELZ 2001, s. 101

počátku děti byly aktivní, po dvou vyvolání přihlášených děti začaly názvy vykřikovat, přijaly tedy volné projevy aktivního učení. Jen v jedné 4. třídě bylo množství samostatně jmenovaných služeb poměrně nízké, po pomoci lektora ale děti uvedly zástupce všech skupin, stejně jako v ostatních třídách nejvíce her.

V rámci každého opakování lekce se objevily nějaké nové služby, většina z nich se ale opakovala při každém cyklu. Pro zkrácení trvání aktivity bylo po prvním setkání psaní služeb nahrazeno připravenými papíry s jejich názvy, jen ty jmenované nově se dopisovaly (viz obr. 4 Komunikační kaná.y známé dětem). V případě některých služeb děti vyjadřovaly bouřlivé reakce v okamžiku, kdy zjistily, že jsou připravené, a tedy známé. Evidentní byly trendy v populárních službách, v prvním roce všechny třídy, resp. jejich chlapecká část, velmi bouřlivě reagovala v případě Minecraftu, v druhém roce se zájem diverzifikoval a tím zeslabil a posunul k mobilním zařízením, jmenovány byly služby, ale také distribuční kanály (Google Play, AppStore). Během brainstormingu, zejména po první jmenované online hře, byli vždy mnohem aktivnější chlapci než dívky. Ty se zapojovaly častěji s méně obvyklými nápady, obvykle to byly ony, které přišly se službou, kterou bylo nutné připsat, protože v předchozích třídách uváděna nebyla. Chlapci častěji při brainstormingu opouštěli zadání a jmenovali služby, které neslouží ke komunikaci, nejčastěji různé vyhledávače a prohlížeče. Dívky se je pak vždy, když znaly jmenovanou službu, snažily opravit. V tomto okamžiku bylo nezbytné porušit jedno ze základních pravidel brainstormingu a vstoupit do aktivity, vysvětlit, že tento typ služeb neodpovídá zadání[414]. Do tohoto vyjádření totiž žáci v souladu s principem aktivity navazovali na jmenované služby a rozvíjeli podobné, které znají. Pokud přitom sklouzli do služeb, které neslouží ke komunikaci, vzdalovali se kvůli návaznostem a asociacím stále dál od zadání.

[414] STEELOVÁ 2007a, s. 23



Obr. 4 Komunikační kanály známé dětem

Když bylo uvedeno přibližně 25 služeb, brainstorming byl ukončen. Poté byly děti vyzvány ke kategorizaci služeb, ve které jim pomáhaly barvy papírů. To opět sloužilo ke zrychlení aktivity, i když pro čistě aktivní učení by si je měly děti stanovit samy na základě rámcových otázek typu: „*Jak bychom mohli některé (...) spojit a vytvořit k nim nadřazený pojem?*“[415] Za delší čas by děti ke kategorizaci naznačené barvami stejně dospěly, což bylo vyzkoušeno v prvních dvou cyklech (před přípravou papírových vodítek). V případě různých názorů dětí na možnosti komunikace v dané službě nebo při nesprávném vymezení zasáhla lektorka s upřesněním. Děti často způsob komunikace nedemonstrovali obecným popisem, ale svou osobní zkušeností.

> „Skype jsem si musel stáhnout do počítače a pak jsem si psal s kámošama.“
>
> „Na Ask dám otázku a lidi mi pak odpovídají. (…) Ask zná asi každej.“
>
> „Badoo je seznamka.“
>
> „Když hraju Minecraft, tak si vždycky povídám s kámošem (…) No přes Skype.“

[415] STEELOVÁ 2007a, s. 23

Poslední uvedená ukázka demonstruje, jak si děti někdy neuvědomují, co konkrétně používají pro komunikaci, často trvali na tom, že si mohou volat s kamarády přes Minecraft, až po zásahu lektorky akceptovali, že většinou k tomu využívají Skype, ne funkci implementovanou do hry. Děti prokazovaly rostoucí zájem v okamžicích, kdy lektorka ukázala znalost prostředí pomocí v něm používaných jazykových projevů (možnosti Minecraft spojené s některými servery, označení pro týmy v různých hrách, např. klany, gangy apod.).

Zajímavým zjištěním bylo, že děti neměly problém s uváděním konkrétních sociálních sítí, několik tříd ale mělo problém s jejich obecným označením, které přijímaly spíše s rozpaky. Naopak někdy jmenovaly méně známé služby, které podle svých vyjádření i používají, např. Twitter nebo Viber.

Vzhledem k tomu, že tato aktivita byla skupinová, nebyly všechny děti nuceny se zapojit, z celé třídy se ale nezapojilo jen několik jednotlivců, čímž se podařila aktivizace studentů, což je jedna ze základních funkcí fáze evokace. Několik žáků bylo aktivních po celou dobu aktivity, většina se však zapojovala vždy v dílčích chvílích, když byly jmenovány určité, podle všeho jimi používané, služby. V souladu s teorií[416] se po prvním odbourání bariér zapojením několika málo jedinců do aktivity podařilo aktivizovat většinu třídy. Lze tedy konstatovat, že až na výjimky došlo k naplnění cílů fáze evokace pomocí brainstormingu, kdy si žáci z chaotických a roztříštěných zkušeností zformovali vědomostní základ již známého pro následující činnosti, které jej rozvíjí a tímto spojením dochází k dlouhodobějšímu zvnitřnění (interiorizaci) a hlubšímu porozumění[417]. Současně došlo k určitému učení, když byly zjištěny a opraveny chybné názory a znalosti. Vlivem navázání na existující znalosti by mělo dojít k dalšímu klíčovému důsledku evokace, vzbuzení vnitřního zájmu žáků řešit stanovenou problematiku, protože si jsou vědomi jeho smyslu a dokáží se s ním ztotožnit[418]. Jeho dosažení naznačuje pozorovaná aktivita a reakce žáků na pokračování v lekci.

[416] GRECMANOVÁ 2000, s. 31
[417] STEELOVÁ 2007a, s. 24
[418] STEELOVÁ 2007a, s. 24

9.2.3.2 Fáze uvědomění si významu

Soutěž pro uvědomění si významu tématu bylo nutné upravit po prvním provedení. Zcela zásadní se ukázalo použití e-mailů v komunikaci, protože všechny děti v prvním běhu velmi rychle pochopily, že v e-mailu je často uvedeno jméno a tak snadno zjistí, s kým se baví. Od druhého běhu se proto e-maily spolu se jmény zařadily mezi zakázané otázky.

Vžití se do situace srovnatelné s komunikací přes internet bylo podpořeno tím, že lektorka místy simulovala jeho fungování např. tak, že když chyběla identifikace příjemce zprávy, tak ji odnesla, ale následně ji vrátila zpět odesilateli s vysvětlením, že internet nemohl zprávu z tohoto důvodu doručit. Podobně bylo zdůrazněno, že lze stejně jako na internetu komunikovat s více lidmi současně, ale při jejich větším počtu už člověk nestíhá odpovídat a nepodaří se mu proto získat tolik informací o jednom člověku, ale málo informací o hodně lidech, z čehož nelze odvodit jejich identitu. Toto bylo nakonec využito jako trest, který nebyl deklarován, dokud se problém neobjevil, stejně jako postih při porušení některého pravidla v soutěži. Ten, kdo se tím cítil poškozen a stěžoval si lektorce, dostal pokyn žádat dvě odpovědi místo jedné v jednom kole jako postih. Tento postup odpovídá aktivnímu učení, kdy si samy děti stanovují vývoj aktivity a je na nich samotných, aby osobně nebo v interakci s ostatními získaly požadované poznatky.

Protože dělení do skupin nebylo podle zájmu dětí, ale podle losování a bylo nutné utajit svou vylosovanou značku, došlo k rozdělení kamarádských skupin. Proti tomu děti neprotestovaly, skrývaly své placky přede všemi. Až když zjistily, kdo je v jejich polovině, začaly sdílet svá čísla a písmena. Opět tedy interakce pro aktivní učení vznikla zcela přirozeně, stejně jako formování vhodně velikých skupin pro interakci, kterou Kasíková stanovila na 2-6 osob[419].

Pro zjednodušení zahájení soutěže děti pro začátek dostaly ukázkové otázky: „Jsi kluk nebo holka?“ „Co teď hraješ na internetu?“ První z uvedených byla často používána, druhá výrazně méně, ukázalo se tedy, že otázky byly skutečně pro inspiraci, ale rychle byly nápady na předmět otázek hledány ve zkušenostech samotných žáků z internetu. Dále pro první kontakt děti dostaly předepsané adresy pro první komunikaci, čímž bylo také zajištěno, že každý na začátku dostane jednu zprávu a bude mít na co odpovídat.

[419] KASÍKOVÁ 1997, s. 38

Pravidla byla poměrně dobře pochopena, pro jistotu byla v každé místnosti zapsána na tabuli. Přesto se děti chodily ptát, zda je nějaká otázka možná, spíše ale ve chvílích, kdy se chtěly pochlubit otázkou, kterou považovaly za povedenou. Podobně se chodily pochlubit také odpověďmi, které byly podle nich zdařilé. Toto chlubení zdařilými otázkami a odpověďmi nebylo zakazováno, ani podporováno.

„Jakou máš barvu vlasů. Jakou mám barvu vlasů? Na to se mě nemůže zeptat, že ne?“

„Kde bydlím? Mám mu dát ulici, nebo město?“

„Co ti napsal?“

„Paní učitelko, já mám strašně zajímavou poštu, přečtěte si to.“

„Já mám geniální otázky, podle toho bych to mohla i zjistit.“

„Paní učitelko, oni mi napsali, jaký máš vlasy a já mastný.“

„Psal, kde bydlíš a já v Poličce.“ „Tak to je hodně dobrý.“ (rozhovor žáků)

„Když se tě zeptaj na bydliště, tak tam dej byt.“ „Nebo bydlím v domě.“ „Bydlím nedaleko školy.“

Děti tak samy přišly na to, jaké postupy je vedou ke stanovenému cíli – odhalení cizí identity a uchování vlastní a sdílely to se spolužáky. Tento tzv. aha-moment přitom kromě efektu učení vede také ke vzbuzení radosti a pocitu, že učení je příjemná věc[420]. Zásadní zjištění tedy nepřišlo od lektorky, ale vrstevníků, bylo pak zvažováno při vlastní aktivitě. Objevilo se ve všech skupinách, někdy přeneseně z druhé skupiny, když si někdo naopak stěžoval, že ta otázka či odpověď mu překazila snažení. Jen při sdílení získaných identit lektorka usměrňovala, častěji však bylo sdíleno přesvědčení na obecné úrovni.

„Já už asi tuším, kdo to je.“

„Ježiši, už vím, to je určitě Kája.“

„Já si píšu s klukem a s holkou asi…“

„Ten, s kým si píšu, ten je nenápadnej jako svrab v zadku.“

„Já mám jednoho tak nenápadnýho kamaráda, že jako…“

„Mě už znaj, tý jo, dva.“

„Ty ses nějak rozepsala“ „Ne, to oni se se mnou rozepsali, já jsem si začala psát se dvěma“

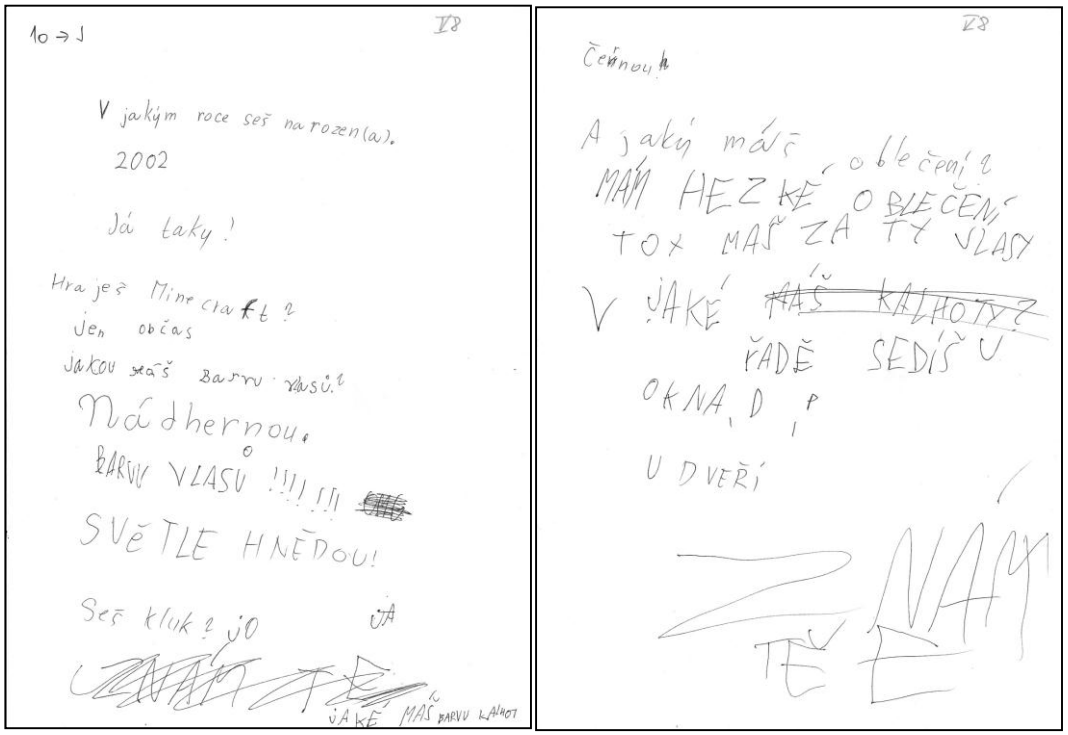
„To jsou nějací tajní ctitelé…“ „Vždyť ani nevědí, kdo jsem.“ „Tušej“ „Hm, tušej, jeden už jo“ (rozhovor žákyň)

„Kolik jich máš?“ „Tři.“ „Já taky tři.“

Děti usilovaly o co nejvíce zprostředkovaných zpráv, když došlo k jejich přenášení, tj. lektorka či její pomocnice odcházely z místnosti, snažily se ji zastavit, že ještě dokončí a pošlou jednu zprávu. Podobně se sbíhaly při nové sérii

[420] STEELOVÁ 2007b, s. 9

doručených zpráv pro jejich rychlé získání. Při psaní odpovědi se soustředily na psaní tak, že často nevnímaly, že jsou volány pro další zprávy. To potvrzuje výše uvedenou obavu v nevhodnosti nasazení pro mladší děti, které by měly větší limity v soustředění se na psaní na úkor obsahu soutěže. Problém s písmem se objevil především u dětí v 5. třídě, kde se identifikovaly podle rukopisu, nejen podle zjištěných informací. Někteří si to uvědomili již na počátku aktivity a dotazovali se lektorky, jak to vyřešit, přičemž sami nabízeli vlastní řešení – že si zprávy nechají psát někým jiným. V druhém roce byly změny písma lektorkou výslovně doporučeny při zahájení soutěže, aby pozornost byla zaměřena opravdu co nejvíce na obsah, ne formu zpráv. Na obrázku 5 je zobrazena ukázka komunikace mezi dvěma žáky při závěru soutěže. Obsah zpráv, který je klíčový i pro zhodnocení průběhu lekce, je předmětem kap. 9.3. Jak již bylo uvedeno, byla plánována pro doplnění poznatků v oblastech, které nemohly být zjištěny prostřednictvím pozorování, jedná se o ověření simulačního efektu aktivity, tedy přijetí činnosti s přenosem z reálného užívání internetu, postupů pro naplnění cíle hry a také pro identifikaci témat, na která jsou děti dotazovány nebo se dotazují přes internet.



Obr. 5 Příklad zprávy v soutěžní části lekce

Aktivně se zapojili všichni žáci (jediná výjimka žákyně, která již na lekci přišla s problémem se spolužáky, je popsána výše), vždy po celou dobu soutěže, která trvala cca 20 minut. Pokud došlo k zaměření pozornosti jiným směrem, bylo velmi krátké (v řádu vteřin), např. při objevení zajímavé knihy v regále. Tato aktivita byla podle pozorování pro žáky zábavná, protože každá skupina projevila nespokojenost při oznámení konce soutěže. Zaujetí aktivitou ale projevovali i výslovně (např. při jejím zahájení i průběhu slovy „*Paní učitelko, to je dobrá soutěž.*“, opakovaně zazněly i výzvy typu „*Pošta, dělej.*“ Nebo rozhovory mezi žáky „*Baví tě to?*“ – „*Jo.*“). Opět tedy pozorování potvrdilo vhodnost činnosti z hlediska aktivizace žáků při učení.

Po ukončení soutěže došlo k jejímu vyhodnocení, přibližně čtvrtina až třetina dětí skončila s body v minusových hodnotách, tedy více žáků odhalilo jejich identitu, než naopak. Tři žáci s nejvyšším počtem bodů získali symbolickou odměnu[421] v podobě placek s internetovou tematikou, o které projevovali zájem. Po vyhodnocení soutěže došlo ke stručnému pozastavení nad jejím průběhem pro upozornění na rozdíly a podobnosti s prostředím internetu, které bylo simulováno. Užitečné otázky a odpovědi byly žáky vykřikovány a vzájemně komentovány. Děti spontánně navrhovaly také možné postupy v situacích, kdy po nich internetový známý bude chtít znát identifikující informace, nejčastěji bylo uváděno jeho zablokování. Možnost uvádění nepravdivých informací byla dětmi jmenována ve všech skupinách ještě před zahájením soutěže, kdy před uvedením pravidla vyžadujícího pravdu ve zprávách vždy zaznělo, že vlastní identita bude chráněna nepravdivými odpověďmi. Zajímavé je, že tento postup často děti viděly u sebe, ale obvykle si ho již nespojily s druhou stranou komunikace, protože po aktivitě tato možnost ochrany identity oproti blokování nebyla uváděna dětmi, ale doplňována lektorkou. Přestože nebylo z pozorování možné hodnotit kvalitu simulace z hlediska propojení aktivity a reality z pohledu žáků, byly děti upozorněny na vhodnost opačného přenosu získané zkušenosti, tedy v reálné komunikaci po otázce od internetového známého hodnocení, zda by uvažovaná odpověď přispěla v soutěži k odhalení identity. Přijetí tohoto směru simulace bylo následně podpořeno závěrečnou aktivitou lekce.

[421] Vhodnost odměny při aktivním učení zdůrazňuje PETRESS 2008

Při hodnocení z hlediska aktivního učení je opět možné konstatovat, že lekce naplnila sledované aspekty. Přestože se jednalo o soutěž, která není pro kooperaci ideální[422], hlavní motivací v aktivitě nebylo vyhrát, což bylo možné vysledovat na tom, že děti se nezajímaly navzájem o množství uhodnutých identit, ale spíše o samotnou podstatu aktivity, tj. účinné a neúčinné otázky a odpovědi, ke kterým obvykle dospěli vlastním zjištěním, které pak sdíleli s ostatními. Projevilo se tedy v teorii popisované poznání větší důležitosti procesu než výsledku[423]. Přestože děti sdílely jen část otázek a odpovědí, takže jejich obsah nebylo možné zcela zhodnotit v rámci zúčastněného pozorování, tato ukázka naznačovala, že hra splnila simulační efekt, který byl následně ověřován triangulací dat, především dokumentovou analýzou. Sdílení poznatků dětí neprobíhalo jen s lektorkou a jejími pomocnicemi, ale také mezi dětmi samotnými, lze tedy vysledovat tzv. peer teaching, které patří k základním prvkům aktivního učení[424]. Při přijetí nastavené formy aktivního učení je zásadní také odbourání omezení se na základě kvality či kvantity činnosti, klíčová je jakákoli aktivita, která je následně otestována a dítě samo získá vědomí úspěšnosti zvoleného postupu, což ještě při zapojení sociální interakce a principu tzv. „lešení“ zvyšuje efektivitu učebního procesu[425]. Vzhledem k tomu, že poznatky staví na znalostech a dovednostech jednotlivců, kteří sice prochází stejnou aktivitou, ale různým způsobem, je naplněna i podmínka individualizace učení a podpořeno zapojení vnitřní motivace žáků, protože poznávají nové informace v oblasti, která je pro ně zajímavá a součástí každodenního života[426]. Z hlediska snahy dětí sdílet nové poznatky i stihnout toho ve stanoveném čase co nejvíce, a naopak projevený zájem neskončit ukazují, že aktivitu přijaly zamýšleným způsobem, protože došlo k naplnění základních cílů fáze uvědomění: udržení zájmu žáka a podnícení žáků sledovat vývoj vlastního chápání nových poznatků (vědomé navazování nových na již existující)[427].

[422] HANSEN ČECHOVÁ 2006, s. 24
[423] KASÍKOVÁ 1997, s. 91
[424] HANSEN ČECHOVÁ 2006, s. 25
[425] STEELOVÁ 2007a, s. 16-17
[426] STEELOVÁ 2007a, s. 18-19
[427] STEELOVÁ 2007a, s. 25

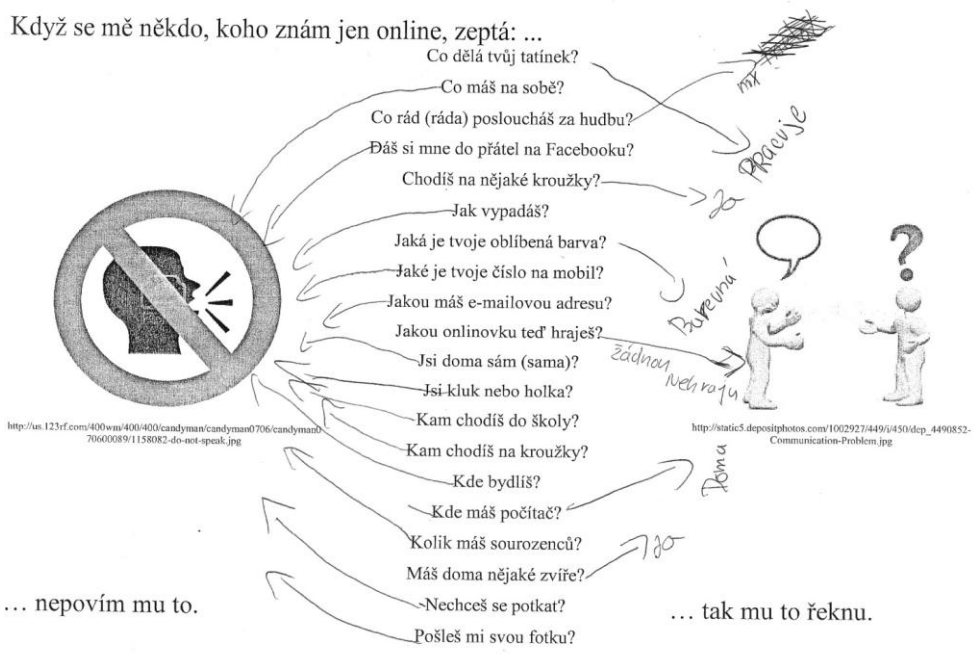
9.2.3.3 Fáze reflexe

Reflexe problematiky byla založena na reakcích na otázky na internetu. Sloužila k ukotvení nových poznatků v předchozí znalostní struktuře dětí, což je smyslem této fáze[428]. Připravené otázky byly uvedeny na papíře a děti ve skupinách diskutovaly o tom, zda by danou informaci poskytly člověku, kterého znají výhradně z internetu. Výsledný dokument je ilustrován na obrázku 6. Pro lekci bylo pozitivním zjištěním, že děti se odkazovaly při volbě odpovědi na předchozí aktivitu, kterou lze proto označit za plnící svou funkci. Při skončení lekce byl tedy patrný přínos v přemýšlení nad poskytováním osobních informací, není ale jasné, jak dlouhodobý tento efekt je. Přestože se jednalo o aktivitu, která ukončovala více než šedesátiminutový program, děti se soustředily na její průběh a po celou dobu, která byla určená práci ve skupině, se bavily o otázkách na papíře. Jen výjimečně tento hovor byl veden nevážně, tyto přístupy se ale objevily jen v páté třídě a vždy jen v jedné až dvou skupinách z 6-8.

„Jak vypadáš? Mám velkou baradavicu."

„Co je komu do toho?"

„Co dělá tvůj tatínek? Pracuje."



Obr. 6 Reakce na otázky od internetového kamaráda

[428] STEELOVÁ 2007a, s. 26

I přes slabší pozornost se děti při výzvě k vyhodnocení zvolených reakcí uklidnily, sledovaly výklad a reagovaly na lektorku. Připravené reakce byly porovnány s vhodnými modely chování, zejména byl kladen důraz na pochopení možnosti odpovědět způsobem, který neposkytne identifikující informace a na možnost neodpovídat. Děti většinou samy v rámci této aktivity rozhodovaly vhodným způsobem, který samy doplnily vlastním komentářem.

> „Chodíš na nějaké kroužky? Já bych mu to řekl, ale neřekl bych mu kam."
>
> „Můžu mu říct, že chodím plavat, ale on neví kam."
>
> „Kde máš počítač?" (lektorka) „No to bych mu neřek." „V pokoji." (žáci)
>
> „Pošleš mi svou fotku?" (lektorka) „Já bych mu poslal svou fotku, ale obličej by nebyl vidět."
>
> „Kdo by odpověděl na otázku: jak vypadáš?" (lektorka) „Jsem neodolatelný." (žák)
>
> „Jakou onlinovku teď hraješ?" (lektorka) „To bych řekl, to má jedno, tak nemůže zjistit moji profilovku a tak." (žák)

Tato varianta dává vodítko, jak se nevzdat komunikace i seznamování přes internet, ale redukovat riziko nalezení v reálném prostředí. Naprostý zákaz by děti mohl odradit od dodržování bezpečnostních pravidel, protože komunikace přes internet je pro ně důležitá. Děti ve 4. třídě a některé i v 5. ještě viděli možnost nepoužívat komunikaci přes internet (např. reakce „*Lepší je se s nikým cizím nebavit.*"), s vyšším věkem již toto řešení ale připadalo stále méně reálné, což u stejných dětí, které v prvním roce deklarovaly možnost nepoužití internetu, ale v druhém změnily názor, potvrdily dospělé respondentky rozhovorů (viz kap. 9.4).

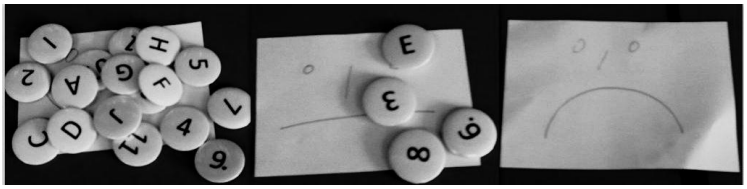
Jiné reakce také naznačují, že děti se z lekce snažily zjistit jak řešit problémové situace, které znají (např. „*A co mám dělat, když mi začne nadávat?*"). V tomto případě po odpovědi lektorky žák ještě několikrát konkretizoval situaci, pro kterou hledá řešení, kdy odcházel s tím, že ví, jak blokovat uživatele Facebooku, který mu začal nadávat. Navázala žákyně, která se ptala, jak má postupovat, když si pořád bude odebírat problematického přítele z Facebooku a on si ji stále bude přidávat. I k tomu dostala reakci od lektorky, jejímž smyslem bylo upozornit všechny žáky na problém slepého přidávání si přátel bez rozmyšlení, o koho se jedná a jaké má zařazení do skupiny přátel důsledky. Tento přechod k řešení reálných problémů žáků byl zcela neřízený lektorkou, v souladu s aktivním učením děti rozhovor iniciovaly samy.

V souladu s cíli reflexe žáci vyjadřovali nové poznatky vlastními slovy a navazovali je na své reálné zkušenosti i na sebereflexe předchozí aktivity, současně

docházelo k výměně názorů mezi žáky, a to na úrovni vysvětlující, ne útočné[429]. Jak ukazuje popis dílčích segmentů, došlo ke strukturování poznatků navázáním nových na staré s tím, že si žáci uvědomovali, proč by aktuálně v komunikaci na internetu postupovali z hlediska poskytování informací o sobě daným způsobem[430]. Závěrečná aktivita jim přitom se strukturováním jednotlivých dílčích poznatků pomáhá, aby po učení nezůstali poznatky roztříštěné, chaotické. Ověření správnosti struktury je přitom realizováno s pomocí ostatních spolužáků a lektora. Přestože tedy aktivita byla skupinová, i zde v rámci diskuze došlo k zohlednění individuality učení žáků, která je pro fázi reflexe důležitá, protože každý si potřebuje pro dílčí poznatky vytvořit vlastní řád navazující na vlastní předchozí zkušenosti[431]. Protože vytváření pevných struktur může trvat déle, než je čas na aktivitu a také i při všech opakováních lekce se nestihlo projít celou tabulku, ale různě dlouhé její části, byla tato aktivita v souladu se stanovenými postupy pro aktivní učení[432] ponechána k navázání ve třídě k diskuzi mezi žáky pod vedením učitelky.

9.2.3.4 Reakce žáků na lekci

Po této aktivitě byla lekce ukončena. Děti byly upozorněny na vhodnost rozšiřujících činností, především ve formě samostatného zkoumání činností a aplikace naučeného na nové (při lekci konkrétně neřešené) případy v souladu s tím, že evokace by měla sloužit také k vytvoření motivace pro další rozvoj v tématu přes ujasnění odpovědí na řešené otázky a tím vytvoření prostoru pro otázky nové[433]. Druhý pokyn vedl k postupu pro jejich zhodnocení lekce. Když žáci opouštěli místnost, nechávali své placky z druhé fáze lekce na obrázcích vyjadřujících názory na celou lekci. Výsledky hodnocení ukazuje obr. 7.



Obr. 7 Zpětná vazba od žáků po lekci

[429] STEELOVÁ 2007a, s. 26-28
[430] STEELOVÁ 2007a, s. 19
[431] STEELOVÁ 2007b, s. 13
[432] STEELOVÁ 2007c, s. 15
[433] STEELOVÁ 2007c, s. 16-17

9.2.4 Diskuze průběhu lekce

Jak bylo uvedeno v popisu metodologie, pozorováním 8 tříd došlo k potvrzení saturace vzorku. Nicméně jak je obvyklé v akčním výzkumu, jsou zjištěné poznatky platné jen pro zkoumanou skupinu osob. Bezpochyby mezi klíčové faktory v prostředí, které měly vliv na průběh lekce a tím na poznatky ze zúčastněného pozorování, patří velikost obce, kde bylo šetření realizováno a které je méně anonymní než velké město. To vede k bližším mezilidským vztahům mezi všemi subjekty výzkumu, včetně výzkumnice, která sice vstoupila jako externí faktor, rychle ale byla přijata jako prvek, který do prostředí patří. K tomu přispívá, že lekce v knihovně pro třídy probíhají pravidelně a vždy jsou vedeny knihovnicí, ne učitelkou. Současně je dětem i učitelům známý i formát lekce založený na aktivním učení a rámci evokace – uvědomění – reflexe. V případě, že by tomu tak nebylo, by bylo nutné déle navazovat vztahy založené na důvěře a otevřenosti mezi všemi skupinami, jejichž význam pro průběh a výsledek lekce byly popsány jak u neformálního vzdělávání (viz kap. 8.1.1), tak i u aktivního učení (viz kap. 8.1.2). Tyto prvky prostředí byly vnímány již při plánování výzkumu a výběru prostředí, je nutné je zdůraznit pro zvážení přenositelnosti do jiných prostředí.

Zúčastněné pozorování splnilo svůj cíl, došlo k potvrzení teorie aktivního učení v rámci navržené lekce, a to ve všech fázích, jak bylo popsáno v předchozí kapitole. Současně se potvrdil edukační cíl lekce. K těmto výsledkům došlo i přes to, že třídní kolektivy se velmi lišily, a to jak na úrovni žáků, ze kterých byly složeny, tak také v oblasti skupinové dynamiky. Tím je potvrzena přenositelnost lekce s udržením dosažitelných cílů lekce navzdory mnoha specifikům kolektivu, je ale v budoucnosti nutné ověřit přenositelnost i do odlišných prostředí, především při změně faktorů jmenovaných v předchozím odstavci.

Pomocí pozorování bylo možné potvrdit právě to, zda nastavení lekce odpovídá postupu a výsledku aktivního učení, zda dochází k získání nových poznatků v řešené oblasti pomocí realizovaných aktivit a především interakce různých členů lekce, které staví na předchozích znalostech a na nich jsou postaveny nové znalostní struktury, které jsou systematicky ukotvené pomocí reflexe. Všechny tyto cíle lekce sledované pozorováním se podařilo naplnit. Pro zvýšení validity akčního výzkumu, ale také pro doplnění dalších hledisek hodnocení

nastavení a průběhu lekce byly dále využity materiály, které během ní děti vytvořily. Jejich analýza je předmětem další kapitoly. Závěry jsou vzhledem k úzkému propojení a vzájemnému doplňování výsledků výzkumů vymezeny společně v kap. 9.6.

9.3 Dokumentová analýza

Zúčastněným pozorováním byly zjišťovány projevy a sdílení mezi žáky, nebylo ale možné zjistit podrobnosti k obsahu komunikace. Proto byla v návaznosti prováděna dokumentová analýza, pomocí které je možné potvrdit, že děti přijaly aktivitu jako simulaci komunikace přes internet, simulační hra pro přenos nových poznatků, který byl pozorování částečně skrytý, je funkční. Simulační a edukační efekt, tj. funkčnost simulační hry, byl sledován analýzou obsahu komunikace a proměnou v oblasti poskytování identifikovatelných informací a naopak schopností dávat na otázky pravdivé, ale ne identifikující odpovědi.

Vzhledem k tomu, že dokumentová analýza navazuje na pozorování, jsou společné některé charakteristiky výzkumu v oblasti sběru dat, blízký je také jejich cíl, protože se jedná o nedělitelné složky akčního výzkumu, jejichž cílem je poskytnout komplexní popis řešení lekce k bezpečnosti digitálních stop dětí vyučované v knihovně.

9.3.1 Metodologie šetření

Obsahová analýza dokumentů patří ve vzdělávání k nezanedbatelným zdrojům informací[434]. V případě kvantitativního přístupu navazujícího na kvalitativní určení proměnných, je cílem objektivní a systematický popis obsahu komunikace[435]. Volba této metody vycházela z vyvážení nevýhod již popsaného pozorování výhodami dokumentové analýzy[436]: přístup k jinak nezjistitelným informacím, nevystavení dat chybám a zkreslení, nereaktivní sběr dat (subjektivita

[434] PELIKÁN 2011, s. 150; SKUTIL 2011, s. 95
[435] SKUTIL 2011, s. 96
[436] HENDL 2008

výzkumníka vzhledem k datům nepodstatná). Naopak ve výsledcích je nutné zohlednit nevýhody metody, především složitou interpretaci zjištění.

Kvantitativní dokumentová analýza tedy navazovala na zúčastněné pozorování s cílem potvrdit efektivitu simulační hry, která je jádrem lekce, protože v ní dochází ke klíčovému přenosu poznatků. Cílem této analýzy bylo zmapovat a ověřit na základě předchozích výzkumů[437], že aktivita v lekci opravdu slouží jako simulace online komunikace a děti přijímají tento způsob komunikace, proto si v lekci zažijí vhodné modely chování. Vedle toho došlo ke komparaci dat z pozorování pro zvýšení validity akčního výzkumu.

Protože tedy bylo ověřováno již známé, byly stanoveny tři základní výzkumné otázky:

VO1: Potvrzuje dokumentová analýza výsledky zúčastněného pozorování v principech aktivního učení?

První výzkumná otázka nejsilněji spojuje analýzu a zúčastněné pozorování tím, že v dokumentech jsou potvrzovány pozorované prvky aktivního učení. Sledovány jsou důsledky interakce mezi žáky tím, že v rámci skupin jsou pokládány totožné otázky a odpovědi, hra je brána vážně se snahou dosáhnout stanoveného cíle, proto jsou pokládány smysluplné otázky. Další dvě výzkumné otázky se zaměřují na další klíčové prvky aktivního učení, jejichž zjištění bylo důvodem zvolení dokumentové analýzy pro triangulaci dat.

VO2: Odpovídá simulační hra tematicky komunikaci na internetu, na kterou se odkazuje?

Druhá výzkumná otázka se zaměřuje na obsah dokumentů. Snahou je proto především potvrdit, že ten odpovídá informacím, které jsou často dotazovány a odpovídány dětmi při komunikaci přes internet. Tím je potvrzeno, že se jedná skutečně o simulaci a je tedy možný přenos získaných zkušeností do reálného života v internetovém prostředí.

VO3: Vede simulační hra žáky k vlastnímu pochopení vhodných reakcí na osobní otázky na internetu?

Poslední výzkumná otázka slouží k ověření edukačního efektu aktivity. Jejím cílem je ověřit, otevřenost žáků v poskytování osobních informací i to, zda to odpovídá výzkumům komunikace dětí na internetu (viz výše). V návaznosti na to

[437] LIVINGSTONE 2011; Polovina dětí reaguje na internetu (...) 2010; KOPECKÝ 2012

je pro tuto otázku potřebné zjistit, zda se během aktivity změnil přístup žáků v poskytování osobních informací z pohledu, jak dobře přispívají k jeho identifikaci. Výsledky v tomto směru mají omezenou platnost vzhledem k tomu, že dokumenty vznikaly postupně, ne všechny kolovaly již od zahájení aktivity, i první odpovědi proto mohou být neidentifikující vlivem lekce, pokud k pochopení došlo již před zahájením tvorby dokumentu, což je nezjistitelné. Jedná se tedy spíše o validaci zjištění zúčastněného pozorování.

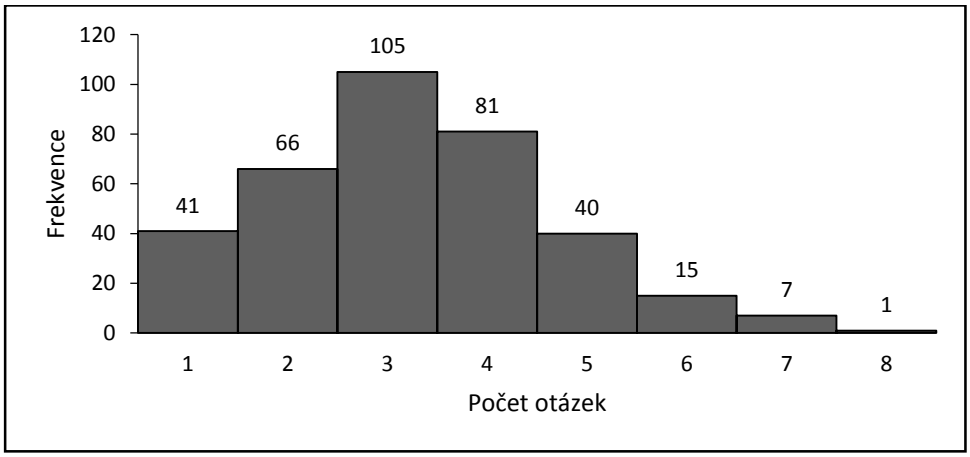
Sběr dat pro analýzu probíhal při všech lekcích akčního výzkumu, pochází z osmi tříd. Žákům byla sice dána možnost dokumenty neposkytnout a odnést si je, ale té využilo jen několik jednotlivců, jak je patrné z chybějících pseudonymů žáků v aktivitě mezi dokumenty. Celkově bylo pro analýzu shromážděno 356 dokumentů, které byly zpracovány v programu SPSS.

9.3.2 Výsledky výzkumu

Analyzované materiály byly získány z lekce realizované v osmi různých třídách ve dvou letech, jednalo se o pět 4. tříd (224 dokumentů) a tři 5. třídy (132 dokumentů). Z každé třídy bylo získáno poměrně srovnatelný počet dokumentů (11,8 % - 14,3 % ze souboru dokumentů), jen jedna byla méně zastoupena (9,8 %). Dokumenty dalo pro analýzu k dispozici celkem 172 žáků, v průměru každý z nich vytvořil 4,14 dokumentu, nejčastěji 3, podrobněji počet dokumentů poskytnutých jednotlivými žáky zobrazuje graf 61.

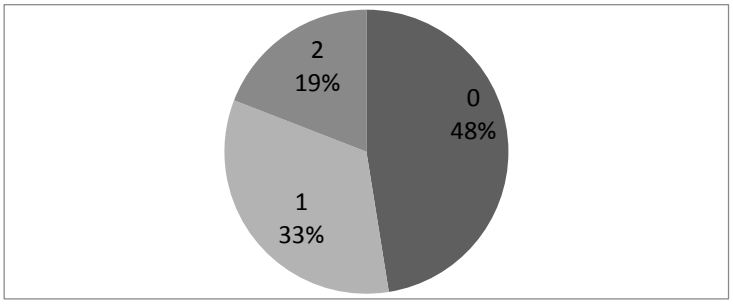
Graf 61 Počet dokumentů poskytnutých jednotlivými žáky

Jednotlivé dokumenty byly analyzovány všechny zanechané po lekci, některé z nich obsahovaly jen otázku, jiné byly dlouhé, oba typy mají pro šetření význam, ale liší se množstvím dat, které z nich je možné vyhodnotit. Tyto rozdíly nejlépe dokumentuje počet položených otázek (viz graf 62), který vlastně znamená počet zahájených různých cyklů dotazování (pokud byla stejná otázka položena na obou stranách, považuje se stále za jeden cyklus, nepřináší nic nového s hlediska sledovaných charakteristik). Pro kvantitativní obsahovou analýzu bylo získáno celkem 1158 otázek, průměrně jich jeden dokument obsahoval 3,25 (modální hodnota byla 3 otázky pro jeden dokument).



Graf 62 Počet položených otázek v dokumentech

Podstatné byly nejen otázky, ale také odpovědi. Těch bylo o něco méně než otázek, protože v rámci soutěže některé nebylo z časových důvodů možné zodpovědět. V rámci odpovědí byl sledován identifikační potenciál, zásadní ale byla jeho reálná smožnost využití. V souladu s pokyny v soutěži děti přesvědčení o odhalení identity druhého vyjadřovaly větou *znám tě*, díky čemuž bylo při analýze možné zjistit, kolik dětí dospělo k tomuto cíli (viz graf 63).

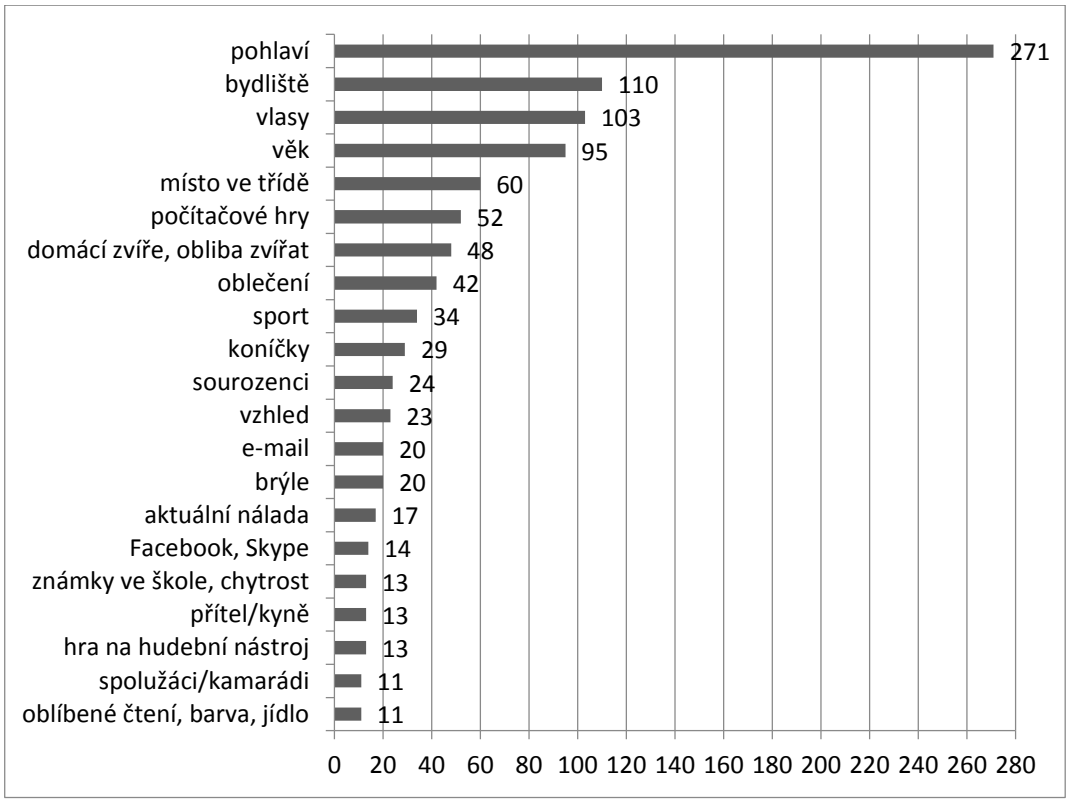


Graf 63 Počet odhalených identit v dokumentech

Některé domněnky o identitě nebyly správné, jak ukázalo zúčastněné pozorování, to ale není předmětem této analýzy. Zásadní bylo uvědomění si možnost identifikovat pomocí informací konkrétní osobu. Některé dokumenty obsahovaly pouze jednu otázku, ne všechny byly tedy schopné poskytnout dostatek vodítek k identifikaci konkrétního spolužáka, přesto jen necelá polovina všech dokumentů nevedla k identifikaci alespoň jedné strany komunikace. To ukazuje, že děti dostatečně pokládaly otázky, které by je dovedly k cíli hry. V případě, že ho nedosáhly, nejde pravděpodobně o důsledek nízkého počtu otázek, spíše jejich kvality (či nevyjádření v dokumentu, že k odhalení došlo), průměrný počet otázek v kategoriích podle počtu odhalených identit v dokumentu se výrazněji neliší (hodnoty: 0=>3,12; 1=>3,35; 2=>3,41). Naopak dosažení cíle nebylo vždy jen zjištěnými informacemi, jak již bylo rozvedeno v rámci zúčastněného pozorování (viz s. 233), roli někdy hrálo poznání rukopisu.

9.3.2.1 Témata v dokumentech

V rámci zjišťování obsahu dokumentů byly tedy sledovány identifikační potenciály odpovědí, v případě otázek jejich pořadí, které vyjadřovalo, jakou důležitost děti informaci přikládají, a proto se ji snaží zjistit spíše než jinou, na kterou se zeptají až v případě dostatku času později. Celkem bylo zakódováno 32 různých tematických zaměření otázek. V rámci dosažení výzkumného cíle bylo klíčové srovnání frekvence výskytu témat v otázkách s výzkumy komunikace na internetu, aby bylo možné potvrdit simulační efekt hry. Tato frekvence výskytu témat, která se v dokumentech objevila více než desetkrát (3 % dokumentů), je zobrazena v grafu 64 Tematické oblasti v analyzovaných dokumentech.



Graf 64 Tematické oblasti v analyzovaných dokumentech

Jak je patrné z proměnných v grafu, jsou různě konkrétní. Při analýze byla kódována co nejkonkrétnější vymezení, u málo zastoupených proměnných došlo k seskupování do širších kategorií. Tak je zachována specifičnost tematického cílení dotazů a současně podpořena možnost statistického zpracování. Přesto některé proměnné zůstaly málo zastoupené a z dalšího hodnocení proto byly vyloučeny. Byly zaměřeny různými směry, objevily se dotazy na politické přesvědčení, majetek, zda je žák pravák nebo levák nebo zda kouří. Vedle těchto omezujících, ale obecných témat, se mezi málo zastoupenými proměnnými někdy vyskytla témata, která slouží opravdu pro přímou identifikaci konkrétního žáka:

„Přišla si dnes poprvé do školy?“

„Máš sádru?“

V jedné třídě se objevily dotazy na identifikátory žáků (číslo ve třídě). Otázka byla zastoupena ve čtyřech dokumentech, kde se tři žáci vyskytovali opakovaně mezi komunikujícími, což odpovídá aha-efektu při interakci v učení.

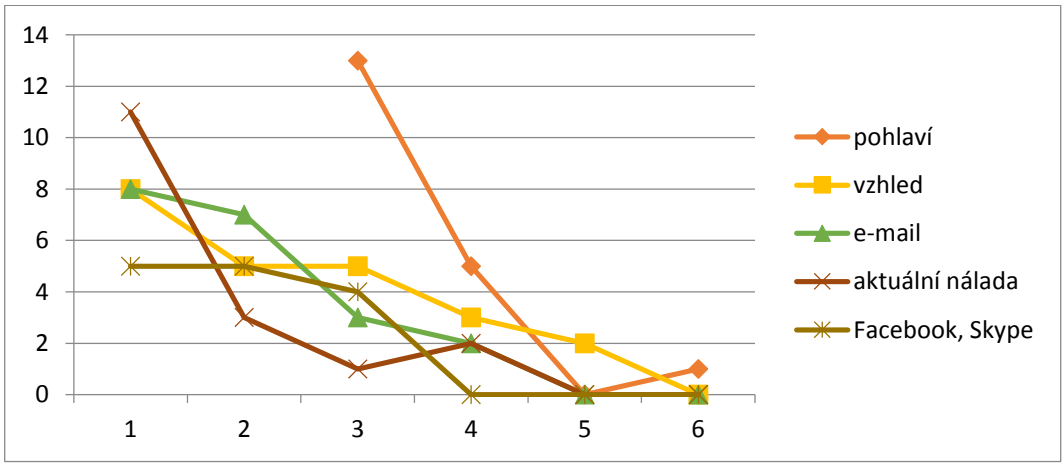
S ohledem na zaujetí dětí v učení je nutné zmínit, že se v dokumentech objevily i nesmyslné otázky (např. Jsi bůh? Znáš mě? Jsi hodná?), kterých ale bylo jen 9 ze všech 1158 otázek, vždy v různých dokumentech. Jejich vliv na aktivitu je

tedy zanedbatelný. Protože málo zastoupené proměnné nemohou být statisticky zpracovány a i vypovídací hodnota v třídění 1. stupně je velmi omezené, jsou otázky zastoupené v méně než 3 % dokumentů z dalšího zpracování vyloučeny.

Při sledování pořadí témat v otázkách se objevily čtyři druhy tendencí, které jsou ilustrovány následujícími grafy. Tyto tendence naznačují funkčnost jednotlivých témat v komunikaci.

a) Otázky pro navázání kontaktu

Komunikace byla zahajována obvykle velmi obecnými dotazy. V dokumentech bylo možné identifikovat témata, která byla používána téměř výhradně pro zahájení komunikace a jejich výskyt na pozdějších místech prudce klesal (viz graf 65 Témata otázek pro zahajování komunikace).



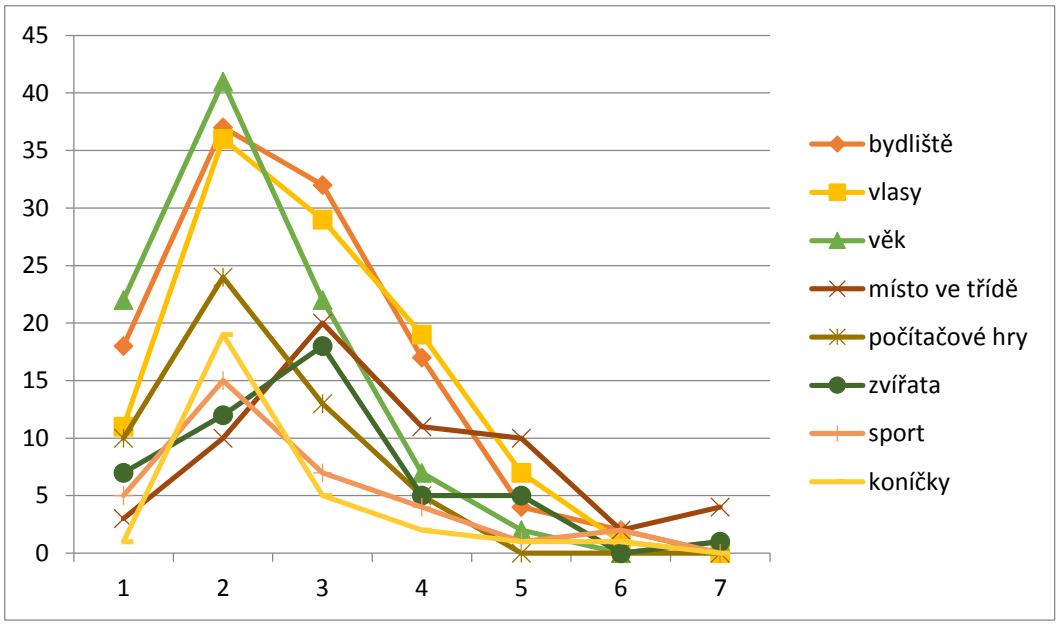
Graf 65 Témata otázek pro zahajování komunikace

Naprosto nesrovnatelně se všemi proměnnými se na prvním místě v dotazech objevovalo pohlaví (ve 219 dokumentech, tj. 61,5 %), na druhém místě to bylo ve výrazně méně dokumentech (33, tj. 9,3 %); obě tyto hodnoty nejsou do grafu zaneseny, aby nedošlo k snížení čitelnosti hodnot ostatních proměnných. Toto výrazné postavení pohlaví může být ovlivněno tím, že dotaz byl ve všech třídách poskytnut jako ukázkový nápad toho, na co se lze ptát. Na druhou stranu spolu s ním byla navrhnuta i druhá otázka na počítačové hry, která se ale mezi průměrnými pořadími objevila až na 7. místě. Vliv navrhnutých otázek tedy není tolik výrazný a postavení proměnné pohlaví spíše vychází z využitelnosti této informace, a to v soutěži i v reálné komunikaci na internetu.

Strmost klesání odpovídá očekávanému využití dotazovaných informací, nejprudší je u již zmiňovaného pohlaví a o řád níž pak u aktuální nálady, která je typickou řečnickou otázkou v písemné komunikaci. Mírně volnější klesání je patrné u e-mailu a profilů v komunikačních službách (jmenovány byly Facebook a Skype), což jsou podobně směřované otázky, jejichž identifikační hodnota je potenciálně poměrně vysoká s ohledem na snadnou dohledatelnost osoby při znalosti jména či přezdívky, která je pro označování komunikujících stran na internetu nezbytná, ale v soutěži byla značně omezená. To podporuje žádaný simulační efekt hry. Poslední zde zahrnutá proměnná je vzhled, kde je klesající tendence, ale nejméně prudká. Vzhled totiž může dobře sloužit jak k rychlé segmentaci komunikujících, tak k upřesnění konkrétní osoby, pokud je využito méně obvyklých charakteristik v cílové skupině.

b) Rychlá segmentace

Nejčastější tendence je na úrovni proměnných, které slouží k rychlému omezení cílové skupiny zjištěním informace, která je specifická pro omezený, ale dost široký okruh spolužáků. Tyto proměnné nejčastěji byly pokládány jako druhé či třetí otázky, v této pozici vždy dosáhly výrazného bodu zlomu, po kterém prudce klesaly, jak ukazuje graf 66 Témata otázek pro rychlé členění.



Graf 66 Témata otázek pro rychlé členění

Charakteristiky menších skupin, které jsou v třídním kolektivu známé, jsou aktuálně hrané počítačové (internetové) hry, zvířata (domácí či oblíbená), sporty a obecně koníčky či kroužky. Jedná se o typické otázky pro rychlé zpřesnění typu jedince prostřednictvím jeho zájmů, které se projevuje nejen v internetové komunikaci. Využití této rychlé segmentace je také vhodným postupem pro dosažení stanoveného cíle hry. Stejné využití je patrné i v případě vlasů, které patří k nejlépe známým a segmentujícím charakteristikám dle vzhledu (např. barvou vlastních očí si nebyly děti jisty, jak ukázalo zúčastněné pozorování).

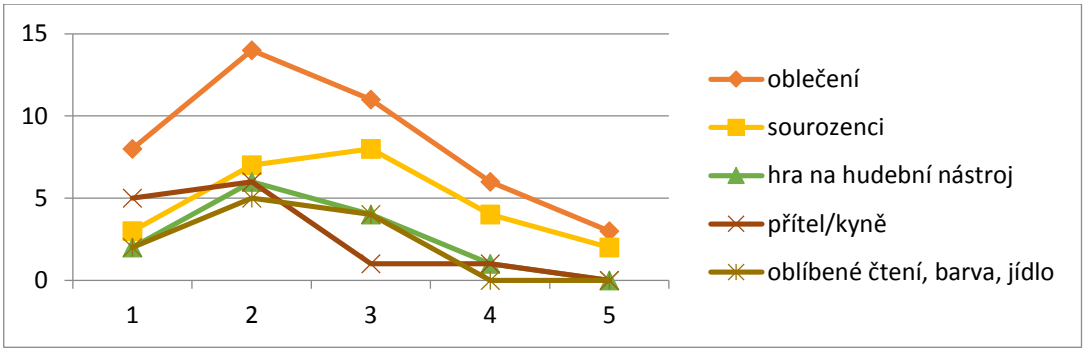
V případě bydliště ve sledovaném kolektivu je také charakteristiku možné zařadit mezi segmentující, protože děti pocházely z několika málo oblastí, kterými se vymezovaly. Pro děti přímo z Poličky bylo častou odpovědí uvedení ulice (nejen názvu obce), proti tomu ty z vesnic jmenovaly jejich názvy. Velmi zvláštní charakteristikou vzhledem ke skupinám v lekci bylo časté zjišťování věku, které v třídním kolektivu má velmi málo identifikující možnosti, přesto se věk objevil v 26,7 % dokumentů. To opět vede k potvrzení simulace prostředí internetu. Na prvních čtyřech místech ve výskytu témat v dokumentech se tak totiž objevilo pohlaví, bydliště a věk, což opět odpovídá internetové komunikaci, kde právě typickým dotazováním na tyto charakteristiky při seznamování (tj. zjišťování, s kým je komunikováno) vznikl akronym A/S/L (Age/Sex/Location).

Poslední proměnná zahrnutá do této skupiny je místo ve třídě, které je již na hranici s následující kategorií, protože jeho tendence je nejmírněji klesající a výskyt je oproti ostatním zde jmenovaným proměnným (průměrné pořadí 2,56) v později položených (průměrné pořadí 3,62). To ukazuje využití otázky spíše pro upřesnění konkrétního člověka, ne tolik segmentaci, i když i pro tyto účely někdy otázka sloužila (např. „*Sedíš u okna?*“ segmentuje cílovou skupinu poměrně dobře, jiné využití bylo typu „*Sedíš v poslední lavici u okna?*“ s jasným odkazem na konkrétní ideu o cíli).

c) Plošně prohlubující otázky

Otázky třetího typu se objevovaly nejčastěji na druhém nebo třetím místě, dominance pořadí ale nebyla tak výrazná jako v předchozích dvou kategoriích (viz graf 67). Slouží opět k segmentaci spíše než ke konkretizaci jedince, ale je výrazně jemnější než v předchozí skupině, protože témata jsou konkrétnější a týkají se

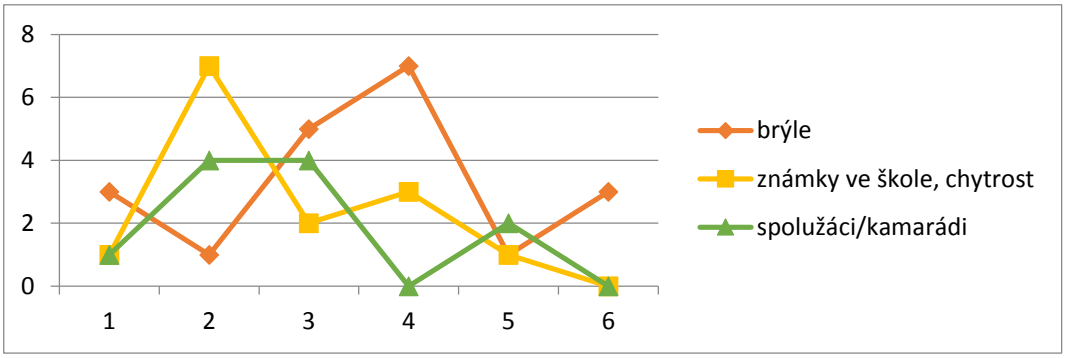
menších skupin. Objevují se proto na místě, kde k detailnějšímu vymezení může dojít. Nejvýraznější křivku má oblečení, které je podobně výrazná charakteristika jako vlasy v předchozí kategorii, ale tím, že není každý den stejné, je při dotazech na něj menší jistota, čímž se proměnná dostává do jiné kategorie.



Graf 67 Témata otázek pro konkrétnější omezení cílové skupiny

d) Otázky specifické pro kolektiv

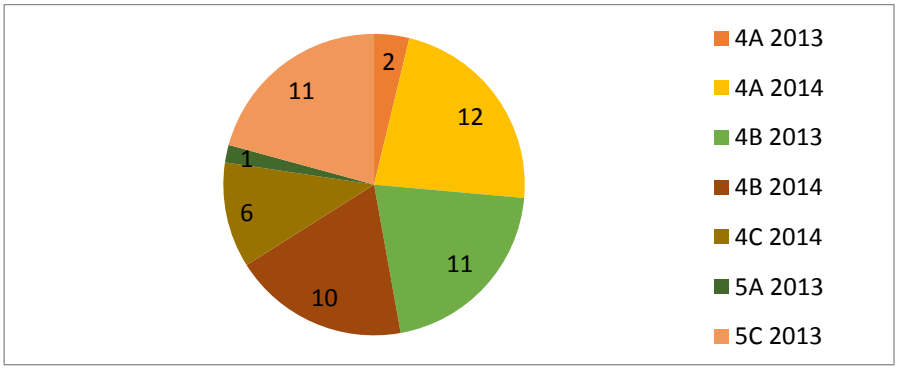
Poslední typ otázek nevykazuje žádnou jednoduchou tendenci jako předchozí kategorie, objevuje se více vrcholů v pořadí výskytu. Jedná se o charakteristiky, které se mohou projevovat jako dobře i špatně identifikující v závislosti na konkrétním kolektivu, např. brýle může nosit jeden i více žáků ve třídě, v případě výběrových tříd je pravděpodobnější, že známky ve škole budou u většiny z nich dobré, dotazy na spolužáky a kamarády jsou opět specifické pro kolektiv a není možné hodnotit kvalitu identifikace při neznalosti sociálního prostředí dětí, může být různá. Proto také vrcholy a propady v pořadí výskytu mohou být ovlivněny ve všech třech zde zařazených proměnných specifiky kolektivu a pro jejich další hodnocení by bylo nutné podrobněji jej poznat.



Graf 68 Témata otázek závislé na kolektivu

Mezi specifickými otázkami si komentář zaslouží málo zastoupené proměnné, které nejsou dále hodnoceny, ale jejich funkce je pravděpodobná pro konkretizaci jedince. Protože směřují právě na jedince, je logický malý výskyt. Odpovídá tomu i průměrné pořadí. Zatímco u kategorizovaných proměnných bylo průměrné pořadí 2,45, v případě málo zastoupených byl průměr 3,14, tedy výrazně vyšší, nicméně 95 % intervaly spolehlivosti se částečně překrývají.

Při zpracování dokumentů se objevilo v 15 % z nich, že žáci se v tématu neomezili na jedinou otázku, ale odpověď rozvíjeli pro získání specifičtější odpovědi, která by jim pomohla omezováním možností identifikovat konkrétního jedince. Jedná se opět o nepřipravený, ale samostatně se objevující efekt pochopení postupu, který funguje i na internetu. Vzhledem k pokrytí jen 54 dokumentů jedenácti sledovanými proměnnými došlo v této části k sloučení témat do pěti širších kategorií. Přestože se tento postup ukazuje jako efektivní pro dosažení stanoveného cíle a bylo by tedy možné předpokládat, že se jedná o postup, na který přijdou starší a tedy zkušenější žáci, tento předpoklad se nepotvrdil, protože byl přítomný v 18,3 % dokumentů ze 4. tříd a 9,09 % dokumentů z 5. tříd. Místo toho se ukázalo, že tento postup byl pravděpodobně opět šířen interaktivitou mezi žáky, protože se neobjevil ve všech třídách srovnatelně často (viz graf 69 Počet dokumentů s více otázkami na stejné téma ve třídách). To je ještě patrnější při zaměření na jednotlivá témata, protože u různých tříd vždy jen jedno z nich převažuje nebo dokonce je zastoupeno jen toto). Statistický test rozdílů nemohl být proveden vzhledem k množství polí v kontingenční tabulce s nulovou hodnotou.



Graf 69 Počet dokumentů s více otázkami na stejné téma ve třídách

9.3.2.2 Identifikace v odpovědích

Při sledování obsahu odpovědí bylo zjišťováno, jestli děti poskytují informace s vysokým potenciálem identifikace nebo naopak. Základním poznatkem ze soutěže, ke kterému směřovala následně i část reflexe, byla právě změna přístupu k poskytování odpovědí na stejnou otázku, tedy aby nebyla dávána konkrétnější odpověď, než je nutná, a pokud se tato nutnost objeví, aby si žák uvědomoval, že reakce může mít důsledek v podobě identifikace jeho osoby někým jiným. Cílem bylo dovést děti k tomu, aby dokázaly odpovídat sice pravdivě, ale současně bezpečně. V reálné komunikaci přes internet, kterou budou v budoucnu chtít vést vážně, je pravda zásadní (např. pokud se budou chtít seznámit s druhým člověkem, nemohou lhát, ale současně není dobré o sobě prozradit informace, které by mohly vést k útoku).

Příklady odpovědí, které jsou pravdivé, ale současně mají nízký potenciál pro identifikaci dotazovaného, dobře ukazuje jedna z vedených komunikací:

> „(…) Kde bydlíš? – V ČR. Kde bydlíš ty? – V Kraji Pardubickém. Kde sedíš? – V lavici. Jaké máš oblečení dnes? – Hezké. Sedíš u okna? – Ne."

V dokumentech bylo možné najít i vyjádření dokládající, že žáci si uvědomují možnost odlišných odpovědí z hlediska identifikace, které přitom budou pravdivou reakcí na stejnou otázku, že úmyslně dávají odpověď ve formě, která k identifikaci nepřispěje:

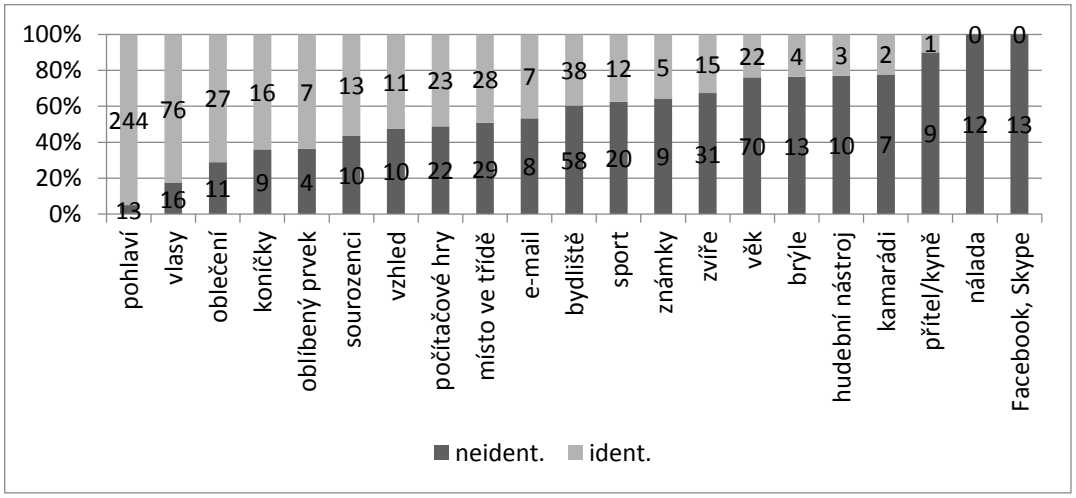
> „(…) Jakou máš barvu vlasů? – Nádhernou. (…) A jaký máš oblečení? – Mám hezké oblečení. To máš za ty vlasy."

Z hlediska typu odpovědí se děti často inspirovaly navzájem, a to jak v kontaktu s tvůrci sdílených dokumentů, tak i interakcí se spolužáky formou diskuze. Proto je možné ve stejných dokumentech najít na stejnou otázku stejné, ale i rozdílné odpovědi. V případě, že druhá odpověď je méně identifikující, takže první straně pomůže méně než jí poskytnutá informace, dojde u uvědomění, které bylo cílem soutěže. Příkladem této komunikace může být:

> „Kde bydlíš? – Na Hegerce a Ty? – V České republice."

Protože cílem byl přístup k odpovědím na aktivitě, v případě, že na jedno téma byly poskytnuty ve stejném dokumentu identifikující i neidentifikující odpovědi (např. při položení stejného dotazu oběma stranami komunikace), byl výsledek hodnocen podle poslední odpovědi k dané proměnné. Témata řazená od těch, která nejčastěji dávala identifikující odpověď, jsou zobrazena v grafu 70.

Protože se dotazované oblasti objevovaly v různém počtu dokumentů, je graf založený na relativních počtech u jednotlivých proměnných.

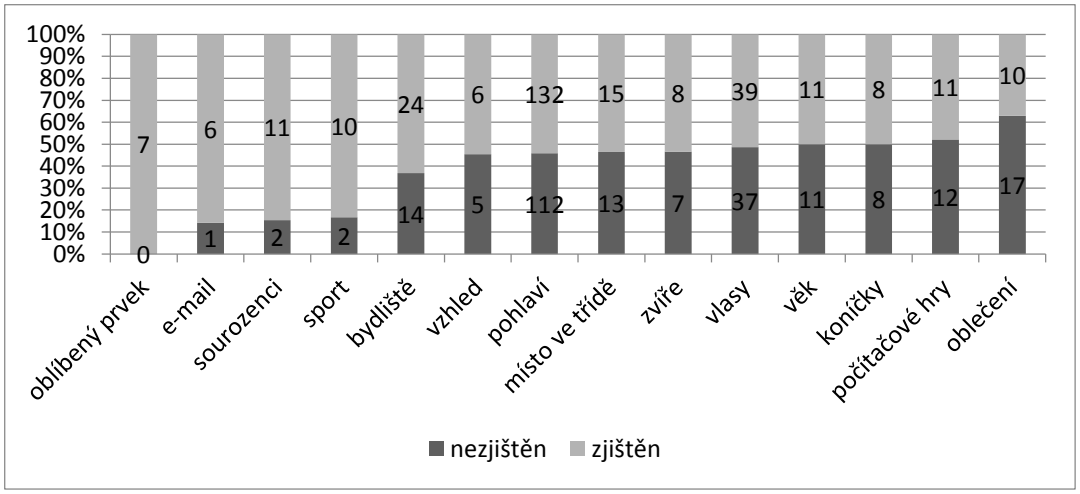


Graf 70 Identifikace v odpovědích dle témat

Identifikující odpovědi byly získány zejména v případě výrazných prvků a obecně známých charakteristik, segmentace skupiny byla tedy z hlediska dotazujícího při využití těchto charakteristik (pohlaví až počítačové hry dle grafu 70) z více než 50 % úspěšná, přitom se jednalo o informace, které mohl velmi dobře bez dalších pomůcek využít k zjištění identity odpovídajícího. V případě místa ve třídě byla často otázka položena velmi konkrétně s cílem potvrzení si zvažované identity, proto se i zde objevilo množství identifikujících odpovědí, přestože se často jednalo jen o odpovědi na otázky zjišťovací. Na druhém pólu škály se objevovaly otázky pro navázání kontaktu (nálada) a směřující na specifická témata (viz s. 249). Právě tato specifičnost často vedla k neidentifikující odpovědi, protože dotázaný reagoval, že se jej daná oblast netýká (např. nemá přítelkyni, nehraje na hudební nástroj apod.).

Při hodnocení, v jakých tématech byly získány identifikující odpovědi, současně dokument ukazuje dosažení cíle v odhalení identity, nejčastěji se objevují témata pro jemnější segmentaci cílové skupiny, dále e-mail, který před vložením zákazu do pravidel často sám o sobě prozradil jméno, následovaly častěji pokládané, ale méně vymezující témata typu sport nebo zvíře. Méně vymezující témata jsou ale většinou blízké 50% úspěšnosti, jsou tedy spíše správnou cestou, která ale ne vždy došla až k výsledku, k tomu mají blíže konkrétnější informace.

Hodnoty proměnných, které byly dostatečně zastoupeny (více než 5 identifikujících odpovědí v dokumentech), přibližuje graf 71.



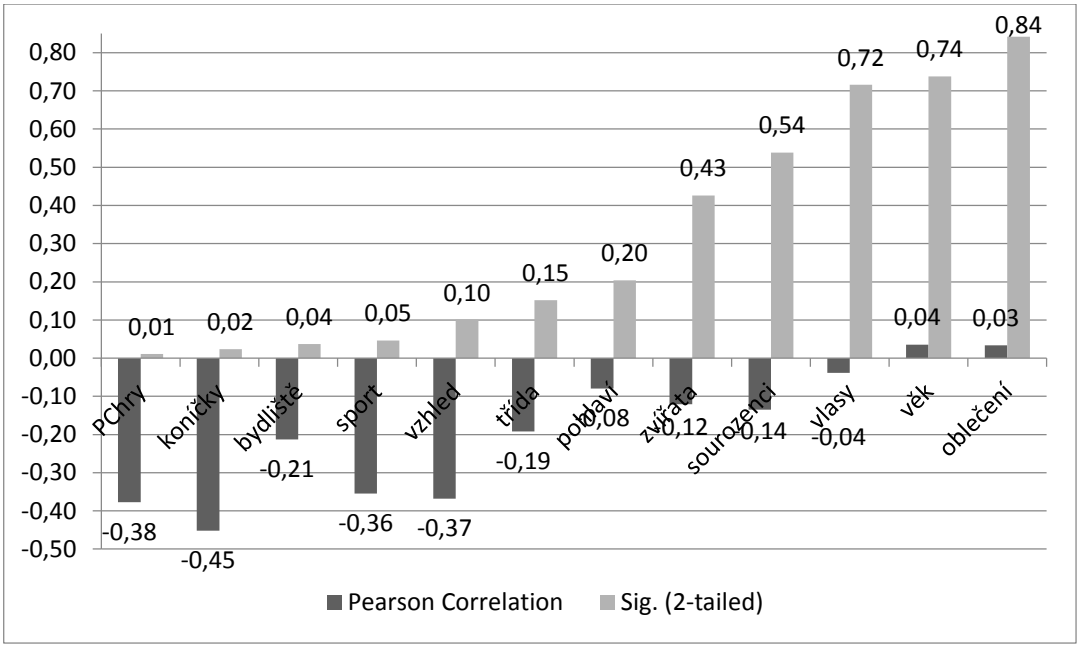
Graf 71 Identifikující témata dle zjištění identity

V rámci hodnocení identifikačního potenciálu poskytnutých odpovědí se z kvalitativního hlediska ukázalo, že žáci jsou v případě některých otázek, se kterými se často setkávají v komunikaci s dospělými, naučeni odpovídat určitou formou a neusilují o odlišné odpovědi pro různé tazatele. To je patrné např. z již popisovaných typů odpovědí na bydliště (viz s. 248). V případě vzhledu se naopak často projevovala kreativita, která mnohdy vedla k nízké možnosti identifikace tázaného, jindy v této proměnné byl vyzdvižen specifický prvek (např. na otázku „*Jaké máš vlasy?*“ byla dána odpověď „*Hodně dlouhé a zrzavo hnědé.*“).

Pro stanovení odpovědí na výzkumné otázky byly sledovaným kritériem korelace pořadí dostatečně zastoupených témat a množství zjištěných identit v dokumentu. Tím bylo zjišťováno, zda téma otevřené později vede k nižší identifikaci subjektu, na základě čehož by bylo možné konstatovat, že postup ve hře zlepšoval poznání v řešené oblasti a tedy simulační hra plní svůj edukační cíl.

Dostatečně zastoupených proměnných ($n > 15$, kdy n je počet případů s validní hodnotou u otázky i odpovědi) pro korelace bylo 12. V grafu 72 jsou zobrazeny hodnoty statistické významnosti i Pearsonova korelačního koeficientu pro každou z těchto proměnných. Korelace potvrzují, že s vyšším pořadím tématu se snižuje míra identifikace u všech proměnných mimo věk a oblečení, kde ale

korelační koeficient je velmi blízko mezní (nulové) hodnoty. Nicméně statisticky významné jsou korelace jen v případě počítačových her, koníčků, bydliště a sportu, ostatní proměnné nedosahují kritické meze.



Graf 72 Korelace pořadí tématu a identifikace odpovědi

9.3.2.3 Specifičnost dokumentů u jedinců a tříd

Jak již bylo řečeno, cílem dokumentové analýzy bylo doplnění výsledků zúčastněného pozorování, které nemohlo poskytnout data k obsahu komunikace v rámci uvědomění si přístupů ke komunikaci na internetu, které zvýší jejich bezpečnost omezením identifikování s využitím poskytnutých digitálních stop.

V případě sledovaných ročníků lze očekávat, že starší děti s více znalostmi budou schopny rychleji psát a podaří se jim proto dosáhnout většího množství otázkových cyklů, ale také využijí svých znalostí k častějšímu dosažení zjištění identity druhé strany komunikace. Oba tyto předpoklady se potvrdily, mezi ročníky byly v obou směrech zjištěny statisticky významné rozdíly. Přestože v ročnících je téměř totožný průměrný počet otázek (4. třída 3,17 a 5. třída 3,39), častěji se vyskytovaly dokumenty s vyšším počtem otázek, průměrná hodnota je ovlivněna extrémními hodnotami i na druhém pólu škály. V případě počtu zjištěných identit jsou rozdíly výraznější, což potvrzují i statistické testy:

- Počet otázek: Pearsonův Chí-Kvadrát 22,403 s p = 0,002, kontingenční koeficient je 0,243;
- Počet zjištěných identit: Pearsonův Chí-Kvadrát 17,285 s p < 0,001, kontingenční koeficient je 0,215.

V rámci ročníků nebyla dále srovnávána jednotlivá témata, protože není možné předpokládat rozdíl ovlivněný věkem, na rozdíl od formy dokumentů a dosažení cíle, bez ohledu na zvolenou strategii. Rozdíly dané znalostmi a zkušenostmi se projevují také na úrovni třídních kolektivů, do nichž jsou děti členěny školou podle studijních výsledků. Statisticky významné rozdíly mezi třídami jsou dalším potvrzením vlivu znalostí na obě proměnné:

- Počet otázek: Pearsonův Chí-Kvadrát 105,668 s p = 0,000, kontingenční koeficient je 0,478 (silný vliv má vyšší počet otázek 5.C);
- Počet zjištěných identit: Pearsonův Chí-Kvadrát 57,292 s p < 0,001, kontingenční koeficient je 0, 372 (výrazněji se lišila 5.B s vyšším počtem zjištěných identit).

Korelační koeficienty jsou v případě tříd vyšší než u ročníků, což ukazuje těsnější vztah mezi sledovanými proměnnými. Projev silnější závislosti počtu otázek a zjištěných identit na třídách ukazuje, že věk není tak silným faktorem, jako spíše právě znalosti problematiky v kolektivu. Protože lekce probíhala formou aktivního učení se silnými prvky interakce mezi žáky během soutěže (ke kterým nedochází napříč ročníky), v případě těchto skupin pro potvrzení vlivu žáků mezi sebou bylo využito statistické porovnání rozdílů nejen na úrovni výsledků, ale také využívaných postupů, tj. používaných otázek v určitém pořadí a identifikačního potenciálu poskytovaných odpovědí.

V případě zjišťování statistické významnosti toho, zda se jednotlivá témata objeví v různých třídách různě často (bez ohledu na pořadí témat nebo možnost identifikace odpovědí) se ukazuje, že výskyt téměř všech proměnných se ve třídách liší. V pořadí od nejtěsnějšího vztahu proměnných to jsou na hladině 1 %: e-mail, bydliště, místo ve třídě, přítel/kyně, počítačové hry, koníčky, vlasy, sport, oblečení, hra na hudební nástroj, Facebook/Skype, spolužáci/kamarádi, věk, zvířata, vzhled, sourozenci a brýle; dále na hladině 5 % ještě oblíbené čtení/barva/jídlo a pohlaví. Statistická významnost se neprojevila jen u nálady a známek ve škole. Vzhledem

k tomuto výsledku je pravděpodobný vliv interakce mezi žáky, protože zástupci ze stejných prostředí v různých kolektivech vykazují různé výsledky, je tedy pravděpodobný právě vliv kolektivu. Pro přísnější hodnocení rozdílů mezi dokumenty je možné testovat nejen výskyt témat, ale také jejich pořadí a kvalitu odpovědí. Z rozdílů mezi skupinami vyplývá, že jen nálada (zahajující otázka) a známky ve škole (možný vliv, že lekce proběhla v rámci školní výuky) představují průřezová témata, která se objevují nezávisle na kolektivu, značná převaha témat se ale objevuje v kolektivech odlišně, což potvrzuje, že děti sdílejí otázky a témata během lekce, takže se přenáší zjištění, která témata jsou klíčová pro pochopení problému a jeho řešení. Výsledek potvrzuje zjištění ze zúčastněného pozorování.

Statistické testování rozdílů mezi jednotlivými žáky nebylo možné vzhledem k malým množstvím případů. I jednotliví žáci byli poměrně kreativní v hledání různých tematických oblastí, příliš se neopakovali, spíše zkoušeli, která otázka se osvědčí a tu případně použili opakovaně. Výskyt těchto opakovaných použití je příliš malý pro vyhodnocování statisticky podložených závěrů.

9.3.3 Závěry dokumentové analýzy

Dokumentová analýza potvrdila výsledky zúčastněného pozorování. Neposkytla sice data pro triangulaci zjištění pro celou lekci, ale jen jednu ze tří částí, nicméně jednalo se o část zásadní, kdy cílem bylo dovést děti k pochopení principů zvýšení bezpečnosti komunikace přes internet produkcí méně identifikujících digitálních stop, aniž by se musely vzdát žádaných služeb. V rámci dokumentové analýzy bylo ověřováno několik faktorů zjištěných pozorováním, které odpovídají třem stanoveným výzkumným otázkám:

- aktivní učení spočívající především v interaktivitě mezi žáky pro vlastní formování klíčových poznatků, na kterém staví celá lekce svou funkcionalitu a jehož fungování je nezbytné pro smysluplnost hodnocení dalších závěrů z dokumentové analýzy,
- simulační efekt hry (přistoupení dětí na paralelu s reálnou komunikací na internetu), který je základním předpokladem přenosu poznatků z lekce do budoucí komunikace na internetu,

– dosažení edukačního cíle hry, tedy skutečné poznání pravidel tvorby digitálních stop v internetové komunikaci a schopnost jich využít.

Aby bylo možné činit z analýzy závěry, je klíčovým předpokladem, že získané dokumenty opravdu tvoří celek, tj. že lekce nevedla každou třídu k jiným výsledkům. V tomto směru dokumenty potvrdily, že navzdory rozdílům v charakteristikách tříd na soutěž všechny reagovaly podobně, protože vykazují podobné společné charakteristiky typu počet otázek, počet znám tě apod. Přestože byly zjištěny statisticky významné rozdíly, intervaly spolehlivosti se z výrazné části překrývají. Tím se ukazuje, že výsledný efekt lekce byl pro všechny třídy podobný, i když proces jeho dosažení se lišil. To odpovídá principům aktivního učení[438], kdy lektor je facilitátorem, zajišťuje průběh procesu, který je ale formován samotnými žáky podle jejich individuálních potřeb.

Samotná hra je žáky brána vážně, jak ukazuje využití proměnných, které jsou smysluplné pro zjištění identity (až na výjimky v řádu promile), a také identifikovaných strategií k stanovenému cíli. Dotazované informace jsou různé, proto byly kódovány do 34 proměnných, 38,42 % z nich ale bylo zastoupeno minimálně, byly využity spíše pro závěr specifikace identity pro zjištění prvku, který jednotlivce odlišuje. I u silněji zastoupených proměnných byly omezené možnosti statistického testování, přestože analýzou procházelo 1158 cyklů dotazování neopakujících se ve stejném dokumentu. Bylo tak možné hodnotit vliv interakce pomocí rozdílů mezi skupinami na úrovni tříd, ne již mezi jednotlivými žáky pro ověření formování strategie vlivem interakce s ostatními k dosažení cíle. Při srovnání průběhu komunikace mezi jednotlivými třídami byly zjištěny statisticky významné rozdíly na úrovni výskytu podobných témat. Při přísnějším hodnocením na úrovni pořadí a kvalitě odpovědi je již významných rozdílů výrazně méně, což může z hlediska interakce být důsledkem toho, že dokumenty vznikaly v různý okamžik průběhu aktivity. Témata i kvalita odpovědí tedy mohla být do dokumentů přenesena po uskutečnění přenosu, ke kterému ale došlo v různé fázi tvorby dokumentů. Podrobněji rozdíly mezi skupinami vymezuje kap. 9.3.2.3. Celkově je možné v rámci první výzkumné otázky potvrdit funkčnost prvků aktivního učení, které se projevily i v rámci zúčastněného pozorování.

[438] Viz kap. 8.1.2 Aktivní učení a model E-U-R

V návaznosti na formu aktivity, která simuluje reálné prostředí, je důležité vyhodnotit, zda si informace v simulační a internetové komunikaci odpovídají. V rámci výzkumů internetové aktivity dětí je zjišťováno, jaké informace jsou sdíleny, přitom se může jednat o komunikaci mezi konkrétními subjekty nebo zveřejnění informace. Lze tedy zhodnotit, zda si odpovídá frekvence výskytu jednotlivých typů informací, a to především pokud jsou poskytnuty tak, že mohou být využity pro identifikaci. Ze srovnání s dvěma výzkumy popisovanými v kap. 6.1 v tabulce 9 je patrné, že komparace není snadná, protože se předchozí výzkumy silně rozchází v zjištěných hodnotách. Proto i srovnání s dokumentovou analýzou je možné jen omezeně, s vědomím specifik daných pravidly hry.

Tabulka 9 Srovnání osobních informací

	Half of the children[439]	Kopecký[440] (zveřejnění; na žádost)	Analýza (výskyt; identifikující)[441]
jméno a příjmení	85 %	80,4 %; 48,1 %	zakázáno
e-mail	nepublikováno	65,8 %; 25,1 %	45,5 %; 16,3 %[442]
jiná intern. komunikace	nepublikováno	21,7 %; 15,1 %[443]	3,9 %; 0 %
bydliště	13 %		30,9 %; 10,7 %
škola	44 %	15,9 %; 5,2 %	8,15 %; 4,5 %[444]
vzhled	71 %[445]	58,4 %; 21,8 %[446]	28,9 %; 21,4 %[447]

Pokud pomineme jméno a příjmení, které byly od počátku zakázány, velmi rychle děti pro jejich zjištění použily e-maily, tj. základní kontaktní internetové údaje, proto i tyto byly pro udržení soutěže od druhého běhu zakázány. Jiné komunikační služby jsou vhodnou informací na internetu, kde lze jejich pomocí dohledat konkrétní profil, v soutěži je ale jejich využití minimální, proto je pochopitelný rozdíl mezi hodnotami. Dalším klíčovým kontaktem je bydliště, které bylo žádáno častěji, než prokazují uvedená výzkumná šetření, což může být způsobeno větším nátlakem na identifikující dotazy. Stále se však jedná o často řešené informace, ať už v simulaci nebo v reálné komunikaci doložené výzkumy.

[439] Polovina dětí reaguje na internetu (...) 2010
[440] KOPECKÝ 2012
[441] Tyto a další informace v dokumentech jsou podrobněji řešeny v kap. 9.3.2.1 a 9.3.2.2
[442] Hodnoty platné jen pro 1. třídu, pak tato informace v dokumentech zakázána
[443] Jen Instant Messengery
[444] Např. kroužek, koníček
[445] Fotografie sebe a přátel
[446] Fotografie obličeje
[447] Vlasy, tj. nejčastěji zastoupený prvek vzhledu

V případě komunikace přes internet je škola dobrou informací pro určení lokace (bydliště může jedinec pravděpodobněji odmítnout poskytnout), ale v soutěži je bezvýznamná, proto k lokaci slouží právě bydliště, u kterého se hodnoty blíží výzkumu z roku 2010. Alternativní místo výskytu může představovat kroužek či koníček, u kterých jsou hodnoty porovnatelné s druhým z uvedených výzkumů.

Pohlaví, oblečení a vlasy (nejvýraznější vzhledové charakteristiky) společně přibližují vzhled pomocí textu, podobně jako fotka obrazem, i zde je tedy patrná souvislost s osobními informacemi, které jsou podle výzkumů velmi často sdíleny v komunikaci dětí přes internet. Velmi zajímavé je množství dotazů na věk, který souvisí se vzhledem, protože simulace probíhala ve třídách, kde jsou děti v podstatě stejně staré, takže jim odpověď nemohla dát dobré vodítko pro identifikaci druhé strany. Je tedy možné, že tak častý výskyt dotazu je opět pod vlivem toho, jak často se s ním setkávají na internetu.

S ohledem na problematickou možnost srovnání dokumentové analýzy s předchozími výzkumy je vypovídací hodnota paralel diskutabilní. Řádově jsou sice informace srovnatelné, je ale otázkou, nakolik využitelnost informací na internetu a v soutěži ovlivňuje výsledky. Pro podporu fungování simulačního efektu ve hře je ale možné využít jazykové projevy žáků, které se objevily v dokumentech, ale je možné je očekávat spíše v prostředí internetu. Patří sem např. použití internetových akronymů v dokumentech (např. OMG). Navzdory tomu, že dokumenty vznikly na lekci zprostředkované školou, se také v jednom z nich objevil náznak šikany přes komunikaci („*[jméno] smrdíš!“).*

Simulační efekt je těžko prokazatelný, protože výskyt informací není možné srovnávat s jejich přesným výskytem na internetu. Nicméně typy často použitých informací, stejně jako specifické jazykové projevy, výrazně podporují jeho funkčnost. S vědomím diskutovaných problémů je proto možné pro druhou výzkumnou otázku vytvořit závěr, že se skutečně jedná o simulaci a je možný přenos získaných zkušeností do reálného života v internetovém prostředí.

K ověření, zda byly získány nové poznatky k přenosu do internetové komunikace, vedla třetí výzkumná otázka. K porovnání posunu od výchozího stavu bylo využito vztahu mezi pořadím tématu a potenciálu identifikace odpovědí. Z výsledků vyplývá statisticky významný rozdíl v žádoucím směru u několika dostatečně zastoupených proměnných. Tuto tendenci má převážná většina

proměnných, která ale není dostatečně významná. Ty, které ji nevykazují, jsou velmi blízké mezní hodnotě. V rámci poslední výzkumné otázky je tedy potvrzeno, že aktivita splnila svůj výukový cíl.

Přestože odpovědi na výzkumné otázky, především druhé, mají svá omezení, celkově výsledky podporují poznatky zúčastněného pozorování, triangulace dat byla v této fázi úspěšná. Poslední příspěvek k potvrzení je kvalitativní evaluace průběhu a výsledků lekce dotčenými subjekty, které bylo částí dále realizovaných rozhovorů (druhou částí byl obecný názor na vzdělávání v knihovně o digitálních stopách).

9.4 Polostrukturované rozhovory o vzdělávání v knihovně k bezpečnosti digitálních stop

Existují různé názory na to, zda by knihovna měla vzdělávat o bezpečnosti digitálních stop, přičemž se objevují také přesvědčení, jak na to pohlíží ostatní klíčové osoby nebo zástupci primárně i sekundárně dotčených cílových skupin. Tato přesvědčení ale velmi často vychází se subjektivního pocitu nežli z výzkumného šetření. Proto byly provedeny kvalitativní rozhovory, jejichž cílem nemohlo být zobecnitelné zjištění, ale možný pohled různých subjektů na knihovny jako instituce vzdělávající o bezpečnosti digitálních stop. Výběr dotazovaných byl účelový pro zachycení zástupců všech identifikovaných klíčových skupin ve vztahu k lekcím tohoto typu pro děti, jedná se tedy o přístup nazývaný 360° zpětná vazba. Byl zjišťován i obecný postoj k tomu, aby knihovna vzdělávala o informační bezpečnosti a faktory, které k němu vedly, včetně vlivu realizované lekce. Rozhovory tedy pokrývají obecný přístup dotazovaných k problematice i jeho praktickou aplikaci díky realizované lekci. Právě tato část rozhovorů je podstatnou součástí akčního výzkumu, protože umožňuje potvrzení vlivu lekce na děti, ale i další osoby, udržitelnost výsledku akčního výzkumu a, dle Kirkpatrickova modelu, dlouhodobý efekt lekce jak z pohledu změny chování žáka (3. úroveň), tak i návazně důsledky pro okolí dětí (4. úroveň).

9.4.1 Metodologie šetření

Kvalitativní polostrukturované rozhovory byly zvoleny jako poslední výzkumná metoda, protože nejlépe odpovídá cíli, který byl považován za nezbytný pro kompletní akční výzkum vzdělávání i pro zjištění postojů a jejich zdůvodnění, které není možné zjistit jinak než kvalitativně[448]. Rozhovory se jevily jako nejvhodnější přístup, protože nebyl zjišťován jen současný stav, ale i minulost a vnitřní názory k tématu, a protože mezi subjekty dotazování existují mocenské vztahy vylučující skupinový sběr dat.

Cílem výzkumu tedy bylo ukázat deklarovaný i skutečný postoj zástupců klíčových skupin k otázce, zda by knihovna měla vzdělávat o bezpečnosti digitálních stop. Dosažením tohoto cíle jsou pak identifikovány argumenty, proč ano či ne, které je možné použít při prosazování této služby knihoven. Pro dosažení tohoto cíle byly formulovány čtyři dílčí výzkumné otázky:

VO1: Jaké pozitivní důvody a důsledky realizace lekcí v knihovnách o bezpečnosti digitálních stop si dotazovaní uvědomují?

VO2: Jak hodnotí dotazovaní vliv realizované lekce v knihovně o bezpečnosti digitálních stop?

VO3: Jaké možné bariéry realizace lekcí v knihovnách o bezpečnosti digitálních stop, které mohou omezit efektivnost nebo zcela zamezit jejich realizovatelnosti, dotazovaní identifikují?

VO4: Jaká řešení bariér realizace lekcí v knihovnách o bezpečnosti digitálních stop respondenti na základě vlastní zkušenosti navrhují?

Výzkumné otázky se snaží zachytit kombinaci pozitivních a negativních aspektů (předpokladů a důsledků) lekce s obecným a konkrétním (na lekci založeným) postojem k lekcím v knihovnách o bezpečnosti digitálních stop. Příloha 3.2 obsahuje soubor otázek, které byly stanoveny pro polostrukturovaný rozhovor a přizpůsobovány konkrétním dotazovaným (formou a nepokládáním otázek, na které dotazovaní nemohli znát odpověď, např. žákyně nemělo smysl se ptát na názor na připravenost absolventů oboru Informační studia a knihovnictví).

Protože byly jasně dány některé klíčové subjekty pro výzkum, jejichž postavení je jedinečné, ale také odlišné, byl zvolen účelový výběr (maximálně

[448] PICKARD 2013

variantní případy) i právě metoda rozhovorů, která umožňuje zohlednit specifika jednotlivých dotazovaných. Vzhledem k realizované lekci i obecněji lekcím pro děti se formují tři skupiny, kterých se dotýkají a jejichž názory jsou proto z hlediska šetření podstatné: knihovna jako realizátor, který do lekcí investuje čas, materiál a lidské zdroje, škola, která je prostředníkem pro uskutečnění lekce a která zajišťuje přítomnost primární cílové skupiny vzdělávání v době výuky a musí být tedy schopná obhájit smysl této spolupráce s knihovnou, a nakonec cílová skupina vzdělávání, tj. děti a sekundárně i jejich okolí, především rodina, jejíž efektivní poučení je smyslem lekce. Vzniklo celkem šest rozhovorů vždy se dvěma různými zástupci jmenovaných skupin:

- knihovna: ředitel knihovny rozhodující o přidělení zdrojů i pro vzdělávání a knihovnice vzdělávající přibližně 3 roky děti od předškolního věku po ukončení sekundárního vzdělávání na systematické a opakované úrovni (přes spolupracující školy každý ročník min. jednou za rok), knihovnice lektoruje i semináře o vzdělávání v knihovnách pro knihovníky,

- škola: zástupkyně ředitele školy (po realizaci rozhovoru jmenovaná ředitelkou), kde všechny 4. a 5. třídy prošly zkoumanou lekcí v knihovně, a učitelka, která na této lekci se svou třídou byla; vzhledem k pracovním pozicím je nutné zdůraznit, že většina zjištění týkajících se školy platí pro 1. stupeň, jen omezeně i pro 2.

- rodina: žákyně, která se lekce zúčastnila, a její matka, která pracuje jako úřednice na Městském úřadě v Poličce a má přímé informace o jednání mezi zřizovatelem a vedením knihovny; pro dodržení etiky výzkumu rozhovor s matkou a dcerou probíhal současně.

Spojení dotazovaných s realizovanou lekcí, které bylo podrobněji popsáno v kap. 9.1, je podstatné proto, že rozhovory jsou součástí akčního výzkumu. Dalším kritériem výběru respondentů je jejich pozitivní vztah k tématu, který sice může mít vliv na výsledky, ale je nezbytným předpokladem pro formulaci akce v cyklu akčního výzkumu (viz kap. 9). Názory různých nedotazovaných klíčových skupin jsou částečně pokryty dotazy na známé reakce přes vybraný subjekt rozhovorů, zásadní poznatky jsou ale spíše najít argumenty a možnosti k tomu, co je možné realizovat a co je efektivní.

Rozhovory byly realizovány v létě a na podzim 2013, tj. několik týdnů až měsíců po lekci, která umožňovala reakci. Knihovnice byla dotazována po prvních čtyřech cyklech lekce, ředitel knihovny a obě zástupkyně školy po pěti, přičemž učitelka čtyři týdny po lekci s její třídou, žákyně a její matka s odstupem 24 týdnů (rozhovory byly odloženy kvůli letním prázdninám a podruhé kvůli volbám na úřadě, kde je matka zaměstnána). Časový odstup slouží k odbourání okamžitého dojmu ve prospěch dlouhodobého vlivu (Kirkpatrick[449] doporučuje 3 měsíce). Jedná se v každé kategorii o zastoupení přímého účastníka lekce a nadřazené pozice. Rozhovory lze tedy považovat za výsledky 3. a 4. úrovně Kirkpatrickova modelu. Pro 4. úroveň je interval odstupu na spodní hranici, ale s ohledem na organizaci a zájmy dotazovaných byl snížen na stejnou délku pro všechny.

Pro dodržení etiky výzkumu byl dotazovanými udělen poučený souhlas (formulář je uveden v příloze 3). Vzhledem ke specifičnosti subjektů byly dopředu výsledky rozhovorů sjednány jako neanonymní, ale pro ochranu dotazovaných je omezena identifikace označováním v textu výhradně zástupnými pojmenováními (ředitel, knihovnice, zástupkyně, učitelka, matka a žákyně). Pro přesný záznam rozhovorů vznikly videozáznamy[450], z nich pak byly vytvořeny přepisy, které byly poskytnuty dotázaným k autorizaci a vyznačení úseků, které měly být ze zpracování vyřazeny pro ochranu dotazovaného nebo jeho okolí. Výsledky rozhovoru byly opět autorizovány dotazovanými ve snaze předejít špatné interpretaci jejich sdělení.

Analýza probíhala otevřeným kódováním, které představuje nejčastější a univerzální přístup k analýze kvalitativních dat[451]. Tento postup umožňuje detailní práci s textem i možnost zjištění významů, které nemusí být ihned zřejmé. Postup byl metodou papír a tužka[452] a techniky *vyložení karet* a konstantní komparace[453], zvláštní software pro zpracování nebyl použit. Celkem bylo zpracováno 5 hodin 2 minuty 26 vteřin záznamů, tj. 136 stran přepisů. Při otevřeném kódování vzniklo 503 kódů, které byly následně rozděleny do 52 kategorií (6 okruhů):

1) Úvod: vymezení digitálních stop; regulace internetu pro bezpečnost; názory na knihovnu; spolupráce školy a knihovny; spolupráce školy a dalších organizací.

[449] KIRKPATRICK 1971
[450] Vliv na dotázané by vzhledem k běžnosti použití neměl být velký – viz CHRÁSKA 2007, s. 184
[451] ŠVAŘÍČEK 2007, s. 211
[452] ŠVAŘÍČEK 2007, s. 213
[453] ŠVAŘÍČEK 2007, s. 223-227

2) Knihovna: poptávka po lekci; zavedení řešení digitálních stop do knihovny; předpoklady knihovny pro řešení digitálních stop; příprava knihovníků na lektorování; požadavky na osobu lektora; příprava knihovníků na lektorování o DS; vzdělávací schopnosti knihovny; možnost alternativy knihovny; zvýšení hodnoty knihovny.

3) Škola: důvody zájmu školy o lekci o digitálních stopách; vysvětlení lekce o digitálních stopách škole; důvody vzdělávání učitelů; přínos řešení digitálních stop ve škole i knihovně současně; řešení digitálních stop ve škole; mínusy školy proti knihovnám; obsah lekce jako školní látka; zahájení koncepčního řešení; forma lekce v knihovně; vliv zkušeností s lekcemi.

4) Rodina: postoje dětí k digitálním stopám v lekcích knihovny; názor rodičů na vzdělávání dětí o digitálních stopách; obecné použití internetu (bez omezení na bezpečnost); znalost práce s digitálními stopami; zkušenost s digitálními stopami (bezpečnostní problém); řešení digitálních stop v rodině; potřeba vzdělávání veřejnosti; potřeba vzdělávání rodičů; informální vzdělávání o digitálních stopách; sebeřízené vzdělávání o digitálních stopách; reakce rodičů na lekci pro ně; reakce rodičů při budování postavení knihovny.

5) Obsah a forma lekce: předmět sdělení (jádro lekce); formát obsahu; děti – forma; děti – obsah; učitelé; veřejnost.

6) Evaluace realizované lekce: průběh; chování po lekci[454]; chování a dílčí poznatky; celkové výsledky[455]; výsledky – rodina; výsledky – škola; lekce bez změny (spokojenost); rozšíření lekce pro jiné ročníky; další možné změny; zájem o navazující lekce.

Dále jsou popsány induktivně zpracované výsledky z kvalitativního šetření rozčleněné podle právě uvedené kategorizace do šesti kapitol.

[454] Ve smyslu 3. úrovně Kirkpatrickova modelu
[455] Ve smyslu 4. úrovně Kirkpatrickova modelu

9.4.2 Výsledky výzkumu

Na základě kategorií vzniklých v analýze rozhovorů jsou dále popsány názory respondentů, které vychází z jejich přesvědčení, ale i ze zkušenosti, a to jak s digitálními stopami samotnými, tak i lekcí v knihovně.

Nejdříve je pozornost věnována kontextu dalších zjištění, základem je vlastní vnímání pojmu digitální stopa, protože to vymezuje uvažování ostatních kategorií. Vzdělávání představuje jednu z mediačních strategií, proto do úvodní části patří komentáře k ostatním možnostem, které by měly být využity paralelně s aktivní mediací. Pro přesnější vymezení prostředí výzkumu slouží vyjádření názoru na knihovnu a její spolupráci se školou pro vzdělávání dětí, které zastávají sami dotazovaní nebo lidé v jejich okolí.

Následně je pozornost zaměřena na samotnou knihovnu, od jejích výchozích možností pro realizaci lekcí o bezpečnosti digitálních stop, až po důsledky, které jí přijetí či nepřijetí této funkce přinese. Stranou nezůstává škola podporující vzdělávání dětí knihovnou. Vyzdviženy jsou klíčové okamžiky, které ovlivnily přijetí lekcí, vč. možnosti řešení tématu přímo školou. Navazuje sféra rodiny, tedy primární a sekundární cílové skupiny. Kromě přístupu k vzdělávání dětí je popsáno řízení digitálních stop v rodině na úrovni znalostí a zkušeností, na což navazuje potřeba vzdělávání dospělých i názory dotazovaných na přijetí nabídky vzdělávání o bezpečnosti digitálních stop knihovnou pro jejich potřeby.

Pro všechny subjekty je základem konkretizace náplně lekcí. Protože není možné oddělit ji pro jednotlivé skupiny, protože se jedná spíše o různou úroveň stejného s vyzdvižením specifik, je obsahová náplň pro všechny zařazena jako samostatná kapitola s možnostmi srovnání přístupů. Evaluace lekce v akčním výzkumu je zařazena na závěr, přestože navazuje na předchozí dvě šetření, protože se jedná o rozšíření a zacílení na specifickou situaci všech předchozích uvedených názorů, v jejichž kontextu je nutné evaluaci lekce vnímat.

9.4.2.1 Kontext názorů

Termín digitální stopy byl dotazovanými definován poměrně jednotně, jako jakýkoli digitální záznam, bez ohledu na zařízení, které bylo využito k jeho vzniku, tím může být např. digitální fotoaparát. Digitální stopy nejsou vnímány na úrovni

určité obsahové náplně, ale spíše ve formě zaznamenané informace, přičemž vznik digitálních stop je v současné společnosti nevyhnutelný. Z toho vyplývá přesvědčení, že téma se týká všech, na druhou stranu nelze omezovat problematiku na něco výhradně negativního, protože existuje možnost pozitivní digitální stopy. Z hlediska formy se již omezení v definicích někdy objevily, a to na prostředí internetu či webu, přestože digitální stopa může vznikat i na počítači nepřipojeném do sítě (např. dočasné soubory). Mezi příklady formátů byly jmenovány jen aktivní digitální stopy, ale tvořené člověkem, o kterém vypovídají, i někým jiným, přičemž někdy je jejich vypovídající hodnota podle matky až překvapivá[456]. Ve vyjádření ředitele knihovny se objevilo přesvědčení, že v oblasti praktického vzdělávání v knihovnách není vhodné operovat s termínem digitální stopy, protože se jedná o akademické označení, ostatní dotazovaní ale toto nepotvrdili, spíše naopak. Nicméně tento názor vedl ředitele k využívání označení informační bezpečnost spíše než bezpečnost digitálních stop, ale výslovně ujistil, že jej používá primárně v kontextu významu tohoto pojmu.

Vedle vzdělávání se mezi zmiňovanými mediačními opatřeními objevilo nastavení zákonných pravidel, protože řešení na nižších úrovních je v současnosti omezené[457]. Přestože jsou vnímána omezení při vzniku právních aktů (viz kap. 3.1) je jejich role považována za zásadní, a to jak pro represivní řešení incidentů, tak nastavení hranic společensky správného chování na internetu. Matka zdůraznila přísnost zákonů především u krádeže identity kvůli jejím negativním důsledkům i v situaci, kdy se ji podaří řešit. Z vyjádření je evidentní, že tento problém ji oslovil a představoval by pro ni lákavý obsah v nabídce vzdělávání[458].

Protože se má jednat o pravidla na úrovni celé společnosti, je akceptován pozitivní přínos nadnárodních organizací (Evropská unie), které mohou prosadit vznik řešení i ve státech, které problematice věnují omezenou pozornost. Stanovení pravidel chování v zákonech představuje formu kultivace prostředí, která je

[456] Matka: „hodně zjistím třeba ze zakládacích listin různých právnických osob, zjistím hodně o těch fyzických osobách, což mě až překvapuje někdy“

[457] Ředitel: „Protože většina rodičů a většina učitelů, což jsou ty dvě jako klíčový autority, který (…) můžou, nebo by měly třeba dítě kontrolovat, (…) se tomu jako větším způsobem nezabývá.“

[458] Matka: „pořád člověk jako se může, i když se mu ten život ztíží, tak se může nějak ubránit, i kdyby ten někdo něco za něj chtěl vykonat, nebo vykonal, jo, ať už by třeba nadělal někdo za Vás dluhy, když to teda řeknu jenom takhle hodně… a nebo že tvrdil někde nějaký věci, který jsou trestný třeba, tak pořád si myslím, že to co tady chybí, s tímhle fenoménem, je trest za to ukradení. A teda tvrdej, no, naprosto nekompromisní.“

vnímána jako klíčová po příchodu jakékoli technologie. Je logické, že se vyvíjí, ale nelze rezignovat na jejich nastavení. Kultivační role je vnímána jako zásadní, protože nespočívá jen v dílčích úpravách, jak je v současnosti časté, ale v zavedení hodnot. Přitom se aktuálně nacházíme ve zlomovém prostředí:

> Ředitel: „je podle mě dobrý si uvědomit, že to, co se děje teď, (…) velmi silně ovlivní to chování internetu těch lidí, který v budoucnu budou kontrolovat. Přirozeně. Protože už na tom Facebooku a na těch sociálních sítích budou, protože, protože dorostou."

Pro další řešení tématu je nutné popsat kontext, do kterého mají být lekce začleněny. Knihovny jsou stále vnímány jako instituce reprezentující hodnoty považované za podstatné, služby jsou ale vnímány omezeně, spíše jen na půjčování knih, což vyjádřila i učitelka, která s třídou navštěvuje lekce v knihovně. To vede k tomu, že veřejnost často necítí potřebu knihovnu navštěvovat, takže lekce slouží i jako osvěta, co vlastně knihovna je, protože rodiče ji dětem ne vždy zprostředkují. Osvěta je vnímána jako výrazně vhodnější ve srovnání s předchozí zkušeností školy ve stejné knihovně v podobě tradičního představení instituce[459].

V době realizace rozhovorů knihovna spolupracovala se školskými institucemi od mateřské školy po gymnázium[460], tj. vzdělávala děti ve věku přibližně rok a půl až osmnáct let. K tomu byl využit úvazek o velikosti 0,6, což je výrazná část ve sledované knihovně[461]. Ředitel zdůrazňuje specifičnost tohoto přístupu, přičemž za vhodné by považoval nastavení spolupráce škol a knihoven ve vzdělávání ze strany ministerstva, ale až v okamžiku, kdy na to knihovny budou především personálně připraveny, a s nezbytným vysvětlením nastavení spolupráce jejím realizátorům, které je ze zkušenosti problémem[462].

---

[459] Zástupkyně: „to byly hodiny, kdy navštěvovaly jednotlivý oddělení knihovny, aby se naučily do té knihovny chodit, dostávaly přihlášky a… aby zvýšily vlastně taky návštěvnost dětí v knihovně. (…) když dřív to měla právě ta paní, byla starší samozřejmě, a tak to bylo spíš formou takového frontálního vystoupení, kdy jim ukázala knížky, nějaký obsah jim řekla, ale takový ty interaktivní prvky, (…) takovou tu hravou metodu, to prostě nebyla schopná, ochotná… Nevím, neměla to v sobě, no. Takže tohle je opravdu pestřejší a bohatší, paní učitelky mají výběr."

[460] Knihovnice: „s velkou poličskou základní školou, s osmiletým gymnáziem, se střední obchodní školou služeb, což znamená kosmetičky, kadeřnice, obchodníci, s mateřskými školkami a s mateřským centrem"

[461] Knihovnice: „v městské knihovně, která má 6 zaměstnanců. (…) úvazek na to informační vzdělávání tam byl uměle vytvořen, byl to úvazek navíc, ale i tak já to mám zhruba na 0,6 úvazku, se věnuju informačnímu vzdělávání a na 0,4 takové té běžné knihovnické práci."

[462] Ředitel: „neexistuje žádná jakoby hromadná iniciativa, která by, která by o tomhle se vůbec nemluví na úrovni ministerstev… (…) Pokud by nastala takováhle diskuze na nějaké vyšší úrovni, tak si myslím, že pokud by byla podaná nějak jako lidsky, což se ne vždy jako bejvá. Problém jako veškerých velkých koncepcí je, že je neumíme vysvětlit těm lidem, který je realizujou… (…) tohle může nastat ve chvíli, kdy ty knihovny budou připravený tohle to, tohle to dělat, což zatím nejsou.

Tradice spolupráce s Masarykovou základní školou byla přibližně tříletá, 1. třídy chodí do knihovny na pasování na čtenáře, lekcí se účastní od 2. třídy, kdy již umí číst, třídy na 1. stupni se lekcí účastní opakovaně v půlročních tematicky zaměřených celcích, na 2. stupni navštěvují lekce jednou za rok, primárně v hodinách češtiny, kdy přínos lekce je spatřován v tom, že literatura je podána záživněji a tím je i lépe zapamatována[463]. Učitelé, resp. žáci, na 1. stupni si volili podle zájmu z připravených přibližně dvaceti lekcí, které téma je zajímá[464].

V pozitivním hodnocení spolupráce školy s dalšími místními organizacemi, ať už s kulturním centrem, muzeem nebo třeba s hasiči, se shodli všichni dotázaní. Přínos je spatřován na různých úrovních: pro děti, které si látku oživí a lépe zapamatují a naučí se přístupu vzdělávat se nejen ve škole, pro školu, která může využít dostupných expertů v oblastech, které by musela dostudovávat, pro město, jehož obyvatelé jsou vzdělanější a uvědomují si potřebnost všech institucí i efektivitu struktury městských organizací, a pro navštívenou instituci, které škola pomůže navázat s dětmi vztah. Pokud tedy škola s dalšími místními institucemi spolupracuje, nejedná se jen o vyplnění času nebo náhradu při plnění vlastních povinností, ale strategii přínosnou pro všechny přímo i nepřímo dotčené.

9.4.2.2 Knihovna

V případě knihovny jsou zásadní její možnosti v oblasti vzdělávání a informační bezpečnosti. Ředitel knihovny vyjádřil přesvědčení, že celé informační vzdělávání v knihovně bude školami vítáno, což potvrzuje to, že učitelka vyjádřila obavu, že rozšíření cílové skupiny lekcí realizovaných knihovnicí sníží její vlastní možnosti navštěvovat je se třídou. Ve sledovaném prostředí došlo k zavedení lekcí o informační bezpečnosti vlivem knihovnou pociťované poptávky od škol a veřejnosti. Ředitel knihovny tuto poptávku vnímal dlouhodobě, nebyl si vědom konkrétního zlomového okamžiku v přesvědčení o významu tématu

Už jen… jako… málokterá knihovna má člověka, který se věnuje pouze informačnímu vzdělávání. A už jen málokterá malá knihovna může mít člověka, který se mu věnuje“

[463] Zástupkyně: „Z těch osmi hodin češtiny, která je na prvním stupni naši, osmi devíti, na druhým stupni maj čtyři, pět, takže tam je to omezený, ale na tom prvním stupni máte poměrně dost literatury, děti se učí číst, tak tam proč číst knížku suchopárně ve třídě a neoživit si ji nějakým takovýmhle způsobem, tak si ty děcka i víc zapamatujou.“

[464] Učitelka: „my teda si většinou dáváme ve třídě hlasovat, třeba které to téma si zrovna vybereme, a teď si samy děcka vybraly poezii, jo, protože jsme ji docela, docela jsme ji probírali.“

digitálních stop, pouze zesílení pocitu v okamžiku jeho vstupu na sociální síť Facebook. Zahrnutí informační bezpečnosti do lekcí knihovny spojoval s řešením témat, která jsou důležitá, ale školou nepokrytá. Původně bylo řešení spatřováno v absolventech pedagogických fakult, což se ale v řádu let nepodařilo, proto si téma zařadil do nutných v knihovně[465]. Jednalo se tedy o manažerské rozhodnutí vedení knihovny, které bylo přes knihovnici zprostředkováno do školy, kde bylo přijato zástupkyní pro první stupeň za jí stanovených podmínek.

Zavádění informační bezpečnosti do lekcí v knihovně nebylo zahájeno až specializovanou lekcí, ale bylo začleňováno postupně. Přestože i knihovnice si uvědomovala potřebu jeho řešení, s ohledem na své znalosti si potřebovala vytvořit zázemí před zakomponováním tohoto pro ni omezeně známého tématu. Při budování této pozice přispělo nastavení spolupráce se školou v tématech, kde si byla knihovnice jistá, a nalezení experta na informační bezpečnost, který by ji ujistil ve správnosti postupu a poskytl možnost konzultací odborné stránky lekce[466].

Schopnost kvalitně pokrýt téma, a to bez zaměstnání nového a neověřeného pracovníka, byla základním předpokladem zahájení lekcí i pro ředitele knihovny. Tuto schopnost podle ředitele má každá knihovna vzhledem k oborové blízkosti a považuje za pravděpodobné, že se situace v tomto směru bude zlepšovat v současnosti existujícím působením propagátorů tématu informační bezpečnosti i elektronických služeb spojených s knihovnami, a také přítomností vzdělaných knihovníků v těchto směrech. Předpoklad existence člověka v knihovně pomoci radou v internetové bezpečnosti vyjádřila i matka, kdy navíc knihovnu vnímá jako

[465] Ředitel: „moje touha, v knihovně, už před sedmi lety bylo, abysme učili ve škole. Abysme učili věci, který…, který v tý škole chyběj, po kterých je nějaká poptávka, což internetová bezpečnost bezesporu, bezesporu je, a… aby… nějakým způsobem jako dokázala zaplnit mezeru, kterou třeba současný, současný pedagogický fakulty úplně, úplně nenabízejí. Ono se ukazuje, že… ten posun na těch pedagogických fakultách je ještě jakoby pomalejší, než třeba já jsem si myslel, a tím pádem mi z toho posledních pár let jako začíná vylejzat, že by to opravdu mohla bejt jedna z hlavních jako funkcí knihoven, … ta je, tahleta vzdělávací …“

[466] Knihovnice: „Pro mne to bylo vždycky atraktivní téma, ale i přes to, že jsem ta mladší generace knihovníků, tak jsem si vlastně velmi dlouho jako by netroufala do něj vkročit úplně na plno. Když jsem koncipovala ty lekce a navázala jsem už úzké vztahy se školou, se studenty, tak teprve v té chvíli v postatě jsem si troufla zakomponovávat prvky informační bezpečnosti do těch lekcí, které byly primárně zaměřené na rozvoj jiných dovedností nebo, nebo znalostí. Asi jsem vždycky, vždycky jsem věděla, a měla jsem to zakomponováno v koncepci vzdělávání, že tahle problematika by tam měla být zastoupena velmi silně. Jak informační bezpečnost, netiketa, další věci. Ale musím říct, že jsem podobně jako ostatní potřebovala nějakou oporu. Potřebovala jsem někoho, kdo tomu tématu opravdu rozumí na plno. Protože sama v té oblasti nejsem úplně úzce specializovaná, a v rámci svého pracovního úvazku nemám tolik prostoru a času na to, abych byla schopná… řekla bych, držet krok s tou problematikou. (…) Protože jsme si byli vědomi toho, že to chceme a že to potřebujeme.“

bezpečné prostředí pro použití internetu seniorkou v její rodině[467]. Na druhou stranu upozorňuje na snižování důvěry kvůli nezabezpečenému Wi-Fi připojení nabízenému knihovnou a významnou neaktuálností obsahu webových stránek knihovny, které si všimla s dcerou[468].

V oblasti připravenosti knihoven realizovat informační vzdělávání jsou dotazovaní zástupci knihovny skeptičtí, jak bylo zmíněno v předchozí kapitole. Problém vidí v chybějící pozici lektora v knihovně, a to i ve větších knihovnách. Tato pozice musí být nastavena, pokud má být koncepčně řešeno informační vzdělávání. V praxi lze ale pozorovat zadání informačního vzdělávání vedením bez zajištění potřeb pro knihovníka – lektora[469]. Knihovníci mohou být odborně připraveni, ale i když nepotřebují doplnit znalosti, jsou příprava i přizpůsobení převzaté lekce časově náročné. Čas je spojen s realizací, což pociťuje škola při domluvě termínů vyhovujících institucím i lidem. Lekce je nutné v klidu kanceláře připravit, mohou být náročné materiálně, není nutné vždy IT vybavení, ale i bez něj je náročná třeba na tradiční výukové pomůcky. To vše jsou zdroje, se kterými knihovník nemůže nakládat libovolně, musí se zodpovídat z efektivního vynaložení nadřízenému, který disponuje s omezeným rozpočtem. Podle ředitele jsou ale tyto náklady přínosné pro knihovnu i zdůvodnitelné u zřizovatele.

Kromě materiálního zázemí je otázka připravenosti knihovníků vzdělávat i na úrovni schopností v oblasti pedagogiky. Ta je podle knihovnice omezená, i když se změnami v kurikulu oboru ISK zlepšuje. Znalosti ale podle ní nejsou tak podstatné jako zkušenosti se vzděláváním, proto doporučuje zavedení praxe pro přípravu studentů, ať už v knihovnách nebo školách, alespoň na úrovni náhledů, podobně jako je tomu u studentů učitelství. To by odbouralo také v současnosti pozorovaný strach absolventů učit děti. Knihovnice považuje pedagogické znalosti za zásadní, protože na témata informační gramotnosti i bezpečnosti jsou podle ní studenti připraveni, nebo jsou naučeni si znalostní deficit doplnit[470]. Tuto schopnost

[467] Matka: „si tam může jít do té knihovny (…) a je taky vlastně na bezpečným prostředí, si myslím, že tam už to je ošetřený tak, že aspoň by… a navíc, když by potřebovala pomoc, tak ji třeba dostane, že se může i zeptat“

[468] Dcera: „ono třeba na stránkách knihovny je… bylo nedávno, byl říjen 2011“

[469] Knihovnice: „Mně se velmi často stává, že vedoucí knihovny, ať už ředitel nebo vedoucí pracovník nějakého oddělení, řekne tak, a teď budete informačně vzdělávat, (…) ale ten člověk na to nemá podmínky k té práci. De facto nemá svou kancelář, kde by v klidu připravil ty lekce. Nemá vyhrazenou část úvazku, jednoduše. Protože na to třeba nejsou peníze v rozpočtu.“

[470] Knihovnice: „Je to spíš o tom, že oni si potřebují najít formu. Většinou… s těmi lidmi, se kterými já jsem měla kontakt, tak po té vědomostní stránce byli připraveni. Nebo minimálně tam jde o to, že

doplnění zadaného tématu knihovnicí vyjádřily i zástupkyně školy, ale s omezením na knihovnici v místě, vyjádřily obavu, že ne každý učící knihovník je takto univerzální, ochotný zabývat se různými tématy. S knihovnicí příliš nesouhlasil ředitel knihovny, především pro oblast informační bezpečnosti považoval za podstatnější expertízu lektora, na druhou stranu sám vyjádřil názor, že expert v knihovně na digitální stopy a lektor mohou být dvě různé osoby[471], pokud budou lekce probíhat jen jednou ročně v rozsahu dvou hodin. Je ale problém, pokud lektor o bezpečnosti digitálních stop se sám nechová bezpečně, jak ukázala zkušenost ředitele s egosurfingem nově přijímané učící knihovnice. Zástupkyně školy sice souhlasily s významem formy lekce, význam didaktické přípravy ale vnímaly nižší, potřebné kvality spatřovali spíše v osobnosti lektora a jeho schopnosti děti zaujmout, i když pedagogická průprava tyto předpoklady podporuje.

Důraz na osobnost lektora nejen pro téma bezpečnosti digitálních stop byl vyjádřen oběma zástupkyněmi školy i rodiny. Bylo pro ně jen těžce představitelné, že by lekce ve stejném formátu probíhaly i při změně lektorky, což se později v roce stalo a lekce probíhají i nadále, i když jak vyjádřila žákyně „*už by to nebylo prostě ono*“. Je možné, že se situace v budoucnosti stabilizuje na dřívější úroveň, pokud se nově učící knihovnici podaří dosáhnout stejné úrovně hodnot, které akcentovaly zástupkyně školy, tj. pěkný vztah k dětem s pochopením jejich mentality a přizpůsobení lekce této mentalitě i jejich aktuální náladě, s čímž souvisí schopnost děti zaujmout a bavit, což obvykle není možné čistě frontální výukou, ale současně udržet autoritu, nebýt příliš kamarádský, udržet určité hranice chování při lekci. Důležité je získat důvěru dětí a dokázat, aby se otevřely lekci, což při vhodném přístupu není těžké, protože se otevřít chtějí, jak ukazuje zkušenost se sdílením rizikových činností při lekci s policistkou. Z toho vyplývá, že při vzdělávání dětí je nezbytná fyzická, ne virtuální osoba lektora, který je přiměje o tématu přemýšlet, jak opakovaně vyjádřil ředitel knihovny.

Jak bylo uvedeno, knihovnice vidí jako základní předpoklad realizace lekce o digitálních stopách zvládnutou didaktiku, např. pomocí e-learningu, resp. blended learningu, bez které je navržená metodika jen těžce aplikovatelná. Poté ale považuje

mají ten přístup a ví, kde si ty informace dohledají. Takže když sami na sobě cítí nějaký deficit, tak jsou schopni si ho doplnit.“

[471] Ředitel: „pokud chceš řešit internetovou bezpečnost, pokud chceš řešit komunikaci, tak v ní musíš bejt. Jo? Je to velmi oblíbený učit něco, co sám neznám a nedělám, ale, ale u tohohle je to jako jednoznačný“

metodiku za potřebnou, protože podobně jako ona, i ostatní knihovníci považují problematiku za zásadní, ale chybí jim opora pro její řešení, což knihovnice tvrdí na základě jejích zkušeností ze seminářů pro knihovníky, které lektorovala[472]. Metodika by měla být stručná, ale komplexní, protože současné nárazové řešení lekcí založené na nalezení pracovního listu a přečtení populárně naučné četby je nedostatečné. Znalostní připravenost v oblasti bezpečnosti digitálních stop je vnímaná jako omezená s tím, že mladší generace knihovníků k ní má blíž, především v prostředí sociálních sítí, a má také zažitý postup dovzdělávání se v potřebných oblastech, u starších knihovníků je ale připravenost a příprava výrazně omezenější. Podobné problémy ale existují u ostatních kulturních a vzdělávacích lokálních institucí, knihovna má proti nim výhodu v oborové blízkosti[473].

Dotazovaní se shodují, že s jistými omezeními jsou v knihovně lidé schopní po doplnění určitých znalostí a získání podpory vedení vzdělávat o bezpečnosti digitálních stop. Ředitel považuje vzdělávání za roli, která udrží význam knihovny i v digitální budoucnosti[474]. Shoda panovala v tom, že informační vzdělávání je přínosem pro knihovnu i pro vzdělávané, přičemž zahrnovat by mělo tradiční i elektronické zdroje, včetně bezpečnosti digitálních stop, a to pro děti i dospělé se zdůrazněním seniorů. Ve všech těchto tématech by měla knihovna budovat svou pozici kontaktního místa pro řešení problémů. Podle dotazovaných by bylo logické, kdyby knihovny toto téma v lekcích nabízely, protože je nerozlučně spojeno s informacemi, které zase patří do knihovny víc než do jiné místní organizace[475].

To vede k vyjádřením možnosti řešení problematiky v alternativní instituci proti knihovně. Tato možnost řešení je vnímána jako reálná, ale jen jako nouzové řešení, když se knihovna rozhodne tématu neujmout. Dotazovaní totiž považují za

[472] Knihovnice: „mezi knihovníky se o tom hovoří a pořád neustále se opakuje, kterak bychom měli, ale oni nemají v podstatě žádnou velkou oporu. Nejsou schopni, nemají takovou sebekázeň, aby si řekli tak, já se teď dovzdělám, všechno to zjistím a pak to začnou předávat dětem. Oni jsou v podstatě ale bezradní, (…) není žádná metodika, nikdo jim zatím nepomohl v tom, aby řekl, podívejte, s dětmi na prvním stupni řešte tato témata a je dobré to dělat tou a tou formou nebo tou a tou metodou. Oni zkrátka nemají nic, o co by se mohli opřít, aby začali. (…) Tak 99 % knihovníků se v podstatě lekne, když začneme řešit tohle téma a říkají mi, my ale sami o tom nic nevíme, a ty děti toho určitě ví mnohem víc, a kdo jsme my, abychom jim říkali, jak se mají chovat v tomhle prostředí."

[473] Ředitel: „je to práce… jako s informací, je to práce s komunikací, to do tý knihovny patří"

[474] Ředitel: „je to obrovská příležitost pro knihovny, (…)obecně s informačním vzděláváním, pokud řešíme, co budou knihovny dělat v době, kdy bude všechno digitalizováno, my ztratíme vlastně ten klasický základ, já si nemyslím, že by to v příštích třiceti letech byl nějaký jako dramatický problém, a… ale nicméně tohleto je jakoby jedna z možností, kterou, kterou … my jako můžeme cítit"

[475] Matka: „mně by se strašně líbilo, kdyby tady opravdu byly i… můžete mít kurz i týhle gramotnosti, s tou bezpečností, (…) tohle ke knihovně patří. Komu jinýmu?

nutné obojí vzdělávání a kontaktní bod, nejblíže k tomu vidí knihovnu, ale ta nepředstavuje jedinou možnost, mezi jmenovanými alternativami byly uvedeny síť prevence na městském úřadě, dům dětí a mládeže, informační centrum pro mládež, kulturní centrum a muzeum, příp. při dotacích od města nebo ve velkém městě komerční subjekt (nebo projekt). Dotazovaní tedy považují za jisté, že centrum řešení informační bezpečnosti v místě vznikne, pokud ho nebude zajišťovat knihovna, tak to udělá jiná instituce. Jedná se tedy o výzvu pro knihovny, zda se této příležitosti chopí, nebo ji přenechají někomu jinému.

Podpora vedení knihovny je nezbytná při systematickém řešení nejen tohoto tématu, ale i ostatních složek informační gramotnosti. Prvním krokem je rozhodnutí managementu, zda bude podporovat vzdělávací funkci knihovny a tím dá k dispozici část svých zdrojů. Proto musí knihovník doložit smysluplnost lekcí, což je u bezpečnosti digitálních stop možné společenskou poptávkou. Právě to byl zásadní argument ředitele knihovny. Pokud jsou lekce efektivní, knihovna podle něj získává vysokou přidanou hodnotu a má smysl je podporovat i na úkor jiných činností. Efektivita lekce je pak argumentem i ke zřizovateli[476]. Pokud se knihovna rozhodne kvalitně využít této příležitosti, vytvoří na úrovni zřizovatele i veřejnosti pozitivní obraz řešením zásadního společenského problému. Informační bezpečnost je podle ředitele knihovny tématem informačního vzdělávání, které je pro okolí knihovny nejsnáze představitelné s průniky do praktického života každého občana. Výhodou knihovny je především lokálnost a dostupnost pro řešení problému, která je již v místě šetření potvrzena praxí.

9.4.2.3 Škola

Knihovnice vyjádřila přesvědčení, že školy nabídku knihoven v lekcích o bezpečnosti digitálních stop přivítají, protože škola toto téma potřebuje zajistit. Skeptičtější přístup vyjádřil ředitel knihovny, podle kterého se objeví reakce

[476] Knihovnice: „jak třeba zřizovatel, vedení města, tak vlastně vedení školy, kteří navzájem spolu komunikují, tak veškeré aktivity té knihovny nesmírně oceňují a jakoby naopak je to další přidaná hodnota. (…) kde vůbec nefunguje systém informačního vzdělávání, tak je to úžasná přidaná hodnota a ta knihovna na tom vlastně může získat i pozici mezi institucemi ve městě.
Matka: „Zrovna tady v Poličce teda musím říct, že o co si ty organizace řeknou, a když to jako… musí to mít teda nějaký smysl, ale u knihovny nemůžete hledat hmatatelnej smysl, (…) tak vždycky knihovna, pokud měla nějaký záměr a dobře ho představila, musíte jednat, komunikovat, což by teda u knihovníků neměl být problém, tak to s tím vedením města vždycky vyjedná“

pozitivní i negativní, není možné vyvodit, které budou převažovat, protože na plošnější úrovni diskuze o zavedení spolupráce neexistuje. Zástupkyně školy komentovaly především vlastní pozici. Výběr lekcí v knihovně pro jednotlivé třídy vychází z jejich aktuálních potřeb, a to pro školní vzdělávací plán i život v současné společnosti, ať se jedná o autora literárního díla, koloběh vody v přírodě nebo informační bezpečnost. Právě bezpečnost digitálních stop je dle učitelky zásadní, především v 4. - 5. třídě, aby si žáci ujasnili, co dělají na internetu[477]. Ten jim totiž není možné zakázat a děti by si ho ani zakázat nenechaly, proto by škola měla zařídit, aby se děti seznámily s tím, jak se zde vhodně chovat. Potřebnost je tak veliká, že by učitelka uvítala i dvě lekce o informační bezpečnosti za rok, jednu zaměřenou na bezpečnou komunikaci a druhou na autorství na internetu a kritický přístup k informacím. Ještě silnější přijetí lekcí v knihovně o bezpečnosti digitálních stop je podle zástupkyň školy možné očekávat v menších obcích, kde je problém s odborníky na toto téma ve školách, v případě větších měst se přístup neodvážily odhadnout.

Přestože se Masarykova základní škola neomezila na očekávání nabídky, ale sama se zapojila do přípravy a nasazení koncepčního vzdělávání o bezpečnosti digitálních stop (což byl také důvod výběru do akčního výzkumu), ani ona neiniciovala toto řešení, spíše vyjádřila nadšení a přijetí po nabídce knihovny. Impulz pro zahájení řešeného typu spolupráce proto musí vyjít z knihovny, nelze očekávat opačný směr. Školu motivovalo částečně její zapojení do grantu, ve kterém se problematika částečně objevila tím, že škola musela řešit práci s autorskými díly podle zákona. Jako prvořadý byl ale opakovaně uváděn zájem dětí o informační bezpečnost, který učitelky pozorovaly na jejich dotazech a který se věkem posiloval[478]. Tento zájem vedl i k tomu, že učitelky na 1. stupni cítily vzrůstající potřebu samy se v této oblasti vzdělávat.

Pro nastavení spolupráce knihovny a školy v lekcích o bezpečnosti digitálních stop byla podle všech dotázaných (kromě žákyně, která se k tomu nevyjádřila) nezbytná osobní komunikace a srozumitelné vysvětlení, co přinese

[477] Učitelka: „protože pak oni vlastně chodí na ten internet, oni si tam chodí asi i dřív, že, samozřejmě doma, jo, ale aby jakoby si ty následky dokázaly všechny jakoby v tý hlavě trošku srovnat,“
[478] Učitelka: „Já si myslím, že už to, že děti jakoby to zajímá, to téma, jo, už od čtvrté třídy prakticky na ten počítač, nebo já nevím, ve druhé možná, sem tam jakoby jdou, že jo, a ptají se vás a tak jakoby nějak taková základní vzdělanost tam asi musí být, že jo, a hold vyspívaj, tak to jde výš a výš.“

škole a co knihovně, a s jakým obsahem budou děti seznámeny[479]. Tato fáze představuje nalezení společných zájmů obou institucí ve prospěch dětí, její výsledek je ale spojen nejen s obsahem, ale také s tím, jak se jsou tito lidé ochotní a schopní domluvit. I nejlepší obsah nemusí vést k úspěchu, pokud mezi zástupci institucí nebudou dobré mezilidské vztahy. Pokud je domluva možná, měl by být dostatečně vysvětlen obsah i pojetí, aby se učitelky nemusely obávat, že se děti v knihovně naučí rizikovému chování, které ještě neznaly, k čemuž podle zástupkyň školy v realizované lekci nedošlo[480], takže se tato obava po zkušenosti rozptýlila. Bez této fáze je také možné navázat spolupráci, pokud si jsou obě strany vědomy významu tématu, ale ne s tak dobrými výsledky a s vyšším rizikem, že spolupráce neproběhne bezproblémově, je také otázkou, zda bude o lekce mít zájem každá třída, nebo jestli dojde k příkazu od vedení školy, což není vhodná varianta, protože učitelé a knihovníci by se ve vzdělávacím obsahu měli vzájemně podporovat. Protože se jedná o osobní kontakt, je kritickým okamžikem změna osoby na jedné straně, která může vést k potřebě nového budování důvěry opakováním jednání o koncepci vzdělávání.

Knihovna by tak měla být prostředníkem i pro vzdělávání učitelů. K tomu by na základní úrovni mělo dojít již při zahájení vzdělávání dětí, aby učitelé chápali, proč se mají lekce účastnit. Lekce by měly sloužit k budování dle slov knihovnice *tandemu*, kdy učitel má blíže k dětem a formě vzdělávání a knihovník k obsahu bezpečnosti digitálních stop, takže si mohou vzájemně pomoci správně nastavit lekci pro děti i na ni navázat ve škole[481]. Zástupkyně školy ale poznamenávají, že knihovník může být inspirací pro učitele i ve formě vzdělávání, pokud využívá metod aktivního učení. Postupně by se podle knihovnice mělo vzdělávání dětí o technické stránce bezpečnosti digitálních stop dostávat z knihovny na učitele, ale

[479] Knihovnice: „co bylo velmi důležité, bylo to, žes, že bylo velmi dobře vysvětleno, proč, máme děti vzdělávat, jakým způsobem to chceme dělat a co bude vlastně tím přínosem, co bude těmi výsledky. V tomhle já považuju za nejdůležitější opravdu komunikaci, osobní setkání, to, aby ti lidé, jak realizátor, knihovník, tak učitel, se setkali a navzájem si o tom promluvili a vysvětlili si to."

[480] Zástupkyně: „Představa některých lidí byla, že si sednou k Facebooku a pojedou, jo, takže se naučej ještě to, co neuměj. Ale Vy jste to pojaly jinak. Takže todle to možná… předem předeslat, jakou formou to bude,"

[481] Knihovnice: „Myslím si, že ano, co se týká absolventů třeba pedagogických fakult, tak tam paradoxně zase není ten vědomostní základ, většinou vůbec netuší o tom, že by měli děti vzdělávat v oblasti informačního bezpečí, v tématu digitálních stop, a zase naopak oni zvládají tu formu. (…) Umí udělat plnohodnotnou vyučovací jednotku. Často to tak bývá i v institucích ve městě. Knihovník ví, co by chtěl dělat, učitel ví, jak to dělat. Proto to propojení a porozumění si myslím, že je hrozně důležité."

knihovna to musí zahájit a podporovat. Knihovna by si pak měla udržet oblast bezpečného chování na internetu, která je jí nejblíže, a v ideálním nastavení by děti procházely vzděláváním o bezpečnosti digitálních stop ve škole i v knihovně.

Je samozřejmé, že škola má možnost řešit problematiku bezpečnosti digitálních stop bez zapojení knihovny, i v tomto případě se ale podle dotazovaných hledá zástupné řešení. To může představovat interní zaměstnanec školy z 2. stupně, kdy ale škola musí řešit suplování a náhrady hodin[482] a ne vždy se i učitel informatiky zaměřuje na bezpečné chování[483], přičemž pro děti je to ještě méně známá osoba než knihovnice. Jinou variantu představuje externí přednášející, který ale neřeší potřebu kontaktního bodu v případě informačního incidentu. Není tedy důvod, proč by externím expertem neměl být knihovník, který je navíc dobře dostupný a děti se s ním setkávají i v jiných lekcích informační gramotnosti.

Vzdělávání o tématu ve škole před zavedením lekcí bylo spíše nárazové, zástupkyně školy i žákyně si vybavily především preventistu, který po ukázce videí Seznam se bezpečně s dětmi o problému diskutoval. Zajímavým zjištěním v rozhovorech bylo, že děti si v prvních letech školní docházky povinně zakládaly e-mail pro komunikaci se školou, ale nebyly poučeny o jeho bezpečném použití, proto většinou obsahoval jméno a příjmení a byl dětmi využíván běžně při různých činnostech na internetu. Kromě e-mailu škola děti podporuje v používání internetu pro jejich vzdělávání. Před zavedením lekcí v knihovně se objevily okamžiky, kdy učitelka musela řešit informační incident na podnět matky, příp. při problematických záběrech školy na YouTube, bez těchto neignorovatelných podnětů se ale s dětmi tématu bezpečnosti digitálních stop na 1. stupni nevěnovala. To ukazuje nedostatečnost řešení tématu i ve škole, která je mu nakloněna, ale zajišťuje si jej vlastními silami. Systematičtěji se o něm nemluví, aby se děti naučily stabilně přemýšlet o bezpečném chování při použití internetu. To, že sice ve škole je osoba, u které se materiály a informace o problematice shromažďují, považuje za nedostatečné i učitelka, podle ní by bylo dobré, aby základní informace o bezpečnosti digitálních stop měl každý[484].

[482] Učitelka: „většinou to učí stejně někdo z druhého stupně u nás nebo, nám to nevyjde tedy ani jako by časově, protože taky musí nějaké hodiny vypouštět“

[483] Zástupkyně: „nevím, jak do hloubky oni třeba by tohle to uměli podat, že jo. Oni Vás naučí Excel a tyhle ty třeba textový programy, ale tohle to zas tolik nevím,“

[484] Učitelka: „máme tady taky, že jo, určitý lidi, který prostě se zabývají těmahle otázkama, jo, takže… jakoby ti kantoři, když je nějakej problém, tak mají za kým jít, jo, kdo to prostě schraňuje,

Při hodnocení vzdělávání dětí o bezpečnosti digitálních stop školou a knihovnou byly v rozhovorech uvedeny určité nevýhody školy ve prospěch knihovny. Jen část z nich je spojena s nedostatečnými znalostmi učitelek v oblasti práce s počítačem, roli hraje i omezení vlivem školy jako instituce formálního vzdělávání. Pro řešení problémů s digitálními stopami a vzdělávání v tomto směru může být pro školu omezením, že děti se zde cítí pod dohledem, a to jak autority učitele, tak i stálého kolektivu, chybí zde zdravá anonymita, aby se dítě uvolnilo a svěřilo s problémem v oblasti digitálních stop, ve škole je těžší říct, že dítě neví, jak se bránit, protože ve škole má prokázat znalost, ne neznalost. Důsledků odlišného vztahu mezi dítětem a učitelem nebo knihovníkem, příp. jiným externím odborníkem ve prospěch řešení tématu bezpečnosti digitálních stop mimo školu si jsou vědomy i zástupkyně školy.

Silný vliv při navazování spolupráce i při hodnocení lekcí měla návaznost lekcí na výuku ve škole, proto jsou základní pomůckou pro práci s lekcemi pro knihovníka školní dokumenty, což si uvědomují všechny strany, které se tohoto jednání v minulosti zúčastnily. Žákyně sice soudila, že knihovna slouží především v návaznosti na předmět český jazyk, vyplývalo to z její zkušenosti, protože na látku z informatiky lekce v knihovně necítila navázané. Proti tomu knihovnice a obě zástupkyně školy uváděly spojení se svým školním vzdělávacím plánem v rámci mezipředmětových vztahů zahrnujících český jazyk vzhledem ke čtení a psaní při aktivním učení v lekcích, ale především přírodovědu, protože do ní patří oblast zdraví, tím i bezpečnost a také informační bezpečnost, vč. Linky důvěry. Zařazení tématu do tohoto dokumentu zavazuje učitele látku s dětmi probrat, ale podle knihovnice i pracovnic školy uvítají, pokud se jí chopí knihovna, protože se v ní učitelky necítí příliš jisté. Lekce se tak stává součástí školní výuky, není proto problém vyčlenit na ni požadované hodiny.

Po získání představy o navržené koncepci zástupkyně školy i knihovnice vyjádřily přesvědčení o vhodnosti zahájit ji již s dětmi od 2. třídy, nejpozději od 4., příp. začátku 5. třídy. Tento věk by měl odpovídat tomu, kdy děti používají samostatně počítač, protože pak by se měly také samostatně rozhodovat o svém chování na internetu. Koncepční přístup je hodnocen jako klíčový, tj. že lekce jsou

vyhledává, že jo, a kdo by měl poradit, jo, ale myslím si, že takový ty základy že není špatný, aby věděl prostě každej,“

naplánovány pravidelné a na sebe navazující, jsou přizpůsobeny obsahově i formálně věku tak, že jsou pro děti přijatelné a zábavné. Přestože se koncepce do praxe zavádí postupně, je vhodné mít stanoven cíl, který je sledován a prezentován zúčastněným. Pestré, aktivní učení je dobře hodnoceno všemi dotazovanými, kdy se děti nenásilnou formou dozvědí něco nového, co ale již částečně bylo probráno ve škole. Toto nastavení lekce je pro učitelku zásadní – pokud má jistotu určité úrovně znalostí, není důležité, o kolik větší je jeden expert, když jiný dokáže potřebný obsah dětem lépe předat. Všichni dotázaní hodnotili pozitivně, že lekce neprobíhala ve škole, ale v knihovně[485], což omezuje důraz na sumativní hodnocení výsledku ve prospěch formativního, děti se soustředí více na to, co má být naučeno, než na formu, např. pravopis, který se v knihovně řeší výrazně méně než ve škole. Pro výsledné hodnocení lekce je proto zásadní forma i obsah[486].

Přes to, jaký obsah a forma jsou před lekcí prezentovány, učitelky nehodnotí lekci do doby, než s ní mají zkušenost. Až ta je tedy zásadní pro dlouhodobé přijetí či nepřijetí lekce, ovšem nemusí se jednat o přímou zkušenost jedné učitelky, ale jedné z nich, hodnocení poté sdílí[487]. Reakci následně lze pozorovat na zvyšujícím se nebo snižujícím zájmu navštívit lekce. Může se tak stát, že i učitelka, která původně o lekci neměla zájem, vlivem pozitivního hodnocení kolegyň se se třídou do lekce zapojí. V případě, že knihovna využije hosta a škole lekci zprostředkuje, očekávají učitelky standard, jako jsou u knihovny zvyklé, pokud se nesplní, má to vliv nejen na hodnocení externího lektora, ale celého vzdělávání v knihovně.

V případě, že je učitel s lekcí spokojen, měl by na ni navázat s dětmi ve vlastní výuce, což je dobré podpořit poskytnutím materiálu, od kterého by učitel mohl začít. Dle knihovnice i zástupkyň školy ale vliv spokojenosti vede také k přenesení znalostí i zprostředkování kontaktu přes učitele k rodičům. Škola tedy sebe vnímala spíše jako prostředníka pro navázání kontaktu, aby knihovna

[485] Učitelka: „Tím, že oni se dostanou i mimo třídu, že jo, tak zase je to trošičku něco jiného a myslím si, že opravdu je to dobrý."

[486] Knihovnice: „Myslím si, že paní učitelky byly velmi, velmi mile překvapené, že i takováhle problematika, které se ony vždycky bály a stranily, lze pojmout touhle formou. Která je pro ně pochopitelná, vidí, že děti se u toho baví, ale že to má opravdu ty vědomostní výstupy a má to ty dovednostní, dovednostní základy."

[487] Učitelka: „jakoby dopředu to stejně nepoznáte, že jo, já si myslím, že je potřeba prostě vidět… toho danýho člověka, že, jak to podává, i když nám řeknete, budu to dělat takhle a takhle, tak ono stejně jako každej člověk prostě to dělá jinak, že jo, ať… co si budeme říkat, a takže si myslím, že jakoby záleží asi na té první hodině, kterou Vy uděláte, a my jsi to zase samozřejmě mezi sebou už řekneme, že jo, jestli to k něčemu bylo, nebo jestli se nám to líbilo, jestli se nám to nelíbilo."

vzdělávala nejen děti, ale i rodiče, k tomu je dokonce ochotná nabídnout svůj prostor a hodnocení kvalit vzdělávání o tématu v knihovně na rodičovských sdruženích a dalších místech kontaktu s rodiči.

9.4.2.4 Rodina

Žáci na připravenou lekci o informační bezpečnosti šli až na výjimky (dle žákyně se v její třídě jednalo o jediného žáka) s nadšením a očekáváním. To ukazuje pozitivní postoj dětí k řešení tématu ve vzdělávání knihovnou. Kladně hodnotí oživení tématu s doplněním nových informací. Současně žákyně projevila zájem o lekci (v rozsahu 90 minut) nabídnutou knihovnou i mimo školu s tím, že by se nesměla křížit s jejími volnočasovými prioritami a musela by mít jistotu, že jí přinese něco nového. Zástupkyně školy k tomu doplnily přesvědčení, že se jedná o záležitost 1. stupně, a to jak z hlediska přínosu, kdy si děti v tomto věku budují postoje, tak i zájmu se zapojit[488]. V postoji venkovských a městských dětí podle nich ve směru přístupu k aktivitám i k tématu není v současnosti rozdíl.

Pohled rodičů na vzdělávání dětí v knihovně na sledované téma se opět nikdo z dotázaných neodvážil zobecňovat, vyjádřili ale svorně přesvědčení, že by převažoval pozitivní postoj. Někteří by uvítali, že děti slyší i od někoho jiného to, co sami říkají, což byl případ dotazované matky, jiní by mohli uvítat, že lektor s dětmi řeší závažné téma, které je pro ně samotné vzdálené, i když je možné, že by si ho spíše spojovali se školou, protože rodiče mají méně přímý kontakt se vzděláváním v knihovně než učitelé a děti. Ne výjimečný by podle ředitele byl i postoj neutrální, protože „*který rodiče zajímá všechno, co je, co je ve škole učí.*“ Matka připomíná, že knihovna nemusí šířit osvětu jen lekcemi, mohla by připravit různé letáčky a nálepky pro děti s připomínkami bezpečného chování na internetu, osvěta také nemusí směřovat jen k dětem, protože ohroženou skupinou jsou například i senioři.

Odkaz matky na seniora vycházel z její zkušenosti ve vlastní rodině. Uvedla příklady dvou příbuzných, z nichž jeden je vášnivý čtenář s omezeným zájmem cokoli dělat na internetu, přestože by mu to usnadnilo čtení, druhý získal od rodiny

[488] Učitelka: „teenageři už toho hodně vědí, že jo, tak už si zas do toho nenechají tolik mluvit, že jo, a tydlety si myslím, že když se nějakým způsobem nastaví, jo, ty malý děti, tak že pak už jakoby v tom pokračujou,“

registraci do knihovny především pro řešení zájmu používat internet, primárně pro komunikaci se známými. Bezpečnost seniorky na internetu by proto matka také uvítala podpořenou knihovnou, toto vzdělávání by podle ní mohlo navazovat na osvětu seniorů, která nedávno probíhala pro jejich ochranu proti nepoctivým prodejcům[489]. Dotazovaná žákyně je silnou uživatelkou internetu, ale v době rozhovorů ho využívala spíše k hrám než ke komunikaci (s půlročním odstupem matka uvedla změnu se značným zvýšením komunikace, což odpovídá empirickým zjištěním[490]). Omezenou komunikaci vedla především přes e-mail, o další typy služeb neměla zájem, protože „*prostě každej den to kontrolovat, jako jestli mi něco nepřišlo a tak, jako to podle mě je nuda*". Vyjádřila přesvědčení, že i její spolužáci, kteří používají Facebook, zde komunikují zejména v rámci třídy (což potvrdila i matka s odkazem na internetovou činnost spolužaček při častých návštěvách), sama necítila informační deficit tím, že profil na Facebooku nemá.

V rámci rozhovorů matka i žákyně odkazovaly na své znalosti v oblasti digitálních stop, žákyně především směřovala k práci s fotografiemi obličeje, které by se na internet neměly dávat, problém je i s jejich stažením. Druhou opakovaně uváděnou oblastí byla bezpečná hesla, ke kterým se vyjadřovala i na úrovni zkušeností založených na práci s hesly u jejích známých. Matka se proti tomu zamýšlela spíše nad veřejnými rejstříky, do značné míry opět díky zkušenostem z jejího zaměstnání, a také nad připojením k internetu a využití IP adresy, které si uvědomila až při přípravě na rozhovor[491]. I dříve se ale zamýšlela nad některými způsoby využití digitálních stop, např. po nákupu v e-shopu. Současně dodává, že se její přístup za dobu použití internetu změnil k vyššímu uvažování nad důsledky poskytnutí informací, uvědomuje si ale, že chyba, kterou mohla udělat před mnoha lety, se může objevit v budoucnosti, aniž by s tím v současnosti mohla cokoli udělat. Sama se ale naučila využívat digitální stopy, a to nejen v zaměstnání, ale třeba i pro zjištění, kdo je současná přítelkyně jejího syna. Přes Facebook našla i nevhodné

[489] Matka: „To bylo taky pak ještě kvůli šmejdům, samozřejmě, ale bylo to už dřív, každoročně, to už letitě funguje. A oni už se nám to teď naučili senioři a už tam moc nechoděj, protože už jsme jich to hodně naučili a zbytek se to naučí od vnoučat, že jo, takže to je pravda."

[490] FINDAHL 2009

[491] Matka: „ty číselný kódy, což jsem já, pokud jde o internet, kdo jsem já, IP adresa, nebo jak se to jmenuje. Je zajímavý, a toto jsem začala o tom přemýšlet, až když jsem si o tom přečetla všechno, tak jsem si říkala, to je teda dobrý, protože já se podívám, sháním nějakou věc, podívám se na ten server, nejsem teda chráněná žádným Proxy serverem a já nevím, jak oni to nazývaj všechny tyhle ty ochranný nástroje trošičku, a je pravda, že do týdne se mně najednou tam úplně v jiných vodách, běžných zprávách, začne objevovat jejich reklama. A to si myslím, že je ono. To je ta moje stopa."

fotky dcery její kamarádky, kterou upozornila i přes obavu, že bude považována za drzou, ale s potěšením zjistila, že dívka uznala svou chybu a fotky stáhla. Přemýšlení o digitálních stopách u matky i žákyně vedlo k tomu, že zvažují poskytnutí informací o sobě přes internet, např. v registracích, proto když je nutné některý údaj uvést a je to možné, vymyslí si jej.

Z hlediska mediačních strategií dotazovaní nebyli příliš nakloněni restriktivním opatřením, především pokud se spoléhá výhradně na ně[492], spíše se přikláněli k aktivní mediaci, protože výhody spojené s použitím internetu podle nich výrazně převažují nevýhody. I rodiče, kteří mají určité povědomí o informační bezpečnosti, se jen málokdy cítí v této oblasti dostatečně pevně nebo vnímají potřebu problematiku řešit, takže se s dítětem snaží bavit, ale jejich ponaučení jsou omezována na případy ve zpravodajství nebo dílčí témata. Opakovaně v rozhovorech zaznělo, že internet a materiály k tématu na něm jsou dobrým zdrojem osvěty, ale nestačí, je nutné děti (ale i rodiče a učitele) vést k přemýšlení o tématu a umožnit jim diskuzi s fyzickou osobou, a to při lekci i v návaznosti na ni, když cítí tuto potřebu. Podle zástupkyně se to možná časem bude měnit, nová generace bude v oblasti informační bezpečnosti poučenější, alespoň u vysokoškolsky vzdělané části populace, méně vzdělaní a starší lidé ale stále budou potřebovat podporu, otázka ale je, zda o ni budou mít zájem.

Z toho vyplývá, že v rodině jsou udržovány základní znalosti a dovednosti práce s digitálními stopami jak vlastními, tak cizími, i přesto byl vyjádřen zájem o lekce v knihovně pro různé členy rodiny. Ukázalo se také, že matka i dcera mají poměrně bohaté zkušenosti s digitálními stopami, jak přímými, tak zprostředkovanými, často ale jednají intuitivně, zamýšlení se nad možnými důsledky zkušenosti je vhodné ještě podpořit, např. materiálem dodaným rodině po lekci, který by matka pro tento účel podle vlastních slov uvítala[493].

Přesvědčení, že by postupně mělo dojít k zapojení rodičů do řešení bezpečnosti digitálních stop, se objevilo u zástupců školy a knihovny. Je ale nutné je nejdříve nějakým způsobem aktivizovat, protože jejich vnímání problému je

[492] Ředitel: „představa, že to dítě sedne k počítači a pustěj mu ho na tři hodiny, nebo na dvě hodiny, protože víc už je to škodlivý, (…) ale… ten obsah jako… je to počítač, že jo, tak co tam asi dělá… hraje tam, dělá si tam nějaký blbosti, (kýve hlavou) chatuje s kamarádama třeba,“

[493] Matka: „ty vaše otázky byli lepší, než to moje přemýšlení. Protože mě dovedly daleko dál“

omezené. K tomu škola může využít např. rodičovské sdružení[494], podle zástupkyně může rodiče aktivizovat strach o jejich dítě, je proto nutné je upozornit na možné negativní důsledky zneužití digitálních stop formou kazuistik. Ředitel knihovny, který v místě téma informační bezpečnosti prosazuje, uvádí, že se setkává s žádostmi o radu od dětí nebo učitelů, ale od rodičů je ještě nezažil. Spoléhat se na neorganizované vzdělávání rodičů není správná cesta, stejně jako očekávat, že si sami najdou cestu do knihovny, opět je nutný impulz od samotné knihovny, který může podpořit škola.

Informální vzdělávání dětí probíhá v kontaktu se staršími členy rodiny při společném použití počítače a v diskuzi s vrstevníky, k rodičům se ale z těchto směrů příliš informací nedostává. Rodiče se informálně v bezpečnosti digitálních stop mohou vzdělávat v zaměstnání, jako v případě dotazované matky, která s nimi pracuje při prováděných kontrolách, ale to je případ jen omezeného množství rodičů. Druhým zdrojem pro informální vzdělávání jsou média, zejména zpravodajství, kde dotazovaní upozorňovali na krádeže identity. Zprávy se ale objevují nahodile, chybí systematický akcent, proto je zástupkyně přesvědčena, že média na podporu tématu nejsou připravena[495], i když jinak by představovaly vhodný zdroj pro osvětu veřejnosti. Při uvědomění si zájmu rodičů vzdělávat se v tomto směru je možné sebeřízené vzdělávání, kde je využíváno především televizních pořadů a obsahu na internetu, což je ale podle matky časově náročné[496], důvodem může být, že má omezenou představu, co hledá, a nezná specializované zdroje pro osvětu v této problematice, nebo jí nevyhovují.

Ze zkušenosti školy vyjádřily její zástupkyně přesvědčení, že sice se objeví nezájem[497] i negativní reakce rodičů na vzdělávání o informační bezpečnosti v knihovně, nebudou ale příliš časté. Zástupkyně ale upozornila na problém, že

[494] Učitelka: „jako jak říkala [zástupkyně] (…), tak právě opravdu třeba i ten jeden, to jedno rodičovský na začátku třeba té páté třídy nebo tak i tomu možná věnovat trošku hloubejc a seznámit ty rodiče s tímhle tím, no, protože já si myslím, že opravdu spousta rodičů si vůbec nedokáže představit jako, co by se mohlo stát,“

[495] Zástupkyně: „média si myslím, že na to úplně připravený teda nejsou, protože… tu bezpečnost a první pomoc to se začalo dělat v posledním roce, že jo, před tím tako jakoby vůbec nic,“

[496] Matka: „Mně třeba nejvíc vadí na tom to, že… to stojí tolik času a vlastně tolik znalostí, i když třeba abstraktních, nemusím úplně všechno o tom vědět, že až třeba z diskuze různých… třeba většinou mladých lidí, já i když jsem v letech, tak zjistím, co je třeba…“

[497] Zástupkyně: „i třeba kdyby se tady udělala pro veřejnost nějaká přednáška, já nevím, třeba by na to nikdo nepřisel. My jsme tady měli nabídku pro rodiče, tehdy to byly nějaký problémy ve výchově a vzdělávání, oslovili jsme celý ročník, že bysme sem vlastně tady tu psycholožku pozvali, že by to bylo pro rodiče, no a vlastně z těch sedmdesáti dětí a potažmo teda asi sto čtyřiceti rodičů, se nám přihlásilo asi pět 5 lidí, kteří měli zájem.“

o vzdělání budou mít spíše zájem rodiče, kteří se dítěti na internetu věnují a zabývající se také jeho ochranou, výrazně horší to bude s rodiči, kteří to berou na lehkou váhu, a proto by lekce více potřebovali. Zástupkyně školy upozorňují, že je nutný citlivý přístup ve vzdělávání rodičů i v jejich informování o obsahu vzdělávání dětí[498], důraz by měl být kladen na to, že obsahem lekce je ochrana proti útokům s digitálními stopami. Pasivita v řešení informačních hrozeb i vlastním vzdělávání je podle zástupkyň školy spojena s tím, že si rodiče nedovedou představit možné důsledky chování jejich dětí na internetu i reálnost problémů, dokud k nim nedojde, jsou přesvědčeni, že pro potřeby svého dítěte toho ví dost. Toto se neobjevuje jen u informační bezpečnosti, ale i jiných problémů dětí. Někteří rodiče dokonce sami ohrožují dítě, především matky malých dětí jsou příliš otevřené na internetu ve sdílení informací, jak upozornila knihovnice, proto by rodiče měli být vzdělávaní ještě před narozením potomka. Přestože rodiče pravděpodobně neprojeví silnější zájem o lekce v knihovně o bezpečnosti digitálních stop, je podle učitelky podstatné s nimi začít a věřit, že se při trpělivém opakování osvědčí a rozšíří[499].

9.4.2.5 Obsah a forma lekce

Podle knihovnice se knihovny informační bezpečností zabývají, ale spíše v oblasti autorského práva a etiky, téma digitálních stop, které je v knihovnách také potřebné, je v praxi pokryto minimálně. Jak je uvedeno v kap. 9.4.2.3, bezpečnost digitálních stop řadí škola do přírodovědy pod oblast obecné bezpečnosti. To odpovídá názoru ředitele knihovny, že bezpečnost digitálních stop patří spíše do občanské vybavenosti, v případě vědních oborů do základů společenských věd než do informatiky, a přesvědčení knihovnice, že škola by měla v informatice pokrývat technická řešení bezpečnosti a knihovna bezpečné chování na internetu. Od toho se odvíjí přesvědčení ředitele o jednoduché podstatě sdělení v lekci, ať už vzdělává děti, učitele, rodiče nebo nejširší veřejnost: „*ona celá internetová bezpečnost je relativně dost banální, ono to není nic jinýho, než, než jako nemluv s cizími lidmi.*“ S tím souhlasila i učitelka, která srovnávala potřebu uvažování nad digitálními

[498] Zástupkyně: „Možná by to muselo být citlivě pojatý, aby si ty lidi neřekli, no jo, oni je to ještě naučej, jo, i takovýhle lidi jsou, jo? Oni ještě jim to ukážou, jak se to má dělat.“

[499] Zástupkyně: „No, ono taky jak by třeba ta první lekce dopadla, že jo. My jsme maloměsto, tady se informace šíří strašně moc.“

stopami před jejich vznikem s rozhlížením před vstupem do vozovky. K tomu je ale potřeba upozornit na iluze (např. vzdálenosti mezi lidmi vedoucí k nemožnosti útoku)[500] a specifika bezpečnosti v internetovém prostředí. Pozitivní je podle dotazovaných již otevření diskuze nad tématem, aby se člověk zamyslel, co zná teoreticky a co dělá. To není samozřejmé, naopak jednoduché propojení vnímají respondenti jako něco, co může velmi pomoci. Nejde tolik o přenesení odborných znalostí, např. definic termínů nebo pouček, ale spíše postojů a přemýšlení o digitálních stopách dřív, než je člověk vytvoří, příp. domýšlení možných důsledků jejich vzniku. K přenesení tohoto postoje nepomohou materiály zveřejněné na internetu různými projekty, je nutná osobní diskuze, jak vyjádřili shodně dotazovaní[501]. Součástí sdělení lekcí by také podle nich mělo být nabídnutím se knihovny jako kontaktního bodu pro řešení problémů s digitálními stopami[502].

Při konkretizaci informací, které by se v lekcích měly objevit, uvedli respondenti řízení vzniku digitálních stop, které nevede k omezení použití internetu s jeho výhodami, a možnosti nápravy digitální stopy. Silný důraz byl kladen na prevenci v chování spíše než spoléhání se na fungování služeb a jejich bezpečnostní principy[503]. To lze přenést i na vzdělávání o netiketě, protože podle ředitele knihovny tato pravidla vzniknou přirozeně při dodržování základních etických principů, jako je zlaté pravidlo nebo kategorický imperativ. Ředitel knihovny přitom zdůrazňuje, že není možné příliš vycházet z obsahu vzdělávání o tématu v západních zemích, protože tam se uživatelé na internetu chovají méně rizikově, ale také je téma již výrazně více řešeno[504]. Z hlediska důsledků, které je vhodné

[500] Ředitel: „akorát ten základní problém je v tom, že to, co řešíš ty, to jsou ty nyance. (…) ta iluze toho, že jsi sám, a že vlastně jako je všechno daleko, je jako, je klíčovej. Jinak by se vlastně jednalo o klasickou jako bezpečnost jako na živo. Ale… ale tohle jakoby je její nevýhoda. Její velká výhoda je, že prostě, že přes internet ti nikdo nedá klackem do hlavy, že jo, což, což až potom…“

[501] Např. učitelka slovy: „A je samozřejmě něco jiného, když si to lidi jakoby přečtou, že jo, což ne každej udělá, a nebo když to bude někdo přednášet a mluvit o tom,“

[502] Zástupkyně: „Myslím si, že taková ta poradenská služba možná pro ty děcka jakoby taky chybí, jo, aby oni měly možnost jakoby se s někým poradit, domluvit, jo, protože asi ne kazdej rodič je v tomhle zběhlej…“

[503] Ředitel: „Pokud se bavíme o tom, že třeba musíme mít jako pořádná hesla, z mýho pohledu je ze všeho nejlíp jako nesvěřovat, nesvěřovat jako, vždycky si velmi rozmyslet, co obecně jakoby do nějakýho veřejnýho prostoru dávám.“

[504] Ředitel: „myslím si, že ovšem tkví v Evropě nebo v Čechách, dokonce možná jako v post, v posttotalitních zemích, na rozdíl třeba od Ameriky, kde já jsem přesvědčen o tom, že třeba chování na sociálních sítích… je výrazně jakoby… jednak oni jsou na nich mnohem míň, to je v celku jako známá věc, a že to chování je výrazně jako umírněnější. Jako, takový jako že ty fotky v těch těch podprsenkách, ty rukovky, který jako v Čechách jsou úplně běžný, že tam by byly jako výrazně víc problematičtější, že to zažití, zažití obecně je to, je to i… je to víc jako hlídaná země, a myslím si, že, že se to tam jakoby řeší i, i ve školách.“

vyzdvihnout při vzdělávání, uvádí matka ztrátu soukromí a kriminální čin v podobě krádeže identity. Se zástupkyněmi školy se shodla, že vhodné je předání poznatků o možných důsledcích formou kazuistik, ne obecnými přednáškami[505], a to opět při vzdělávání nejen dětí (v jejich případě se podle matky i dcery není nutné obávat strachu vedoucího k omezení použití internetu, protože je pro ně příliš důležitý, dokáží se s informacemi vyrovnat).

Z hlediska formy lekce pro děti by mělo jít o koncepční přístup přibližně od 3. třídy vzhledem k použití internetu dětmi, byl doporučen minimální rozsah 90 minut za rok, učitelka by uvítala lekce na začátku i na konci školního roku, které by na sebe navazovaly. Lekce by měly být učitelům známé všechny (a ideálně více lekcí s odlišným pojetím problematiky digitálních stop), aby mohli s knihovníkem zvolit, která z nich je vhodná pro konkrétní třídu. Pro děti by měla být účast na těchto lekcích povinná v rámci školní docházky prostřednictvím zařazení do školního vzdělávacího plánu. Lekce by měla být pestrá, rozhodně ne na úrovni pouhé přednášky, a kvalitní, děti musí mít jistotu, že lektor obsahu rozumí, ale současně je dokáže zaujmout[506]. Matka s dcerou uváděly zájem o lekce, při kterých společnou tvorbou knihovníka a dětí vznikne nějaký materiál, může se jednat o zápisky, obal na sešit s informacemi o problematice nebo např. komiks. Produkt po lekci by měl sloužit nejen k udržení informací v paměti dítěte, ale knihovník by měl podpořit učitele v návaznosti na lekci tím, že mu také poskytne nějaký materiál, např. jednoduchý pracovní list.

Obsah lekcí pro děti by měl navazovat na lekce v knihovně k informační gramotnosti, kde děti zjistí, jak s informací pracovat, především u dětí na 2. stupni je nutné informační bezpečnost prohlubovat v souvislostech mezi těmito tématy přes dokumentovou gramotnost. Respondenti se shodují, že základem obsahu jsou informace o řešení internetových problémů (spíše než samotné tyto problémy, i když i ty by se měly v lekcích objevit, jak již bylo uvedeno, zejména formou

[505] Zástupkyně: „to byla výuka šokem, protože si to vůbec nedovedli představit, jo? Jedna všichni vědí, co to kyberšikana je, jo, všichni už počítač viděli někdy, ale tohle je opravdu šokovalo. A pak teda na to tak nějak naskočili a byly schopní vnímat."

[506] Zástupkyně: „Vy jim něco pustíte, něco ukážete, oni musí vidět, že tomu rozumíte, a udělat to pestrý, to je důležitý, no. Naše děti už se nespokojí s nějakým obyčejným filmem, protože… už jsou trošku rozmlsaný a zhýčkaný a už se pro ně musí opravdu hodně udělat, aby je to zaujmulo, no."

kazuistik)[507], především preventivní na úrovni chování, jak již bylo popsáno výše při vymezení obsahu lekcí pro libovolnou cílovou skupinu. V prvním kroku je nutné doplnit povědomí o fungování internetu[508], následně by pozornost měla být zaměřena na omezení sdílení osobních informací, zejména fotek a videí, netiketu, krádež identity a kyberšikanu.

Aby mohli učitelé na lekci v knihovně navázat, musí vědět, co bylo jejím obsahem a také mít znalosti pro jeho rozvedení při vlastním kontaktu s dětmi, o který na této úrovni učitelky projevily zájem podle zástupkyň školy (a při kontaktu výzkumnice se všemi učitelkami z 1. stupně při zahájení akčního výzkumu). Proto dotazovaní, především zástupci školy, zdůrazňovali potřebnost vzdělávání učitelů knihovnou. Současní učitelé, ale i absolventi pedagogických fakult, pokud se nespecializují na informatiku, nemají v rámci odborného vzdělávání příliš příležitostí rozvíjet se v informační bezpečnosti. Toto vzdělávání je pak obvykle omezeno na přednášky bez praktické složky, které podle slov zástupkyň školy za sebou mají všechny učitelky, ale výsledky nepovažuje nikdo z nich za dostatečné. Výjimečná práce s kazuistikami ukázala, že je tato forma mnohem efektivnější, proto je vhodné jí využít i při kontaktu s učitelkami. Jejich vzdělávání knihovnou o bezpečnosti digitálních stop by mělo probíhat na dobrovolné úrovni formou Face-to-Face interaktivní lekce, protože podle učitelky si poskytnuté materiály k tématu projde málokdo, spíše je jejich obsah jen povrchně mezi učiteli sdílen[509]. Za vhodnou není považována ani technika webinářů, kterou by mohli přijmout knihovníci, ale učitelé spíše projevují zájem o fyzický kontakt při svém vzdělávání v řešeném směru. Učitelé i knihovníci by při vzdělávání mohli být podle knihovnice podpořeni e-learningovým kurzem, základem ale je fyzické setkání, ideálně formou workshopu, jak dodávají zástupkyně školy, vzhledem k omezenému zapamatování toho, co si ihned nevyzkouší, s aktivním, příp.

[507] Učitelka: „Protože samozřejmě, já si myslím, že ono je i docela dobré je jakoby vystrašit, že jo, co se týká zrovna tohodle, ne, aby si to uvědomily, že jo, a pak jim samozřejmě ještě jakoby připomenout ty možnosti, které tam jsou."

[508] Knihovnice: „A musím říct, že do určité míry je tam nutná i určitá jakoby teoretická osvěta. Už vůbec princip fungování internetu… je poměrně velký problém. Protože děti mají sice ve škole … informatiku, (…) ale oni se tam učí v podstatě … mechanicky zacházet s nástroji a s programy. A nikdo jim nevysvětlí, alespoň já tu zkušenost mám z více škol, nikdo jim nevysvětlí princip fungování internetu, takže to si myslím, že by taky mělo být jedno z témat."

[509] Učitelka: „prostě tady nejsou na tom všichni tak, že k tomu počítači zasednou a prostě… nahledaj si to, jo, i když třeba… já nevím, řekneme si, tak na těchhle stránkách si to najdete, jo, tak… myslím si, že stejně potom jakoby každej přijde a řekne, hele, jak to je, jo, a… nebo prostě myslím si, že polovina tady učitelů z toho prvního stupně takových jakoby bude."

dramatickým učením, protože to aktivizuje nejen děti, ale i učitele. Tyto lekce by sice měly sloužit k předání znalostí, ale na takové úrovni, kterou učitelé opravdu potřebují a s ujištěním, že téma zvládnou.

Pokud si knihovna dokáže vybudovat postavení instituce pro osvětu v bezpečnosti digitálních stop, podaří se jí získat přístup k veřejnosti, jejíž zájem o vzdělávání nejen v této problematice je v současnosti omezený. Dotazovaní vyjádřili přesvědčení, že má smysl směřovat i k tomuto cíli a věřit, že se osvědčení lekcí pro veřejnost rozšíří. Pro tuto skupinu, z níž knihovna může zaujmout z počátku jen omezenou část, je proto schůdné využít elektronické formy osvěty, např. matka doporučuje sekci o informační bezpečnosti pro dospělé na webových stránkách knihovny. Nemusí se jednat jen o materiály vytvořené knihovnou, ale i o rozcestník na ověřené informační zdroje, které jsou podle matky špatně dostupné[510]. Ředitel zmiňuje i možnost webinářů pro tuto cílovou skupinu, především v malých knihovnách, protože nevěří v návštěvnost fyzických lekcí, které by jinak preferoval on i knihovnice.

9.4.2.6 Evaluace realizované lekce

Názory uvedené v předchozích kapitolách představují obecný přístup dotazovaných k problematice této dizertační práce. Je možné předpokládat, že tyto názory byly ovlivněny realizovanou lekcí, stejně tak jako opačný vliv lekce na formování názorů. Pro akční výzkum je ale klíčový výsledek evaluace s tím, že vlivy jsou kontrolovány triangulací dat.

Průběh lekce byl i s odstupem hodnocen velmi pozitivně, dotazovaní sami upozornili na potvrzení většiny teoretických východisek zohledněných při tvorbě lekce (viz kap. 8.1.2 Aktivní učení a model E-U-R a navržená koncepce v kap. 8). Forma aktivního učení přispěla k tomu, že i méně motivovaní jedinci se zapojili a o tématu diskutovali na lekci i po ní, nechali se strhnout ostatními. Již při lekci se děti ptaly na navazující vzdělávání v rámci školy. V efektech aktivního učení podle knihovnice hrála roli zkušenost dětí s lekcemi v knihovně podobného formátu, efekt by se objevil, i kdyby neproběhly, ale nebyl by tak silný. Učitelka i žákyně hodnotily pozitivně délku i obsahovou vyplněnost, které vedly k zapojení dětí

[510] Matka: „Protože vlastně nikde se k tomu nedopracujete, asi by člověk musel hodně hledat, buď už v odbornejch pracích, jo, nebo už třeba v nějakých speciálních článcích, bych třeba řekla,“

v průběhu celé lekce[511]. Učitelka vyjádřila silnou spokojenost s formou lekce, která byla pro ni i pro děti v tomto tématu nová, toto hodnocení ji vedlo k projevům zájmu rozšířit její využití i pro další ročníky ve škole (viz níže).

Dotazovaní vyjadřovali přesvědčení o uskutečnění simulačního efektu ve fázi uvědomění významu v lekci (i když s omezením odhadu identity dle rukopisu), který dětem umožnil, aby si samy uvědomily žádané poznatky v bezpečí knihovny[512]. Knihovnice pouze doporučila, aby při efektivním průběhu nebyla aktivita ukončována z časových důvodů, dokud děti zjišťují nové skutečnosti[513]. Lekce ukázala, že některé děti mají poměrně dobré znalosti v informační bezpečnosti, ale jiné o ní téměř netuší. Oběma skupinám dětí ale lekce otevřela téma, nad kterým by měly přemýšlet, což často nedělají, i když znalosti k tomu mají[514], bylo tedy dosaženo stanoveného i požadovaného cíle podle všech dospělých dotazovaných.

Z hlediska 3. úrovně Kirkpatrickova modelu evaluace byly uváděny i dlouhodobé pozitivní důsledky lekce u dětí. Všichni dotazovaní vyjádřili, že lekce s odstupem několika měsíců sice nevedla k tomu, aby děti dokázaly odříkat představená pravidla, ale při řešení vzniku digitální stopy se zamyslí, poskytnou nebo neposkytnou ji vědomě se zvážením důsledků, a tím je jejich chování častěji bezpečné, než kdyby lekce neproběhla[515], i když si to třeba neuvědomují. Jedná se

[511] Učitelka: „slepé místo tam nebylo, protože furt ty děti vlastně byly v akci, že jo, furt něco dělaly, (…) ani se jim nějak nechtělo, že jo, že by klidně v tom ještě pokračovaly, takže si myslím, že byly… opravdu… jako že pracovaly celé ty dvě hodiny, že byly docela v tahu."

[512] Knihovnice: „myslím si, že velkou devizou té lekce je, že děti si vlastně na všechno přijdou sami. Že si to vyzkouší a uvědomí si, jak se chovat a možná si spíš uvědomí, že to, jak se chovají teď, může mít své důsledky. (…) Protože těm dětem úplně nedochází, se nedívají na to tak, jako by do budoucna. A je dobré, že si to vyzkouší tam, kde se cítí v bezpečí, v kolektivu, který znají a v podstatě s oporou ať už toho knihovníka nebo toho učitele.

[513] Knihovnice: „Ve chvíli, kdy se ta hlavní část té hry a uvědomění si, mnohem víc rozjede, a je vidět, že ty děti komunikují, že je to baví a že si i mezi sebou vlastně navzájem povídají o tom, jaké otázky jsou vhodné, kdo se jich kdy třeba na internetu na co ptal, a zkouší to na ty své spolužáky aplikovat, tak bych tu hru asi úplně násilně neutla s tím, že potřebujeme 15 minut na závěrečnou aktivitu, už bych s dětmi na konci jenom prodiskutovala, a třeba tu závěrečnou tabulku, kde už přiřazují konkrétní výroky, tak bych jim klidně nechala do školy."

[514] Učitelka: „ta první, první lekce, že… že si myslím, že jim dala dost, jo, že byly… že samy byly překvapený jakoby, co… že zjistily, jakoby co můžou, co nemůžou, jo, že opravdu je to, asi jim to normálně nedojde. Jo, když u toho počítače sedí. Něco tam nacvakaj a myslej si, no jo, tak to pošle, ale že si potom jakoby zpětně uvědoměj, to asi normálně u toho počítače není, kdežto tam si myslím, že opravdu… já, já jsem byla spokojená.

[515] Ředitel: „přestože si nemyslím, že by ty děcka dokázaly jako odříkat nějaký poučky nebo nějaký pravdy, který prostě se tam dozvěděly, tak podle mě je přesně todle (…) ta důležitá věc, protože oni až se dostanou do týdle tý situace, (…) to prožití tomuhle toho způsobí to, že, že to tomu dítěti, myslím si, jako naskočí. Že už někdy, zatímco teď, když sedí a chatuje, tak de facto nemá nějakej základ, nemá ten impulz k tomu se nad tím zamejšlet, což prostě děti jako dělávají, to ne…

o postoj vžitý praktickým nácvikem na lekci. Samozřejmě to nezaručí, že negativní digitální stopu děti nevytvoří, jsou si ale vědomy, co je správné, a když se podle toho nechovají, tak si to uvědomují. Současně je z vyjadřování matky i žákyně evidentní, že digitální stopu vnímají i na její rovině pozitivní, pokud prezentuje znalosti a dovednosti (např. blog nebo umělecká videa).

V konkrétních případech práce s digitálními stopami byly dcerou a matkou uváděny podle nich vhodné postupy při registraci k různým službám, především k Facebooku, dále pravidla pro silou autentizaci a práci s fotkami v elektronickém prostředí, které byly vztahovány k poznatkům řešeným na lekci[516]. Při registraci žákyně nyní postupuje obezřetně, registruje se jen v případě, že je to opravdu nutné, pokud zváží, že není, tak je ochotná si i odepřít obsah, o který měla zájem, ani se nepodívá na požadované údaje[517]. V případě, že k registraci chce přistoupit, tak vkládá falešné údaje, kde je to možné. Žákyně vyjádřila názor, že když v registraci je zadán e-mail, je tím prozrazeno i jméno, i když uživatelské jméno je falešné, nezvažovala možnost e-mailu ve tvaru bez jména[518].

V případě, že by žákyně chtěla vytvořit skutečný profil, např. na Facebooku pro komunikaci se spolužáky, kde musí uvést určité informace pravdivé, zdůrazňovala uvedení jen nezbytně nutných údajů (v žádné představitelné službě by nebyla ochotná udat např. rodné číslo a e-mailovou adresu), tj. jen křestní jméno, ne příjmení, fotku by nepoužila vlastní, ale své kočky. To je totožný postup, jako zná od své kamarádky, a podobný jako u kamaráda, který je sice na fotce sám, ale v kapuci bez viditelného obličeje a s kytarou v ruce. Z hlediska zpřístupňování fotografií žákyně uvedla odstranění fotky ze svého profilu pro e-mailovou schránku, která ji zobrazovala. V případě používání sociální sítě popsala význam

nemyslím, nechci jako dělat, děti nejsou blbý, ale, ale vnímání nebezpečí je něco, co se učí, že jo, a zvlášť u něčeho tak nevině vypadajícího, jako, jako samotný počítač."

[516] Žákyně: „já jsem si třeba vzpomněla, jak jsme se bavili právě o těch sociálních sítích o takhle o těch bezpečnostech, jak se nemáme jako registrovat, nemáme dávat do toho ty svý fotky a takhle jako o těch věcech jsme se právě bavili, tak na to jsem si hlavně vzpomněla. Ale ono už je to opravdu hodně dlouho"

[517] Žákyně: „Pokud není jako na něco potřeba registrace, a když je, tak to prostě nechám, protože třeba na filmy, třeba někde, na tom Voyo, třeba, to je…"

[518] Žákyně: „musíš mít nějaký přihlašovací jméno, takže to je… to si vymyslíš, ale pak je třeba ten e-mail, že jo. Ale jako to si, to tam prostě musíš zadat ten e-mail, ale jako, že jo, to prostě tam musím… takže si ho můžeš třeba dát kokoko, ale musíš tam mít svůj e-mail na svý jméno."

autorizace[519] a také několik pravidel pro silná hesla, která ilustrovala na podobě hesla její kamarádky, které žákyně z části znala.

Poslední úroveň Kirkpatrickova modelu směřuje k výsledkům lekce na okolí vzdělávaných. Zde dotazovaní popisovali především vliv na prostředí školy a rodiny a také zahájení diskuze o tématu mezi dětmi, která podle učitelky probíhala několik dní po lekci spontánně z podnětů dětí. Dospělí dotazovaní vyjádřili přesvědčení, že lekce vedla k diskuzi dosti velké části dětí s rodiči o bezpečnosti digitálních stop iniciované dětmi. Přestože tento výsledek nebude u všech dětí, podle učitelky: „*i kdyby, já nevím, čtvrtina, jo, to s těma rodičema probrala, tak si myslím, že i to je veliká zásluha*“, současně vyjádřila přesvědčení, že vlivem této diskuze byla zahájena i kontrola a zamezení rizikových činností v oblasti digitálních stop. Matka toto přesvědčení z části potvrdila, omezení diskuze podle ní bylo vlivem toho, že se zamyslela nad činnostmi žákyně na internetu a posoudila je jako dostatečně bezpečné[520]. Diskuzi podle ní výrazně více vyvolaly otázky, které dostala pro přípravu k rozhovoru, podobný materiál by proto uvítala po lekci, aby na ni mohla navázat i ona v rodině, a to jak v komunikaci s žákyní, tak i pro ujasnění přístupu k bezpečnosti vlastních digitálních stop[521]. Vlivem lekce tedy může dojít k sekundárnímu předání poznatků rodičům a také k zjištění na jejich straně, že tu knihovna je k dispozici i pro toto téma, což se stalo i u dotazované matky. Pokud bude lekce kvalitní, tak zejména na malém městě se to dle dotázaných rozšíří, a tím se ovlivní názory rodičů, ať už původně byly jakékoli.

Rozhovory přinesly poznatky také o vlivu lekce ke škole. Jak již bylo uvedeno v kap. 9.4.2.3, před lekcí se objevovaly obavy na straně učitelek z pojetí

[519] Žákyně: „Tak jako třeba ono je dobrý, (…) že si zadáš nějaké přihlašovací jméno, (…) teď si tam dáš nějaký heslo. A někdo to má udělaný tak, že třeba když se podíváš na tu jeho stránku, když dáš to jeho přihlašovací jméno jako do vyhledávání, tak jako tam… tam jako se ti jako objeví třeba, že, že, jestli ho znáš, tak jako jestli ho máš v přátelích, tak se na něj můžeš podívat, ale jinak je to zamčený jako ta stránka. A někdo třeba má i kontrolní otázku, kdyby se mu tam někdo chtěl dostat a kdyby třeba uhád to heslo, tak se mu tam ještě objeví jako kontrolní otázka, že třeba… co má Anička nejradši za jídlo. A takhle jako. A to už je pak jako těžší, pokud to není někdo, kdo opravdu je známej, kdo to jenom prostě tak… nějak si zjistil…“

[520] Matka: „nějak hodně jsme o tom nemluvily. Právě proto, že mně přišlo, že Jůlinka se tolik nepohybuje v nějakým úplně nebezpečným prostředí, no. Nebo nebezpečným, pohybuje, ale nedělá tam snad tolik stop.“

[521] Matka: „já to pořád beru, že je to velká, jako velká… zbraň, která může bejt i nebezpečná, ale až teprve když jsem si to přečetla, tak mě to jako, všechno jsem si to dala do kupy. Přestože jsem si četla ty svý smlouvy a vlastně jak to technicky asi tak může vypadat, jo, ale malinko jako člověk něco cítí, když už víte, jak hodně často něco vidíte, tak jako vám to tadyhle někde jako bliká, něco děláte instinktivně, jo, ale pak si to musíte jako sestavit, no. Tak malinko jsem si to sestavila.“

tématu. I přesto se na ni přihlásily, aby si ji vyzkoušely a následně hodnotily pozitivně její nastavení. Podobně jako pro matku, i pro učitele by podle dotazovaných prospělo k přenesení výsledků lekce do jejich prostředí poskytnutí materiálu knihovníkem, bez kterého bylo řešení problematiky ve škole omezené na diskuzi s dětmi nad materiálem z reflexe v lekci a nad informačními incidenty, které se v poslední době ve škole objevily. Učitelka dále uvedla, že důsledky lekce doznívaly v diskuzích několik dní, nicméně by uvítala, kdyby na lekci mohla s dětmi navázat ještě týž den ve škole[522]. Současně, stejně jako matka, pozitivně hodnotí vliv lekce i na své vlastní znalosti[523], především v oblasti digitálních stop, ale také poznání toho, co všechno děti v této oblasti znají a dělají.

Spokojenost zástupkyň školy s lekcí se odráží v jejich přímém hodnocení, lekce se jim líbila zejména proto, že se líbila dětem, současně byla přínosná[524] a obsah odpovídal plnění několika cílů stanovených ve školním vzdělávacím programu. Spokojenost se ale projevuje i v tom, že nechtěly na lekci nic měnit. Naopak ji chtěly nabídnout i dalším ročníkům ve škole, s případným drobným přizpůsobením pro jiný věk, než pro jaký je aktuálně určena. Toto rozšíření si učitelka i knihovnice dokázaly představit pro mladší děti (učitelka až od 2. třídy), ne pro starší věk, kdy už nejsou tolik otevřené, jak je potřebné pro soutěž. Silný důraz učitelka kladla na zajištění udržitelnosti lekce i dalších lekcí pro jiné ročníky, aby došlo k zajištění opravdu koncepčního přístupu, kdy každý rok budou děti navštěvovat navazující lekci v knihovně o bezpečnosti digitálních stop. V nejbližší době by učitelka uvítala lekci pro 3., 4. a 5. třídu, případně s jiným lektorem, pokud to bude jediná možnost udržení lekce v nabídce. Respondenti ze školy jsou tedy s řešením informační bezpečnosti v knihovně spokojeni, proto ji podporují a iniciativně se snaží o udržení a rozšíření nastaveného standardu ve frekvenci

[522] Učitelka: „možná by bylo ještě lepší, kdyby třeba ten seminář s Vámi nebo ta beseda, byla první dvě hodiny nebo první tři, aby jsme měly my možnost ještě návaznost zrovna ve třídě jakoby potom, jo, protože oni samozřejmě ten druhej den, jakoby, kdy se tomu vrátíme, ale už to, není to už úplně vono, že, jo."

[523] Učitelka: „Že mně to hodně dalo a, musím říct, že i jsem si spoustu věcí opravdu taky uvědomila, že to člověk bere jako automaticky, že jo, a když to potom jakoby slyší třeba od Vás, jo, tak… si to uvědomí asi daleko víc a… bych řekla jako obyčejnej člověk, jako, kterej se nad tím běžně nezamýšlí, jako, že si to fakt neuvědomí,"

[524] Učitelka: „Já si myslím, že ty děcka z toho byly docela nadšený, když tedy s Vámi tam pracovaly, a že přišly fakt spokojení. A že jim to hlavně i něco dalo, protože některý o tom vědí hodně, někteří o tom vědí málo,"

a cílových skupinách vzdělávání nejen o informační gramotnosti v tradičním pojetí, ale se zahrnutím informační bezpečnosti.

9.4.3 Závěry z výzkumu

Rozhovory přinesly zajímavá zjištění, a to v pozitivním i negativním aspektu, převládaly ale kladné přínosy lekce, které ani nebyly předpokládány, když např. matka žákyně uvedla, že lekce ji přiměla k diskuzi s dcerou i k zamyšlení jí samé o různých stránkách rizikové komunikace. Ze strany knihovny i školy bylo hodnocení tak pozitivní, že obě instituce trvaly na minimálně opakování, v ideálním případě i rozšíření lekce. Všichni dotazovaní se shodli, že knihovna má své místo ve vzdělávání o bezpečnosti digitálních stop, a to nejen při vzdělávání dětí.

Šetření ukázalo pohledy různých klíčových osob ve vztahu ke vzdělávání v knihovně o bezpečnosti digitálních stop, které byly spíše podobné než rozdílné. Byly identifikovány určité slabiny realizace lekcí, ale i možnosti řešení, které jsou ověřeny z jejich vlastní praxe. Tím byly definovány argumenty využitelné při diskuzi ohledně bariér na různých úrovních, které brání realizaci lekce jinde.

Dotazovaní sice identifikovali možné bariéry, ale poskytli ke všem také vodítka pro možná řešení. Znalostní bariéry knihovníků je vhodné řešit pomocí blended learningu a dostupností experta pro konzultace. Časové, provozní a materiální podmínky pro realizaci lekcí musí vytvořit vedení knihovny, které za to může získat hodnocení efektivity vzdělávání pro prezentaci zřizovateli při žádosti o podporu této činnosti, dalším argumentem ke zřizovateli i veřejnosti může být řešení vážného společenského problému knihovnou tam, kde se toho dosud nechopila jiná instituce. Bariéry na straně školy mohou odstranit obě právě uvedené argumenty, zásadní je především dobrá komunikace a vysvětlení, co škole lekce přinesou, včetně přizpůsobení výukovým cílům školy stanoveným v jejích školních dokumentech. To je pro učitele podstatné, vedle toho ti ale vyžadují, aby lekce byla pro děti přínosná a aby je dokázala zaujmout. Kvalita obsahu i formy vedoucí k zaujetí dítěte je řešením některých bariér i na této úrovni, děti internet zajímá, motivace je zde tedy velká, klíčové je ale na ni správně reagovat. I když je motivace slabší, tak ji lze zvýšit nastavením aktivního učení a strhnutím dítěte zájmem ostatních. Pokud dítě odejde z lekce spokojené, je nejlepším šiřitelem spojení vzdělávání v knihovně a bezpečnosti digitálních stop nejen mezi vrstevníky, ale

především v rodině, kde může otevřít diskuzi s rodiči a případně je přesvědčit, aby se sami nechali knihovnou vzdělat.

Představeny byly názory různých subjektů na to, co a proč funguje, kde byly jejich obavy, problémy i jejich řešení. Argumenty jsou rozvedeny ve výsledcích výzkumu výše, jejich základy lze shrnout pomocí SWOT analýzy v tabulce 10.

Tabulka 10 SWOT analýza realizace vzdělávání v knihovně o bezpečnosti digitálních stop z pozice knihovny dle rozhovorů

Silné stránky	**Slabé stránky**
- Lokální instituce nejvíce zaměřená na informace, média a IT. - Životní zkušenost v práci s IT. - Sdílený pocit potřeby vzdělávat o informační bezpečnosti, hl. digitálních stop. - Návaznost na již realizované vzdělávání (informační gramotnost). - Připravenost knihovníků mladší generace dovzdělat se, základní znalosti v informační bezpečnosti z vysokoškolského studia. - Zážívnější řešení témat vedoucí k lepšímu zapamatování. - Existence ověřené metodiky vzdělávání respektující specifika současných knihoven. - Již existující spolupráce knihoven a škol. - Stálá dostupnost v lokalitě (možný kontaktní bod). - Vyvolání větší otevřenosti pro hledání řešení rizikových a problémových situací na internetu. - Hodnocení více jako sumativní, než formativní.	- Knihovny jako reprezentace hodnot, služby omezeny na půjčování knih. - Ne vždy kvalitní elektronické služby. - Personální nepřipravenost koncepčně vzdělávat v potřebném rozsahu (pozice lektora, pedagogické schopnosti). - Omezený rozpočet vedoucí k omezeným lidským zdrojům (úvazek na vzdělávání omezením jiné práce). - Obava z řešení nedostatečně známého tématu s dětmi, které IT rozumí více než většina knihovníků.
Příležitosti	**Hrozby**
- Aktuální situace společenské poptávky, kdy se očekává subjekt, který ji bude řešit. - Lekce i jako osvěta o knihovně samotné. - Omezení mediace právními předpisy. - Nedostatečnost aktivní mediace u rodičů a učitelů. - Budování expertní pozice v lokalitě pro práci s informacemi a IT. - Navázání vztahu s perspektivními uživateli knihovny (dětmi). - Řešení tématu v rámcovém vzdělávacím programu. - Doplnění poznatků o bezpečnosti digitálních stop předávaných rodiči a učiteli pro rozšíření množství dětí dotčených tématem (každému může vyhovovat jiná forma).	- Pokrytí tématu jinou místní organizací, když se jej neujme knihovna, např. síť prevence na městském úřadě, dům dětí a mládeže, informační centrum pro mládež, kulturní centrum a muzeum, příp. při dotacích od města nebo ve velkém městě komerční subjekt (nebo projekt).

Témata, která respondenti pro vzdělávání dětí v knihovně vyzdvihli, odpovídají nejčastějším problémům v praxi[525]. Podobně odpovídá odborným doporučením[526] zájem o zaměření na principy bezpečného chování, ne tolik o technické či právní aspekty informační bezpečnosti. Ve výzkumu se potvrdilo, že knihovna je u dětí jedním ze zdrojů pomoci pro děti, ale není tolik pro tento účel využívána rodiči[527], předchozím výzkumům odpovídá i shoda respondentů, že spolupráce školy a knihovny ve vzdělávání o informační bezpečnosti může mít pozitivní dopady na všechny zúčastněné[528].

Součástí rozhovorů byla také poslední fáze evaluace realizované lekce, která se i na 3. a 4. úrovni Kirkpatrickova modelu ukázala jako efektivní. Pozitivně ji hodnotili všichni dotazovaní, drobné připomínky k průběhu lekce byly zohledněny v úpravách navržené koncepce vzdělávání v kap. 8.2. Lekce splnila stanovený cíl v dlouhodobém postoji při vzniku digitálních stop dětí, které nyní ví, jak by měly postupovat, jejich činnost je pak dána vědomým a uváženým rozhodnutím. Vedle toho ale lekce zapůsobila i na okolí dětí, tj. učitelku a rodinu žáků, kde následovala diskuze z podnětů dětí, jejímž výsledkem bylo zvýšení aktivní a někdy i restriktivní mediace v domácím použití internetu dítětem, ale materiály poskytnuté v lekci, příp. v návaznosti na ni pro rozhovory vedly i k zamyšlení dospělých o jejich vlastní práci s digitálními stopami a znalostmi práce dětí při jejich tvorbě a správě.

Přestože se bariéry mohou objevit, není možné dopředu je očekávat a věřit v jejich nepřekonatelnost, rozhovory prokázaly reálnost praktické aplikace navrženého konceptu v této dizertační práci. Právě ukázka fungování nasazené koncepce s pozitivními důsledky pro všechny strany by měla vést k přesvědčení dalších knihoven, že není důvod nezkusit to i ve vlastní instituci a využít výhod, které tato spolupráce ve vzdělávání přináší.

[525] LIVINGSTONE 2011
[526] RANGUELOV 2010; MARTIN 2012
[527] LIVINGSTONE 2011
[528] MARTIN 2012

9.5 Limity akčního výzkumu

Omezením této případové studie je jistě její regionální zaměření. Jedná se o jedinou případovou studii, která je tedy samozřejmě ovlivněna prostředím a okolnostmi realizace lekce. Z toho důvodu byly tyto souvislosti podrobně popsány a je připravována validace výsledků opakováním lekcí v dalších prostředích, a to z hlediska velikosti obce i množství zkušeností škol s vzděláváním dětí v knihovnách, zvažováno je také ověření aplikovatelnosti lekce do jiných vzdělávacích institucí, a to v rámci formálního i neformálního vzdělávání. Toto srovnání by mělo ukázat, do jaké míry jsou výsledky průkazné pro doložení potenciálu neformálního vzdělávání nejen v knihovnách pro zvyšování internetové bezpečnosti dětí. Výsledky zde řešeného zúčastněného pozorování také budou dále komparovány z dalších aplikovaných výzkumných metod. Pro triangulaci metod byla jako součást akčního výzkumu využita také dokumentová analýza zpráv vytvářených v hlavní části lekce a rozhovory s různými subjekty ve vztahu k lekci, tj. učící knihovnice, ředitel knihovny, učitelka, zástupkyně ředitele, žákyně a její matka. Rozhovory byly použity také pro zhodnocení subjektivity zúčastněného pozorování, které realizoval jediný výzkumník. K tomu bylo využito především informací od knihovnice a učitelky, které se zúčastnily lekcí.

Omezením akčního výzkumu obecně je nemožnost jeho zobecnění na širší populaci, je pevně svázán s prostředím, ve kterém je realizován. Jeho cílem ale není potvrzení obecně platných závěrů. Jak bylo konstatováno již v úvodu akčního výzkumu, jeho smyslem je představit funkčnost a možné přínosy realizace navržené metodiky vzdělávání o digitálních stopách. Pro zobecnění výsledků by bylo nutné použít jiné výzkumné metody a také cíl šetření by byl odlišný, jde již nad rámec této práce nejen vymezením, ale především časovými možnostmi. Rozšíření realizace koncepce se bude pohybovat pravděpodobně v řádech let a je pro něj nezbytné doložení, že se jedná o dobrou praxi, kterou je vhodné vyzkoušet i ve vlastní knihovně.

S ohledem na specifika akčního výzkumu se autoři shodují[529], že při hodnocení jeho důvěryhodnosti je nutné aplikovat jiná kritéria než v tradičním

[529] PICKARD 2013, s. 163

kvalitativním výzkumu. K hodnocení realizovaného akčního výzkumu je použito klasifikace validity[530]:

- Demokratická validita: Kritérium lze považovat za naplněné, ke kolaboraci výzkumníka a participantů ve všech fázích cyklu akčního výzkumu došlo. Formování lekce probíhalo na základě reakcí a činností žáků a učitelů a průběžným konzultacím s knihovníkem přítomným na lekcích, menší, ale stále vliv na úpravy lekce měly také dvě konzultace s ředitelem knihovny a dvě se zástupkyní ředitele, nejmenší zásahy vzhledem k nejslabšímu zapojení do lekce měly podněty od matky žákyně. Vlivy subjektů jsou popsány v rámci všech tří šetření, každé totiž představovalo jeden nebo více cyklů akčního výzkumu.

- Výstupní validita: Realizované intervence se vždy ukázaly jako pozitivní v dalším cyklu, někdy se ale zásahem objevily nové problémy. Především doplnění pravidel při identifikaci nevhodného postupu (např. zjištění identity z e-mailu, rukopisu apod.), který se ve třídě rozšířil, takže se neprojevil jiný, po zásahu vedl k objevení odlišného nevhodného postupu. Poslední tři cykly (2. rok výzkumu) již ale ukázaly saturaci výzkumu, kdy významnější intervence nebyly nutné.

- Procesní validita: Toto kritérium je obvykle zajišťováno triangulací metod sběru dat, která byla využita. Cílem je podpořit, že výstup je efektem realizovaných procesů. Triangulace v popsaném výzkumu skutečně vedla k vzájemnému potvrzování výsledků.

- Katalytická validita: V rámci výsledků jednotlivých výzkumů byla snaha co nejlépe popsat a triangulací potvrdit, že proces akčního výzkumu opravdu vedl ke změně u všech zúčastněných vlivem jejich vlastního přispění. Přijetí vlastní role v akčním výzkumu si byli vědomi dospělí, u dětí se výzkumem nepodařilo prokázat, svůj přínos pro změnu si pravděpodobně příliš neuvědomovaly.

- Dialogová validita: Kritérium akcentuje vliv na intervence nejen na základě názorů jednotlivých účastníků, ale i vliv komunikace mezi vrstevníky (resp.

[530] HERR, Kathryn a Gary L. ANDERSON. The action research dissertation: a guide for students and faculty. In: PICKARD 2013, s. 163-164

ostatních ve stejné pozici, např. učitelů, v angličtině *peer review*). Ten se prokázal na straně dětí a školy v rozhovorech, v případě rodičů a knihovníků tento typ validity není zjištěn.

Existuje více dalších přístupů k hodnocení validity akčního výzkumu, které ale akcentují velmi podobná kritéria, není nutné se vyjadřovat k více různým přístupům. Podstatným společným rysem mnoha kritérií v různých kategorizacích je především přínos akčního výzkumu pro participanty. Akční výzkum vznikl v místě realizace na základě podnětu od participantů, konkrétně ředitele knihovny a knihovnice, jak se ukázalo v rozhovorech, původ podnětu byl ještě před tím u zástupkyně ředitele školy. To odpovídá doporučením pro akční výzkum, který, přestože je součástí dizertační práce a naplněním jejího cíle, byl iniciován samotnou cílovou skupinou výzkumu. Výsledky pozorování a rozhovorů dále ukazují, že všichni přímo dotazovaní a většina subjektů pozorování a dokumentové analýzy, jsou přesvědčeni o pozitivních důsledcích akčního výzkumu nejen v době jeho provádění, ale také následně po převzetí knihovnicí vzdělávající v zkoumané knihovně v příštích letech. V tom se spojuje i dostatečné naplnění kritérií hodnocených v bodech výše.

9.6 Závěry z akčního výzkumu

Cílem akčního výzkumu bylo ukázat kvalitu nastaveného konceptu vzdělávání v knihovně o informační bezpečnosti, který odpovídá reálným podmínkám současných knihoven a staví na jejich možných pozitivních vlivech při řešení těchto lekcí. V průběhu šetření došlo k několika cyklům změn v koncepci, nejvíce problémů bylo odstraněno v rámci zúčastněného pozorování, které sloužilo k přímému hodnocení efektivity lekce na 1. úrovni Kirkpatrickova modelu. Po dostatečných úpravách proběhlo několik cyklů potvrzujících, že již změny v metodice nejsou potřebné, jen je nutné lekci vždy přizpůsobit konkrétní třídě, což odpovídá pedagogickým principům. V návaznosti na to byly hodnoceny dokumenty vytvořené na lekci pro zjištění edukačního efektu lekce, který se podařilo prokázat. Poslední realizované šetření v akčním výzkumu směřovalo na hodnocení chování a výsledků po lekci, pro potřeby dizertační práce bylo spojeno se zjišťováním

názorů klíčových subjektů ve vztahu k lekci na to, že by knihovna měla vzdělávat o bezpečnosti digitálních stop, protože „*v současnosti je vzdělávání nejlepší legální cestou vštípit dětem kulturu online bezpečnosti*“ [531].

Z dílčích výsledků je možné vyvodit, že se podařilo dosáhnout stanoveného cíle akčního výzkumu a upravit a ověřit efektivitu navržené lekce a do určité míry i celé koncepce, kterou tato lekce reprezentovala. Na lekci děti dospěly k žádoucím poznatkům vlastní činností, k čemuž bylo využito metod aktivního učení. Pomocí pozorování a dokumentové analýzy se podařilo prokázat výskyt požadovaných efektů aktivního učení ve všech aktivitách v lekci, ale také edukační efekt lekce. Přestože nebylo možné zcela prokázat simulační efekt jádrové aktivity v lekci, nebylo ho ani možné vyvrátit a v navazujících rozhovorech všichni dotazovaní vyjádřili přesvědčení, že k němu došlo.

Rozhovory ukázaly, že všichni dotazovaní považují řešení tématu této práce v praxi za přínosné pro všechny strany. Vycházejí přitom z vlastní zkušenosti s realizovanou lekcí. Díky tomu mohou posoudit, co bylo správně, a to jak při samotné lekci, tak při nastavování spolupráce i v celém navrženém konceptu vzdělávání o bezpečnosti digitálních stop. Část rozhovorů sloužila pro evaluaci lekce, takže výsledkem byla i mírná úprava koncepce (především doplnění části otázek pro rodiče), většina zjištění ale spíše směřovala k argumentům, proč by knihovny měly vzdělávat o bezpečnosti digitálních stop, a to primárně děti, v druhé řadě učitele a nakonec i rodiče a širokou veřejnost. Rozhovory potvrdily, že východiska popsaná v teoretické části této práce jsou reálná, i když v některých místech nemusí vše proběhnout tak snadno jako u zapojených institucí, protože ty byly vybrány kvůli zvýšenému zájmu o toto řešení. Je ale dosti pravděpodobné, že získané argumenty i ověřená efektivita lekcí povedou k rozšíření zájmu a aplikaci do praxe i v jiných místech. Je totiž možné, že koncepce nebude některou ze stran přijata, ale jak ukazuje tento výzkum, je jisté, že alespoň někde přijata bude.

Je tradiční rolí knihoven, že učí rozlišovat mezi důvěryhodnými a nedůvěryhodnými informačními zdroji, a to jak v případě dokumentů, tak i lidí. A právě toto je základem mnoha informačních hrozeb, především ve spojení s digitálními stopami, i jejich vhodného řešení, které by mělo spočívat především v uvážlivém chování po rozmyšlení důvěryhodnosti zdroje a možných důsledků

[531] CHANG 2010, s. 527

poskytnutí informace. Knihovny by proto měly pokračovat v této dlouhodobé činnosti a rozšířit ji o problematiku řešenou v této práci, protože tím budou reflektovat současné potřeby společnosti. Samozřejmě nejen knihovny by měly vzdělávat o tomto tématu, neměly by ale spoléhat na jeho pokrytí učiteli nebo rodiči, protože knihovna může podpořit jejich činnost vzhledem ke svému potenciálu představenému v kap. 4.3. Jak učitelé a rodiče, tak i knihovny mohou přinést potřebné poznatky z různých pohledů, takže zasáhnou větší množství dětí, vhodná je také jejich spolupráce pro pomoc dětem v oblasti znalostí i řešení informačních incidentů. Dítě, ale i dospělý pak má možnost vybrat si instituci, člověka i přístup, který mu pro lekci i řešení problému nejvíce vyhovuje, což je v tomto citlivém tématu velmi vhodné. Akční výzkum ukázal, že spolupráce mezi školou, knihovnou a rodinou je nejen možná, ale pro všechny strany i přínosná.

10 Závěr práce

S rostoucím významem informací, informačních technologií a internetu pro potřeby společnosti v různých využitích od fungování kritických infrastruktur státu po volnočasové aktivity jedince, roste také význam informační bezpečnosti. Pro její efektivní aplikaci je nutné řešit jak technickou, tak uživatelskou stránku práce s informacemi, kdy především druhá jmenovaná oblast je blízká činnosti knihoven, které se dlouhodobě věnují podpoře uživatelů při práci s informacemi.

Jak bylo představeno v teoretické části práce, v oblasti informační bezpečnosti jednotlivců, se kterými knihovny pracují, je zásadním rizikovým faktorem nevhodné zpřístupnění digitálních stop. Protože informační hrozby je často zneužívají a obrana proti nim je nejefektivnější v rámci prevence, je nutné věnovat se řízení vzniku a správě digitálních stop. Jak je prezentováno podrobně v teoretickém ukotvení problematiky, toto téma spadá do informační gramotnosti, k jejímuž rozvoji se knihovny hlásí, a právě ony mají významný potenciál kterak přispět ke zvýšení povědomí veřejnosti prostřednictvím vzdělávání formou lekcí i poradenství v případě vzniku problému. Tento potenciál je z části specifický pro Českou republiku, většina definovaných východisek je ale rozšiřitelná i na jiná prostředí. Proto je možné se částečně inspirovat zkušenostmi zahraničních, především anglo-amerických knihoven, které se vzdělávání v oblasti digitálních stop v současnosti již silně věnují. Zaměřují se na jednu stranu na bezpečnostní rizika s nimi spojená, ale současně budování tzv. pozitivní digitální stopy, jejímž smyslem je vytvářet prezentaci člověka, která jej podporuje a je jen omezeně zneužitelná, slouží především k předvedení jeho schopností a osobnosti jeho okolí, ať už přátelům nebo zaměstnavateli. Tento trend pravděpodobně nezmizí, proto je spolu s představeným potenciálem českých knihoven pravděpodobné, že i v současnosti spíše nahodilé formy vzdělávání v knihovnách o bezpečnosti digitálních stop se budou postupně rozšiřovat a usazovat v nabídce především pro školy. Knihovny současně přestávají mít význam pouhého zprostředkovatele informací, kterých je s internetem dostatek, jejich role je ale stále v řízení zprostředkování a předávání této schopnosti, což odpovídá i předmětu této práce.

Tato dizertační práce si stanovila dva základní cíle. Protože v době zahájení řešení tématu mohla vycházet jen z omezených informací k tomu, jak se knihovny věnují bezpečnosti digitálních stop při vzdělávání dětí, bylo nejdříve nezbytné

zmapovat, zda vůbec k něčemu takovému v českých knihovnách dochází, příp. na jaké úrovni. První dvě dotazníková šetření v letech 2011-2012 prokázala, že knihovny téma zcela neignorují, věnují mu ale omezenou pozornost, stále preferují, především ve vztahu k dětským uživatelům tradiční témata, jako je čtenářství. Naprostá většina knihovníků ale vyjádřila přesvědčení, že vzdělávat děti v tomto směru je důležité. Pravděpodobně i z toho důvodu sami projevili zájem o vlastní rozvoj v oblasti informační bezpečnosti (na kterou byl kvůli nejasnému řešení problematiky v praxi první dotazník zaměřen), kterou pro své potřeby zaměřovali právě především na bezpečnost digitálních stop.

Knihovny jsou ve vztahu k bezpečnosti dětí na internetu ve složité situaci, protože musí vyvažovat svobodný přístup k informacím a ochranu dětí. Technické prostředky jsou omezeně využitelné ne tolik kvůli jejich finanční náročnosti, jako spíše kvůli tomu, že vedou právě k omezení svobodného přístupu k informacím. V knihovnách je problematická také mediace na úrovni monitoringu, protože knihovny musí zachovávat informační soukromí dětí, nemohou proto sledovat vše, co se objevuje na monitoru nejen dětem, ale třeba i dospělým, kteří sedí na počítači vedle dítěte. V současnosti proto mediace v knihovnách představuje nevyřešenou otázku, ke které se přistupuje různě a ne vždy vhodně, přestože se knihovny snaží postupovat co nejlépe v rámci svých možností. Z toho vyplývá, že nejschůdnější formou, a podle výzkumů také nejefektivnější[532], je aktivní mediace formou učení dětí, jak se vhodně chovat při práci s digitálními stopami.

Omezené řešení tématu ve vzdělávání v knihovnách může být způsobeno obavami z toho, že by knihovníci ztratili své postavení autority a experta, protože děti mají často lepší znalosti informačních technologií než oni, proto není snadné se je pokoušet něco v tomto směru učit. Jak ale vyplývá z této práce, obava není zcela na místě, protože i přesto, že děti mají často rozsáhlé znalosti internetu, jsou často omezeny na část problematiky, která obvykle vychází z toho, co je baví. A to informační bezpečnost příliš není. Nelze popřít, že i v ní děti znalosti mají, slabší je to ale podle výzkumů[533] s jejich dovednostmi a postoji. České děti se chovají dosti silně rizikově, k čemuž patří i nevhodné řízení vzniku digitálních stop. Proto by je knihovníci měli v tomto směru podpořit tím, že je dovedou k tomuto postoji,

[532] DUERAGER 2012
[533] Např. LIVINGSTONE 2011

především zprostředkováním životní zkušenosti s informačními technologiemi, ale i bezpečností obecně, protože bezpečnost digitálních stop vychází ze stejných základů, které jen rozšiřuje o specifika své formy. Knihovníci proto mohou využít svých specifických znalostí, především v hodnocení a třídění informací a zdrojů, ve kterých spočívá i bude spočívat jejich přínos.

Následně proto bylo nutné zjistit, s jakými znalostmi knihovníků může navržená koncepce vzdělávání operovat a zda vůbec má smysl připravovat vzdělávání dětí knihovníky, nebo bude nejdříve nutné vzdělat samotné knihovníky. Didaktické testování prokázalo, že knihovníci již mají určité znalosti v problematice, které jsou obvykle dostatečné pro lekce v požadovaném rozsahu na základní škole, pro návaznosti v práci se staršími studenty a dospělými je ale vhodné je dále podpořit. Jak bylo možné očekávat vzhledem k zaměření služeb knihovny, znalosti knihovníků jsou vyšší v oblasti bezpečného chování než v technických možnostech ochrany, což odpovídá i pravděpodobnému očekávání uživatelů knihovny. Podle výsledků všech tří výzkumů mapujících situaci v českých knihovnách v řešeném zaměření není knihovníkům nutné vysvětlovat význam problematiky, ale spíše ji přenést do reálných možností jejich práce, protože osobní motivace je základem rozvoje jejich znalostí a tím také vytvořením předpokladů, aby byli schopní o bezpečnosti digitálních stop vzdělávat.

Přes omezenou úroveň znalostí je možností podpory knihovníků pro vlastní rozvoj i zavedení tématu do nabídky vzdělávání metodika lekcí o bezpečnosti digitálních stop pro žáky 3. – 9. třídy základních škol a odpovídajících ročníků středních škol, protože uvádí téma do reálných možností většiny knihoven. Z toho důvodu je metodika vytvořena s co nejnižšími požadavky na vybavení. Lekce jsou postaveny na formátu aktivního učení, aby podpořily specifika knihoven pro vzdělávání a současně byly co nejefektivnějším doplněním vzdělávání ve škole nabídkou alternativního přístupu k potřebnému tématu, které podle rámcových vzdělávacích plánů musí být nějakým způsobem školou řešeno. Součástí metodiky je také materiál, který by měl sloužit pro zahájení diskuze o řešeném tématu ve škole i rodině žáka, aby došlo k sekundárnímu přenosu znalostí i aktivní mediace i do ostatních klíčových prostředí pro dítě. Do metodiky byly také zahrnuty zkušenosti lektorů s realizací lekcí a materiály doporučené případným lektorům pro vlastní vzdělání, aby tímto byli podpořeni s omezením požadavků na lidské zdroje.

Základním záměrem dizertační práce, který ale nebylo možné naplnit bez předchozího popsaného cíle, bylo vytvoření metodiky vzdělávání v knihovnách o bezpečnosti digitálních stop, která by byla osvědčená a využitelná v současných podmínkách knihoven. K tomu bylo využito akčního výzkumu, který se pro ověření výsledků triangulací dat skládal ze tří větších šetření: zúčastněného pozorování, dokumentové analýzy produktů dětí na lekci a rozhovorů s klíčovými osobami ve vztahu k lekci. Tato šetření potvrdila, že lekce využívá možností aktivního učení, které děti baví a současně je pro ně přínosné, protože děti při něm samy získají potřebné znalosti a zkušenosti díky činnosti vlastní i ostatních spolužáků, dochází tedy k tzv. *peer teaching*, které je pro české děti nejpřijatelnější formou v oblasti informační bezpečnosti[534]. Dokumentová analýza potvrdila, že ve fázi uvědomění si významu děti získávají potřebné poznatky a do určité míry je možné potvrdit, že si je děti dokáží propojit s prostředím internetu při jeho reálném požití i v budoucnosti po lekci. K ověření tohoto vlivu i dalších výsledků byly využity rozhovory realizované s odstupem po lekci, které prokázaly efektivitu lekce hodnocenou pozitivně všemi zúčastněnými subjekty.

Vedle toho také rozhovory sloužily k získání obecného postoje dotčených osob na vzdělávání v knihovnách o bezpečnosti digitálních stop. I v tomto směru jsou zjištění pozitivní, což je do určité míry ovlivněno výběrem dotazovaných. Na základě zjištění sice není možné zobecňovat, že všichni tuto roli knihoven přijmou s nadšením, je ale možné konstatovat, že se mohou vyskytnout na různých stranách zavádění koncepce do praxe různé bariéry, ty ale jsou překonatelné. V případě, že dojde k nasazení konceptu, může přinést pozitivní důsledky pro všechny zúčastněné, nejen děti, které se chovají bezpečněji. Obsah lekce pro děti v knihovně se může přenést i na sekundární cílové skupiny, tj. učitele a rodiče, a vybudovat u nich jak určitou úroveň znalostí, tak také změnit přístup ke službám a potřebnosti knihovny. Lekce o bezpečnosti digitálních stop mohou být nejsilněji pociťovanou potřebou pro řešení, která v současnosti v lokalitách mimo velká města není řešena. Mohou se jí ujmout knihovny a získat tak vysokou přidanou hodnotu, ale pokud to neudělají, jsou dotazovaní přesvědčení, že se této společenské poptávky chopí jiná instituce. Je totiž nezbytné, aby se problematika v místě reflektovala, a to nejen lekcemi, ale i zajištěním kontaktního bodu pro řešení problémů. Otázkou tedy

[534] LIVINGSTONE 2011, s. 123-129

zůstává, zda se této funkce knihovny rozhodnou chopit a pokusí se takto o upravení své činnosti, aby více odpovídala potřebám společnosti v oblasti, která patří k jádru služeb knihovny.

Internet by měl být vnímán jako nástroj, s čímž je spojená možnost jeho využití i zneužití. Může tedy dětem přinést mnoho výhod, ale také je ohrozit. Při rozvoji dětí v práci s internetem je proto vhodné podporovat oba tyto směry. Většina zkušeností dětí s internetem je a pravděpodobně bude pozitivních, ale útoky mohou mít natolik negativní vliv, že je vhodné se jim věnovat, i když by mohly zasáhnout jen omezenou část dětí, protože není možné říct, která část z nich to bude. Je proto dobré stavět především na prevenci, ukázat, že vše má možné řešení a že pro dítě jsou k dispozici lidé, kteří mu pomohou. Vzdělávání je výrazně efektivnější než řešení právní nebo technickou cestou, jak bylo doloženo v na to zaměřených kapitolách, restrikce by měla být menší, aby dítě nemělo obavu se svěřit, protože porušilo nějaké pravidlo, ale také aby znalo vhodnou reakci, protože bude připraveno, že problémová situace může nastat. Současně lekce formou aktivního učení, které rozvíjí zkušenosti dětí v této oblasti, podpoří jejich schopnost rozpoznat problém a nalézt řešení. Je proto vhodné děti především vzdělávat pro zvýšení jejich bezpečnosti v oblasti digitálních stop a knihovny v tom mohou významně přispět.

Problém bezpečnosti digitálních stop je do značné míry postaven na nevhodném zhodnocení důvěryhodnosti šířených informací. Jedná se tedy o problém starý stovky let, s jehož řešením knihovny dlouhodobě pomáhaly. Nyní se jen dostal do nové formy v digitálním prostředí, ale zůstává stejně vážný, ne-li vážnější vzhledem k informační společnosti. Digitální stopy, jejich užití a odpovědné budování by měly byt řešeny knihovnami z mnoha důvodu popsaných v této práci. Podstatné je, že všechny tyto činnosti nejsou o ničem jiném než o vyhledávání a organizaci tohoto specifického typu informací, a to je to, co knihovny dělají a umí nejlépe. Proto by měly reagovat na tuto společenskou poptávku a do své odpovědi vložit vlastní expertízu, což ukáže, že knihovny nejsou překonané instituce, ale jsou klíčové pro podporu digitálního občanství, kterému se stále přibližujeme.

11 Seznam použité literatury

11.1 Monografie a kapitoly v knihách

BELZ, Horst a Marco SIEGRIST. 2001. *Klíčové kompetence a jejich rozvíjení: východiska, metody, cvičení a hry*. Vyd. 1. Praha: Portál, 375 s. ISBN 8071784796.

BJØRNÅVOLD, Jens a Aviana BULGARELLI. 2008. *Validation of non-formal and informal learning in Europe: a snapshot 2007*. Luxembourg: Office for Official Publications of the European Communities, 48 s. ISBN 92-896-0509-X. Dostupné z: http://www.cedefop.europa.eu/EN/Files/4073_en.pdf

BOTT, Ed a Carl, SIECHERT. 2004. *Mistrovství v zabezpečení Microsoft Windows 2000 a XP*. 1. vyd. Brno: Computer Press, 696 s. ISBN 80-722-6878-3.

BYČKOVSKÝ, Petr. 1982. *Základy měření výsledků výuky: tvorba didaktického testu.* Praha: ČVUT.

CEJPEK, Jiří. 2005. *Informace, komunikace a myšlení*: *úvod do informační vědy*. 2. přeprac. vyd. Praha: Karolinum, 233 s. ISBN 80-246-1037-X.

CIVALLERO, Edgardo. 2007. Action-Research application in Evidence-Based practice for libraries. In: *IFLA Conference Proceedings* [online]. s. 1-7 [cit. 2014-08-30]. Dostupné z: EBSCOhost

COX, Christopher N. a Elizabeth Blakesley LINDSAY. 2008. *Information literacy instruction handbook*. Chicago: Association of College and Research Libraries, 236 s. ISBN 978-083-8909-638.

ČÁP, Jan. 1993. *Psychologie výchovy a vyučování*. 1. vyd. Praha: Univerzita Karlova, 415 s. ISBN 80-706-6534-3.

FISH, Tony. 2009. *My digital footprint: a two-sided digital business model where your privacy will be someone else's business!*. London: Futuretext, v, 191 s. ISBN 978-095-5606-984.

FONTANA, David. 1997. *Psychologie ve školní praxi: Příručka pro učitele*. 1. vyd. Praha: Portál, 383 s. ISBN 80-717-8063-4.

GRAYSON, Robert. 2011. *Managing your digital footprint*. 1st ed. New York: Rosen Central. ISBN 14-488-1319-0.

GRECMANOVÁ, Helena, Eva URBANOVSKÁ a Petr NOVOTNÝ. 2000. *Podporujeme aktivní myšlení a samostatné učení žáků*. Vyd. 1. Olomouc: Hanex, 159 s. Edukace. ISBN 80-857-8328-2.

HANSEN ČECHOVÁ, Barbara. 2006. *Nápadník pro rozvoj klíčových kompetencí ve výuce*. Praha: SCIO, 177 s. ISBN 80-869-1053-9.

HENDL, Jan. 2006. *Přehled statistických metod zpracování dat: analýza a metaanalýza dat*. Vyd. 2., opr. Praha: Portál, 583 s. ISBN 80-736-7123-9.

HENDL, Jan. 2008. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 2., aktualiz. vyd. Praha: Portál, 407 s. ISBN 978-80-7367-485-4.

CHANDRA, Praphul. 2009. *Wireless security*. Amsterdam: Newnes, xvi, 726 s. ISBN 978-1-85617-529-6.

CHEVALIER, Jacques M. a Daniel BUCKLES. 2013. *Participatory action research: theory and methods for engaged inquiry*. 1st ed. London: Routledge, xxi, 469 s. ISBN 9780415540322.

CHRÁSKA, Miroslav. 2007. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. Vyd. 1. Praha: Grada, 265 s. ISBN 9788024713694.

CHRÁSTKA, Miroslav. 1999. *Didaktické testy*. Vyd. 1. Brno: Paido, 1999, 91 s. ISBN 80-859-3168-0.

KASÍKOVÁ, Hana. 1997. *Kooperativní učení, kooperativní škola*. Vyd. 1. Praha: Portál, 147 s. ISBN 8071781673.

KIRKPATRICK, Donald L. 1971. *A practical guide for supervisory training and development*. Reading, Mass: Addison-Wesley, ISBN 978-020-1037-463.

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. 2012. *Nebezpečí internetové komunikace III*. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci. ISBN 978-80-244-3087-4. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

KOVÁŘOVÁ, Pavla a Iva ZADRAŽILOVÁ. 2013. The Influence of Technological Changes on the Definition of Information Literacy. In: KURBANOĞLU, Serap, Esther GRASSIAN, Diane MIZRACHI, Ralph CATTS a Sonja ŠPIRANEC (eds.). *Worldwide Commonalities and Challenges in Information Literacy Research and Practice European Conference, Ecil 2013, Istanbul, Turkey, October 22-25, 2013*. Revised selected papers. Cham: Springer, s. 118-125. ISBN 9783319039183. DOI: 10.1007/978-3-319-03919-0_14. Dostupné z: http://link.springer.com/10.1007/978-3-319-03919-0_14

KOVÁŘOVÁ, Pavla. 2012. *Trendy v informačním vzdělávání*. 1. vyd. Zlín: VeRBuM. ISBN 978-80-87500-18-7.

KRÁL, Mojmír. 2006. *Bezpečnost domácího počítače: prakticky a názorně.* 1. vyd. Praha: Grada, 334 s. ISBN 80-247-1408-6.

LEEDER, Chris. 2014. Pilot-testing an Online Credibility Evaluation Learning Tool. In: *IConference 2014 Proceedings* [online]. iSchools, 2014-03-01 [cit. 2014-08-30]. DOI: 10.9776/14058. Dostupné z: https://www.ideals.illinois.edu/handle/2142/47296

LIVINGSTONE, Sonia M. a Leslie HADDON. 2009. *Kids online: opportunities and risks for children*. Portland (OR): Policy Press, xix, 272 s. ISBN 978-184-7424-389.

LYON, David. 1994. *The electronic eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 270 s. ISBN 08-166-2515-8.

MAŇÁK, Josef, Vlastimil ŠVEC a Štefan ŠVEC. 2005. *Slovník pedagogické metodologie*. 1. vyd. Brno: Paido, 134 s. Pedagogický výzkum v teorii a praxi, sv. 3. ISBN 80-731-5102-2.

(Part IV) Marketing & Promotion: (Chapter 17) Behavioral Targeting. 2007. *Entertainment, Media & Advertising Market Research Handbook*. Loganville: Richard K. Miller & Associates, s. 117-121. ISBN 9781577831068.

MATĚJKA, Michal. 2002. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, x, 106 s. ISBN 80-722-6419-2.

MCLUHAN, Marshall. 2008. *Člověk, média a elektronická kultura: reprezentativní výbor z celoživotního díla proroka a mága elektrického věku a elektronické revoluce.* Dotisk 1. vyd. Brno: Jota, 415 s. ISBN 9788072171286.

MITNICK, Kevin. 2003. *Umění klamu*. HELION S.A., 348 s. ISBN 83-7361-210-6.

MÜLLER, Hans Jörg, Florian ALT a Daniel MICHELIS. 2011. *Pervasive advertising*. London: Springer, ix, 364 s. ISBN 978-085-7293-510.

NIXON, Paul G, Vassiliki N. KOUTRAKOU a Rajash RAWAL. 2010. *Understanding e-government in Europe: issues and challenges*. New York: Routledge, xxviii, 322 s. ISBN 02-038-6609-6.

NOVOTNÝ, Oto. 1997. *Trestní právo hmotné*. 3. přepracované vyd. Praha: Codex. ISBN 80-859-6324-8.

PELIKÁN, Jiří. 2011. *Základy empirického výzkumu pedagogických jevů*. Praha: Karolinum. ISBN 978-80-246-1916-3.

PICKARD, Alison Jane. 2013. *Research methods in information*. 2nd ed. London: Facet. ISBN 978-185-6048-132.

POŽÁR, Josef. 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

RAMSEY, Geoff a Vipin MAYAR. c2011. *Digital impact: the two secrets to online marketing success*. Hoboken (N.J.): John Wiley, v, 298 s. ISBN 9780470905722-.

ŘÍČAN, Pavel. 1990. *Cesta životem*. 1. vyd. Praha: Panorama, 435 s. ISBN 80-703-8078-0.

SKUTIL, Martin. 2011. *Základy pedagogicko-psychologického výzkumu pro studenty učitelství*. Vyd. 1. Praha: Portál, 254 s. ISBN 9788073677787.

SMEJKAL, Vladimír. 2001. *Internet a §§§.* 2. aktualiz. a rozš. vyd. Praha: Grada, 284 s. ISBN 80-247-0058-1.

SNYDER, Lawrence. c2011. *Fluency with information technology: skills, concepts*. 4th ed. Boston: Addison-Wesley, xviii, 795 s. ISBN 01-360-9182-2.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007a. *Co je kritické myšlení (vymezení pojmů a rámce E-U-R)*. Příručka 1. Praha: Kritické myšlení.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007b. *Čtením a psaním ke kritickému myšlení*. Příručka 3. Praha: Kritické myšlení.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007c. *Čtení, psaní a diskuse ve všech předmětech*. Příručka 4. Praha: Kritické myšlení.

ŠÁMAL, Pavel. 2010. *Trestní zákoník II.: § 140 až 421: komentář*. 1. vyd. Praha: C. H. Beck, 2 v. ISBN 97880740017892.

ŠIMÍČKOVÁ-ČÍŽKOVÁ, Jitka. 2003. *Přehled vývojové psychologie*. 2. nezměn. vyd. Olomouc: Univerzita Palackého, 175 s. ISBN 80-244-0629-2.

ŠTEFEK, Tomáš. 2012. Bezpečné městečko na dlani. In: FRIEDLOVÁ, Zdeňka a Pavla GAJDOŠÍKOVÁ. *Knihovny současnosti 2012: sborník z 20. konference, konané ve dnech 11.-13. září 2012 v Pardubicích*. 1. vyd. Ostrava, s. 70-74. ISBN 978-80-86249-65-0.

ŠVAŘÍČEK, Roman a Klára ŠEĎOVÁ. 2007. *Kvalitativní výzkum v pedagogických vědách*. Vyd. 1. Praha: Portál, 377 s. ISBN 9788073673130.

ŠVEC, Štefan. 2009. *Metodologie věd o výchově: kvantitativně-scientické a kvalitativně-humanitní přístupy v edukačním výzkumu*. České rozš. vyd. Překlad Jana Cacková. Brno: Paido, 302 s. ISBN 978-807-3151-928.

VÁGNEROVÁ, Marie. 1999. *Psychopatologie pro pomáhající profese: variabilita a patologie lidské psychiky*. Vyd. 1. Praha: Portál, 444 s. ISBN 8071782149.

VÁGNEROVÁ, Marie. 2000. *Vývojová psychologie: dětství, dospělost, stáří*. Vyd. 1. Praha: Portál, 522 s. ISBN 8071783080.

VÁGNEROVÁ, Marie. 2005. *Vývojová psychologie*. Vyd. 1. Praha: Karolinum, 467 s. ISBN 978-802-4609-560.

VANÍČKOVÁ, Eva, Kamil PROVAZNÍK a Zuzana HADJ-MOUSSOVÁ. 1997. *Sexuální zneužívání dětí*. 1. vyd. Praha: Karolinum, 82 s. ISBN 80-718-4479-9.

VANÍČKOVÁ, Eva. 1999. *Sexuální násilí na dětech: výskyt, podoby, diagnostika, terapie, prevence*. Vyd. 1. Praha: Portál, 118 s. ISBN 80-717-8286-6.

WESTIN, Alan. 1967. *Privacy and Freedom*. New York: Atheneum.

Základní statistické údaje o kultuře v České republice 2012. III. díl, Knihovny a vydavatelská činnost. 2013. Praha: NIPOS - Centrum informací a statistik kultury, 67 s. ISBN 978-80-7068-274-6. Dostupné také z: http://www.nipos-mk.cz/wp-content/uploads/2013/05/Statistika_kultury_2012_III.KNIHOVNY_web.pdf

ZURKOWSKI, Paul G. 1974. *The Information Service Environment Relationships and Priorities.* Related Paper No. 5. Washington (D.C.). Dostupné z: http://files.eric.ed.gov/fulltext/ED100391.pdf

11.2 Články v periodikách

ÁLVAREZ, M., A. TORRES, E. RODRÍGUEZ, S. PADILLA a M.J. RODRIGO. 2013. Attitudes and parenting dimensions in parents' regulation of Internet use by primary and secondary school children. *Computers* [online]. Roč. 67, s. 69-78 [cit. 2014-08-28]. DOI: 10.1016/j.compedu.2013.03.005. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0360131513000833

BECHMANN, Anja. 2014. Non-informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies*. Roč. 11, č. 1.

DOMBROVSKÁ, Michaela, Hana LANDOVÁ a Ludmila TICHÁ. 2004. Informační gramotnost - teorie a praxe v ČR. *Národní knihovna: knihovnická revue* [online]. Roč. 15, č. 1, s. 7-18 [cit. 2014-07-24]. ISSN 1214-0678. Dostupné z: http://knihovna.nkp.cz/nkkr0401/0401007.html

DÖRING, Nicola. 2014. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting?. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. Roč. 8, č. 1 [cit. 2014-08-28]. DOI: 10.5817/CP2014-1-9. Dostupné z: http://cyberpsychology.eu/view.php?cisloclanku=2014031401

EKE, Helen Nneka. 2012. Creating a digital footprint as a means of optimizing the personal branding of librarians in the digital society. *Webology*. Roč. 9, č. 2, s. 31-40.

GALLAGHER, Frank a Kat STEWART. 2011. Information literacy beyond the library: Cable in the Classroom. *College & Undergraduate Libraries* [online]. 2011-03-10, roč. 18, č. 1, s. 111-118 [cit. 2014-08-28]. DOI: 10.1080/10691316.2011.550537. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/10691316.2011.550537

GINSBERG, Jeremy, Matthew H. MOHEBBI, Rajan S. PATEL, Lynnette BRAMMER, Mark S. SMOLINSKI a Larry BRILLIANT. 2008. Detecting influenza epidemics using search engine query data. *Nature* [online]. 2008-11-19, roč. 457, č. 7232, s. 1012-1014 [cit. 2014-08-28]. DOI: 10.1038/nature07634. Dostupné z: http://www.nature.com/doifinder/10.1038/nature07634

HARRIS, Amy. 2010. Active learning for the Millennial Generation. *Georgia Library Quarterly* [online]. Fall 2010, roč. 47, č. 4, s. 13-14 [cit. 2014-08-30]. ISSN: 2157-0396. Dostupné z: EBSCOhost

HARRIS, Margaret S. G. 2012. Fulfilling a European Vision through Flexible Learning and Choice. *European Journal of Education* [online]. Roč. 47, č. 3, s. 424-434 [cit. 2014-08-30]. DOI: 10.1111/j.1465-3435.2012.01535.x. Dostupné z: http://doi.wiley.com/10.1111/j.1465-3435.2012.01535.x

HERRINGTON, Kim. 2010. Now is the Time! Teen Tech Week in a School Library. *Young Adult Library Services* [online]. Winter 2010, roč. 8, č. 2. s. 9-10 [cit. 2014-08-30]. ISSN 15414302. Dostupné z: http://search.proquest.com/docview/217697643

HUSSAIN, Mohammed Ali a Sarath Babu DUGGIRALA. 2012. Secure Anonymous Route Discovery Protocol for Ad Hoc Routing in Ad Hoc Wireless Networks. *International Journal of Computer Technology and Applications* [online]. Jan 2012, roč. 3, č. 1. s. 495-501 [cit. 2014-08-30]. Dostupné z: ProQuest Technology Collection

CHANG, Charlotte. 2010. Internet Safety Survey: Who will protect the children. *Berkeley Technology Law Journal* [online]. Roč. 25, č. 501, s. 501-527 [cit. 2014-08-30]. Dostupné z: http://www.btlj.org/data/articles/25_1/0501-0528%20Chang_Web.pdf

CHESTER, Jeff a Kathryn MONTGOMERY. 2008. No escape: Marketing to kids in the digital age. *Multinational Monitor* [online]. Roč. 29, č. 1 [cit. 2014-08-30]. Dostupné z: http://www.multinationalmonitor.org/mm2008/072008/chester.html

JANSSEN, José, Adriana J. BERLANGA a Rob KOPER. 2011. Evaluation of the Learning Path Specification. *Journal of Educational Technology & Society* [online]. Roč. 14, č. 3, s. 218-230 [cit. 2014-08-30]. ISSN 1176-3647. Dostupné z: http://search.proquest.com/docview/1287031475

JOINER, Richard, Jeff GAVIN, Jill DUFFIELD, Mark BROSNAN, Charles CROOK, Alan DURNDELL, Pam MARAS, Jane MILLER, Adrian J. SCOTT a Peter LOVATT. 2005. Gender, Internet Identification, and Internet Anxiety: Correlates of Internet Use. *CyberPsychology* [online]. Roč. 8, č. 4, s. 371-378 [cit. 2014-08-30]. DOI: 10.1089/cpb.2005.8.371. Dostupné z: http://www.liebertonline.com/doi/abs/10.1089/cpb.2005.8.371

JUVONEN, Jaana a Elisheva F. GROSS. 2008. Extending the School Grounds?-Bullying Experiences in Cyberspace. *Journal of School Health* [online]. Roč. 78, č. 9, s. 496-505 [cit. 2014-08-30]. DOI: 10.1111/j.1746-1561.2008.00335.x. Dostupné z: http://doi.wiley.com/10.1111/j.1746-1561.2008.00335.x

KAPADIA, Apu, Tristan HENDERSON, Jeffrey J. FIELDING a David KOTZ. 2007. Virtual Walls: Protecting Digital Privacy in Pervasive Environments. *Pervasive Computing* [online]. Berlin, Heidelberg: Springer, s. 162 [cit. 2014-07-24]. DOI: 10.1007/978-3-540-72037-9_10. Dostupné z: http://link.springer.com/10.1007/978-3-540-72037-9_10

KIM, Won, Ok-Ran JEONG, Chulyun KIM a Jungmin SO. 2011. The dark side of the Internet: Attacks, costs and responses. *Information Systems* [online]. Roč. 36, č. 3, s. 675-705 [cit. 2014-07-25]. DOI: 10.1016/j.is.2010.11.003. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0306437910001328

KIRKPATRICK, Donald. 1996. Great Ideas Revisited: Revisiting Kirkpatrick's Four-Level Model. *Training and Development* [online]. Roč. 50, č. 1, s. 54–57 [cit. 2014-08-30]. Dostupné z: EBSCOhost

LANDOVÁ, Hana a Zdeňka CIVÍNOVÁ. 2010. Aktivity vysokoškolských knihoven v oblasti informačního vzdělávání: vývoj v letech 2006-2010 na veřejných vysokých školách v ČR. *ProInflow* [online]. Roč. 2, č. 2 [cit. 2014-07-24]. ISSN 1804–2406. Dostupné z: http://pro.inflow.cz/aktivity-vysokoskolskych-knihoven-v-oblasti-informacniho-vzdelavani-vyvoj-v-letech-2006-2010-na-vere

LEANDER, Lina, Sven Å CHRISTIANSON a Pär Anders GRANHAG. 2008. Internet-initiated sexual abuse: adolescent victims' reports about On - and Off -line sexual activities. *Applied Cognitive Psychology* [online]. Roč. 22, č. 9, s. 1260-1274 [cit. 2014-07-26]. DOI: 10.1002/acp.1433. Dostupné z: http://doi.wiley.com/10.1002/acp.1433

LI, Lili a Lori LESTER. 2009. Rethinking Information Literacy Instructions in the Digital Age. *The International Journal of Learning* [online]. Roč. 16, č. 11, s. 569-577 [cit. 2014-08-30]. ISSN 1447-9494. Dostupné z: EBSCOhost

LORENZ, Michal. 2012. Informační věda – předmět neznámý. *Inflow* [online]. Roč. 5, č. 7 [cit. 2012-08-20]. ISSN 1802-9736. Dostupné z: http://www.inflow.cz/informacni-veda-predmet-neznamy

Manifest IFLA o přístupu k Internetu. 2002. *Bulletin SKIP* [online]. Č. 2 [cit. 2014-08-30]. Dostupné z: http://wwwold.nkp.cz/o_knihovnach/konsorcia/skip/Bull02_23.htm

MARCOUX, Elizabeth. 2010. Cybersecurity a school libraries. *Teacher Librarian* [online]. Roč. 67, č. 2, s. 67-68 [cit. 2014-08-30]. Dostupné z: http://search.proquest.com/docview/846786568

MARTIN, Nigel a John RICE. 2012. Children's cyber-safety and protection in Australia: An analysis of community stakeholder views. *Crime Prevention and Community Safety* [online]. Roč. 14, č. 3, s. 165-181 [cit. 2014-08-30]. DOI: 10.1057/cpcs.2012.4. Dostupné z: http://www.palgrave-journals.com/doifinder/10.1057/cpcs.2012.4

MOORE, Shelley C. 2012. Digital Footprints on the Internet. *International Journal of Childbirth Education* [online]. Roč. 27, č. 3, s. 86-91 [cit. 2014-08-30]. Dostupné z: http://search.proquest.com/docview/1039291547

MORENO, Megan A., Katie G. EGAN, Kaitlyn BARE, Henry N. YOUNG a Elizabeth D. COX. 2013. Internet safety education for youth: stakeholder perspectives. *BMC Public Health* [online]. Roč. 13, č. 1, s. 543- [cit. 2014-08-30]. DOI: 10.1186/1471-2458-13-543. Dostupné z: http://www.biomedcentral.com/1471-2458/13/543

O'NEILL, Brian. 2012. Trust in the information society. *Computer Law* [online]. Roč. 28, č. 5, s. 551-559 [cit. 2014-08-30]. DOI: 10.1016/j.clsr.2012.07.005. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001409

OHM, Paul. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* [online]. Roč. 57, č. 1701 [cit. 2014-08-30]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

OOLO, Egle a Andra SIIBAK. 2013. Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 7, issue 1. DOI: 10.5817/CP2013-1-7. Dostupné z: http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501

PETRESS, Ken. 2008. What Is Meant by "Active Learning?". *Education* [online]. Summer 2008, roč. 128, č. 4, s. 566-569 [cit. 2014-08-30]. ISSN: 0013-1172. Dostupné z: EBSCOhost

PIHT, Sirje, Piret LEHISTE, Rea RAUS a Mariliis LAZAREV. 2012. The relevance of evocation and reflection cards in the learning process. *Problems of Education in the 21st Century*. Č. 41, s. 61-74.

PINTO, Caro. 2013. Teaching Librarians & Project Management: New Expectations for the Digital Age. *Archive Journal* [online]. Č. 3 [cit. 2014-08-30]. Dostupné z: http://www.archivejournal.net/issue/3/notes-queries/teaching-librarians-project-management-new-expectations-for-the-digital-age/

POLING, Devereaux A. a Julie M. HUPP. 2009. Active Learning Through Role Playing: Virtual Babies in a Child Development Course. *College Teaching* [online]. Fall, 2009, roč. 57, č. 4, s. 221-228 [cit. 2014-08-30]. ISSN 8756-7555. Dostupné z: http://search.proquest.com/docview/848215353

Polovina dětí reaguje na internetu na zprávy od cizích lidí – ze zvědavosti. 2010. *HN Tech* [online]. 9. 2. 2010 [cit. 2014-08-30]. Dostupné z: http://tech.ihned.cz/c1-40440600-polovina-deti-reaguje-na-internetu-na-zpravy-od-cizich-lidi-rodice-je-prilis-nechrani

PORADA, Viktor a Roman RAK. 2006. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue* [online]. Roč. 2, č. 4, s. 1 – 21 [cit. 2014-08-30]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

PRENSKY, Marc. 2001. Digital Natives, Digital Immigrants. *On the Horizon* [online]. Roč. 9, č. 5 [cit. 2014-05-04]. ISSN 1085-4959. Dostupné z: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

RABUŠICOVÁ, Milada, Klára ŠEĎOVÁ, Kateřina TRNKOVÁ a Vlastimil ČIHÁČEK. 2004. K otevřenosti škol vůči rodičům a veřejnosti. In: *Studia paedagogica: Sborník prací filozofické fakulty brněnské univerzity* [online]. s. 59-72 [cit. 2014-08-30]. ISSN 2336-4521. Dostupné z: http://www.phil.muni.cz/journals/index.php/studia-paedagogica/article/view/395/551

RANGUELOV, Stanislav. 2010. Summary Report Education on Online Safety in Schools in Europe. *New Horizons in Education* [online]. Roč. 58, č. 3, s. 149-163 [cit. 2014-08-30]. ISSN-1683-1381. Dostupné z: http://files.eric.ed.gov/fulltext/EJ966666.pdf

SALTZMAN, Marc. 2008. Identity thieves 'phishing' the Internet. *Star - Phoenix* [online]. Sep 20, 2008, E.14 [cit. 2014-08-29]. ISSN 0832-4174. Dostupné z: http://search.proquest.com/docview/348892935

SMART, K. L., C. WITT a J. P. SCOTT. 2012. Toward Learner-Centered Teaching: An Inductive Approach. *Business Communication Quarterly* [online]. 7. 11. 2012, roč. 75, č. 4, s. 392-403 [cit. 2014-08-30]. DOI: 10.1177/1080569912459752. Dostupné z: http://bcq.sagepub.com/cgi/doi/10.1177

SOLON, Olivia. 2012. How much data did Facebook have on one man? 1,200 pages of data in 57 categories. *Wired* [online]. 28. 12. 2012 [cit. 2014-08-28]. Dostupné z: http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook

STASIUNAITIENE, Egle a Lina KAMINSKIENE. 2009. Qualitative Parameters for Evaluation Procedures of Non-Formal and Informal Learning Achievements. *Quality of Higher Education* [online]. Č. 6, s. 117-140. ISSN-1822-1645. Dostupné z: http://files.eric.ed.gov/fulltext/EJ870192.pdf

TAMBAUM, Tiina. 2010. Expectations of the elderly for the Internet as an influencing factor for the internet teaching. *Problems of Education in the 21st Century* [online]. Roč. 22 [cit. 2014-08-30]. Dostupné z: EBSCOhost

TERESEVIČIENĖ, Margarita, Vaiva ZUZEVIČIŪTĖ a Monika IVOŠKAITĖ. 2008. Assessment and Recognition of Achievements of Non-Formal and Informal Learning – Function in Context of Lifelong Learning, Achievements and Challenges. *Socialiniai tyrimai (Social Research)* [online]. Roč. 11, č. 1, s. 67-73 [cit. 2014-08-30]. ISSN 1392-3110. Dostupné z: http://etalpykla.lituanistikadb.lt/fedora/get/LT-LDB-0001:J.04~2008~1367164334343/DS.002.1.01.ARTIC

THOMPSON, Samuel T. C. 2013. Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries* [online]. Roč. 25, č. 4, s. 222-225 [cit. 2014-08-30]. Dostupné z: http://ejournals.bc.edu/ojs/index.php/ital/article/viewFile/3355/2966

TUOMAITE, Virginija and Vaiva ZUZEVICIUTE. 2008. Validation and Recognition of Non-Formal and Informal Learning of Employees as Prerequisite of Lifelong Learning. *Organizacijø Vadyba: Sisteminiai Tyrimai* [online]. Č. 45, s. 99-113 [cit. 2014-08-30]. ISSN 1392-1142. Dostupné z: http://search.proquest.com/docview/222760897

VAN HELVOORT, A. A. J. 2010. Impact of Recent Trends in Information and Communication Technology on the Validity of the Construct Information Literacy in Higher Education. *Technological Convergence and Social Networks in Information Management* [online]. s. 61-73 [cit. 2014-08-30]. DOI: 10.1007/978-3-642-16032-5_6. Dostupné z: http://link.springer.com/10.1007/978-3-642-16032-5_6

VOGELSTEIN, Fred. 2010. What if the Facebook (Un)Privacy Revolution Is a Good Thing?. *Wired* [online]. 29. 5. 2010 [cit. 2014-08-28]. Dostupné z: http://www.wired.com/2010/05/facebook-firestorm-good-thing/

WALRAVE, Michel, Ini VANWESENBEECK a Wannes HEIRMAN. 2012. Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. Roč. 6, č. 1 [cit. 2014-08-30]. DOI: 10.5817/CP2012-1-3. Dostupné z: http://www.cyberpsychology.eu/view.php?cisloclanku=2012051201

WEAVER, Anne. 2010. Facebook and Other Pandora's Boxes. *Access*. Roč. 24, č. 4, s. 24-32.

WEAVER, Stephen D. a Mark GAHEGAN. 2007. Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*. Roč. 97, č. 3, s. 324-350.

WEEDEN, Shalynn, Bethany COOKE a Michael MCVEY. Underage Children and Social Networking. *Journal of Research on Technology in Education* [online]. 2013, roč. 45, č. 3, s. 249-262 [cit. 2014-08-30]. DOI: 10.1080/15391523.2013.10782605. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/15391523.2013.10782605

WOLD, Thomas. 2010. Protection and access: To regulate young people's internet use. *International Journal of Media and Cultural Politics* [online]. Roč. 6, č. 1, s. 63-79 [cit. 2014-08-30]. DOI: 10.1386/macp.6.1.63/1. Dostupné z: http://www.ingentaconnect.com/content/intellect/mcp/2010/00000006/00000001/art00005

ZUBER-SKERRITT, Ortrun a Margaret FLETCHER. 2007. The quality of an action research thesis in the social sciences. *Quality Assurance in Education* [online]. Roč. 15, č. 4, s. 413-436 [cit. 2014-08-30]. DOI: 10.1108/09684880710829983. Dostupné z: http://www.emeraldinsight.com/10.1108/09684880710829983

11.3 Webové zdroje

ANGWIN, Julia a Jennifer VALENTINO-DEVRIES. 2010. The Information That Is Needed to Identify You: 33 Bits. In: *Digits* [online]. 4. 8. 2010 [cit. 2014-08-28]. Dostupné z: http://blogs.wsj.com/digits/2010/08/04/the-information-that-is-needed-to-identify-you-33-bits/

Aukro nápověda: komentáře a hodnocení prodeje. [b.r.]. *Aukro* [online]. [cit. 2014-08-28]. Dostupné z: http://napoveda.aukro.cz/18967/18959/20205/system-komentaru-hodnoceni-prodeje-na-aukru

Benefits of JonDonym. [b.r.]. *JonDonym* [online]. [cit. 2014-08-28]. Dostupné z: https://anonymous-proxy-servers.net/en/benefits.html

Big6 Skills Overview. c2013. *The Big6* [online]. [cit. 2014-08-28]. Dostupné z: http://big6.com/pages/about/big6-skills-overview.php

Březen měsíc Internetu 2008: Akce pro veřejnost v Knihovně města Plzně, p. o. 2018. In: *Knihovna města Plzně, p. o.* [online]. [cit. 2014-08-28]. Dostupné z: http://www.knihovna.plzen.eu/aktuality/bmi08.rtf

Certifikáty a ocenění e-shopů. c2014. *Ověř si to* [online]. [cit. 2014-08-28]. Dostupné z: http://www.oversito.cz/uzitecne-informace/certifikaty-a-oceneni-e-shopu/

Citizenship in the Digital Age: Sample Lesson Plans for Grades 1-12. 2012. In: *New York City School Library System* [online]. 4. 4. 2012 [cit. 2014-08-28]. Dostupné z: http://schools.nyc.gov/NR/rdonlyres/3CA0188D-66A2-490C-9E90-1EFCADA92F8C/0/Citizenshipinthedigitalage.pdf

Davis Elementary Internet Safety Month Lesson Plans. c2002-2014. *Davis Library* [online]. [cit. 2014-08-28]. Dostupné z: http://cfbportal.schoolwires.net/Page/25483

Digital Footprint. 2014. *Manheim Township High School Library* [online]. [cit. 2014-08-28]. Dostupné z: http://hs.mtwp.libguides.com/content.php?pid=363642&sid=3320865

DUERAGER, Andrea a Sonia LIVINGSTONE. 2012. How can parents support children's internet safety?. In: *LSE Research Online* [online]. London: EU Kids Online [cit. 2014-08-28]. Dostupné z: http://eprints.lse.ac.uk/42872/1/How%20can%20parents%20support%20children%E2%80%99s%20internet%20safety%28lsero%29.pdf

Egosurf. c2014. *Oxford Dictionaries* [online]. [cit. 2014-08-28]. Dostupné z: http://www.oxforddictionaries.com/definition/english/egosurf

Electronic Communications Regulations: Guidance on the rules on use of cookies and similar technologies. 2012. In: *Information Commissioner's Office* [online]. [cit. 2014-08-29]. Dostupné z: http://ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.pdf

FINDAHL, Olle. 2009. Preschoolers and the Internet: will children start to use the Internet when they start walking? In: *London School of Economics & Political Science* [online]. [cit. 2014-08-28]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/Conference%20Papers%20and%20abstracts/Emerging%20Issues/Findahl.pdf

FISHER, Clarence. 2010. Stalking in English Class. *Remote Access even from here* [online]. [cit. 2014-08-28]. Dostupné z: http://www.evenfromhere.org/2010/10/13/stalking-in-english-class/

Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013. 2014. *Gartner* [online]. 13. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://www.gartner.com/newsroom/id/2665715

GÉBLOVÁ, Alena. 2014. Síť veřejných knihoven máme nejhustší na světě. *Český statistický úřad* [online]. [cit. 2014-08-28]. Dostupné z: http://www.czso.cz/csu/2013edicniplan.nsf/c/EA002B5940

Get your Data!: Make an Access Request at Facebook! [b.r.]. *Europe versus facebook* [online]. [cit. 2014-08-26]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

HEMBREE. 2013. Thinking about Digital Footprints. *Bulldog Reader Blog* [online]. 6. 10. 2013 [cit. 2014-08-28]. Dostupné z: http://bellbulldogreaders.edublogs.org/2013/10/06/thinking-about-digital-footprints/

In the fishbowl. 2013. *COETAIL* [online]. 21. 4. 2013 [cit. 2014-08-28]. Dostupné z: http://www.coetail.com/bqdressler/tag/digital-footprint-2/

Information Literacy Competency Standards for Higher Education. 2000. In: *American Library Association* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ala.org/acrl/sites/ala.org.acrl/files/content/standards/standards.pdf

Information literacy skills. 2012. In: *CILIP* [online]. [cit. 2014-08-28]. Dostupné z: http://www.cilip.org.uk/sites/default/files/documents/Information%20literacy%20skills.pdf

Information literacy standards for student learning: Standards and indicators. 1998. In: *Innovative Library Initiatives Promotion Group* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ilipg.org/sites/ilipg.org/files/bo/InformationLiteracyStandards_final.pdf

IRGENS, Morten. 2013. What does it all mean? *The Business of Better* [online]. 1. 8. 2013 [cit. 2014-08-26]. Dostupné z: http://www.businessofbetter.com/?p=2057

ISTE Standards: Students. c2007. In: *International Society for Technology in Education* [online]. [cit. 2014-08-28]. Dostupné z: http://www.iste.org/docs/pdfs/20-14_ISTE_Standards-S_PDF.pdf

Jelly Bean 4.2: A new and improved Jelly Bean. [2012]. *Android* [online]. [cit. 2014-08-26]. Dostupné z: http://www.android.com/versions/jelly-bean-4-2/

JonDonym, AN.ON and Tor. [b.r.]. *JonDonym* [online]. [cit. 2014-08-28]. Dostupné z: https://anonymous-proxy-servers.net/en/help/jondonym.html

KASÍK, Pavel. 2009. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. In: *Technet* [online]. 19. 11. 2009 [cit. 2014-08-28]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka

LEYDEN, John. 2005. Americans are pants at password security. In: *The Register* [online]. 6. 5. 2005 [cit. 2014-08-28]. Dostupné z: http://www.theregister.co.uk/2005/05/06/verisign_password_survey/

LIBRARIANTIFF. 2014. Digital Citizenship at CMS. *Mighty Little Librarian* [online]. 27. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://www.mightylittlelibrarian.com/?p=1081

Live! Ghostery V.2.1 for Firefox. 2010. *Ghostery* [online]. 26. 4. 2010 [cit. 2014-08-28]. Dostupné z: https://purplebox.ghostery.com/post/551213088

LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG a Kjartan ÓLAFSSON. 2011. Risks and safety on the internet: The perspective of European children. Full Findings. In: *London School of Economics & Political Science*. London: LSE, 168 s. ISSN 2045-2551. Dostupné z: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf

LochyProduction. 2013. Česká Televize | Na Stopě | Metin 2 | Krádež Účtu. In: *YouTube* [online]. 7. 2. 2013 [cit. 2014-08-28]. Dostupné z: https://www.youtube.com/watch?v=d7bo5gQSZhI

MADDEN, Mary. 2007. Digital Footprints: Online identity management and search in the age of transparency. In: *Pew Internet & American Life Project* [online]. [cit. 2014-08-28]. Dostupné z: http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf

MADDEN, Mary. 2012. Privacy management on social media sites. In: *Pew Internet & American Life Project* [online]. 24. 2. 2012 [cit. 2014-08-28]. Dostupné z: http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

MARTÍNEZ-CABRERA, Alejandro. 2010. Erasing all digital footprints 'impossible'. In: *SFGate* [online]. 6. 7. 2010 [cit. 2014-08-28]. Dostupné z: http://www.sfgate.com/business/article/Erasing-all-digital-footprints-impossible-3259754.php

MORRIS, Kathleen. 2013. Teaching Children About Digital Footprints. *Primary Tech* [online]. 22. 2. 2013 [cit. 2014-08-28]. Dostupné z: http://primarytech.global2.vic.edu.au/2013/02/22/teaching-childre-about-digital-footprints/

Overview. [b.r.] *Do Not Track: Universal Web Tracking Opt Out* [online]. [cit. 2014-08-28]. Dostupné z: http://donottrack.us/

PEMI. 2012. Jaký je skutečný počet českých uživatelů Facebooku? In: *Marketing journal.cz* [online]. 18. 5. 2012 [cit. 2014-08-28]. Dostupné z: http://www.m-journal.cz/cs/jaky-je-skutecny-pocet-ceskych-uzivatelu-facebooku__s288x9161.html

POTÁČEK, Jiří. 2003-. Informační bezpečnost. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR [cit. 2014-08-28]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000074&local_base=KTD

Presidential Committee on Information Literacy: Final Report. 1989. *Association of College and Research Libraries* [online]. Chicago: American Library Association, 10. 1. 1989 [cit. 2014-08-28]. Dostupné z: http://www.ala.org/acrl/publications/whitepapers/presidential

Přístup k osobním údajům na Facebooku: Kde na Facebooku najdu své údaje? c2014. *Facebook* [online]. [cit. 2014-08-28]. Dostupné z: https://www.facebook.com/help/405183566203254

QUICK, Susannah, Gillian PRIOR, Ben TOOMBS, Luke TAYLOR a Rosanna CURRENTI. 2013. In: *Názory uživatelů na přínosy informačních a komunikačních technologií ve veřejných knihovnách v České republice: Závěrečná zpráva* [online]. TNS - Bill&Melinda Foundation [cit. 2013-11-02]. Dostupné z: http://www.ikaros.cz/images/201308/Cross-European_Libraries_Survey_CZE.pdf#

Rámcový vzdělávací program pro základní vzdělávání: se změnami provedenými k 1. 7. 2007. 2007. In: *Ministerstvo školství, mládeže a tělovýchovy* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy [cit. 2014-08-28]. Dostupné z: http://www.msmt.cz/uploads/soubory/zakladni/SP_RVPZV_2007.zip

Riding the Waves or Caught in the Tide?: Insights from the IFLA Trend Report. 2013. In: *IFLA Trend Report* [online]. Hague: IFLA [cit. 2014-08-28]. Dostupné z: http://trends.ifla.org/files/trends/assets/insights-from-the-ifla-trend-report_v3.pdf

Safer Internet for Children: Qualitative study in 29 European countries - summary report. 2007. In: *European Commission* [online]. [cit. 2014-08-28]. Dostupné z: http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf

See the evolution of an indicator and compare breakdowns: Households with access to the Internet at home. 2014. In: *Digital Agenda Data* [online]. [cit. 2014-08-28]. Dostupné z: http://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-breakdowns#chart={%22indicator-group%22:%22internet-usage%22,%22indicator%22:%22h_iacc%22,%22breakdown-group%22:%22Celkem%22,%22unit-measure%22:%22pc_hh%22,%22ref-area%22:%22CZ%22}

Soutěž a seznam zapojených organizací. 2014. *Saferinternet CZ* [online]. [cit. 2014-08-28]. Dostupné z: http://www.saferinternet.cz/soutez-a-seznam-zapojenych-organizaci-2014.html

Statistika kultury. c2007. *Ministerstvo kultury* [online]. Praha: Ministerstvo kultury [cit. 2014-08-28]. Dostupné z: http://www.mkcr.cz/scripts/detail.php?id=5018

SULLIVAN, Laurie. 2011. Behavioral Targeting For Facebook. *MediaPost Publications* [online]. 16. 3. 2011 [cit. 2014-08-26]. Dostupné z: http://www.mediapost.com/publications/article/146799/behavioral-targeting-for-facebook.html

SWALLOW, Erica. 2011. How Recruiters Use Social Networks to Screen Candidates: Infographic. *Mashable: The Social Media Guide* [online]. October 23, 2011 [cit. 2014-08-26]. Dostupné z: http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/

SWETNAM, Lorena. 2013. Digital Citizenship, Digital Footprint & Digital Literacy. *It all started in the library…* [online]. 29. 8. 2013 [cit. 2014-08-28]. Dostupné z: http://lswetnam.blogspot.cz/2013/08/digital-citizenship-digital-footprint.html

SWGDE and SWGIT Digital & Multimedia Evidence Glossary. 2005. In: *Crime-Scene-Investigator.net* [online]. 2005, 01/14/2011 [cit. 2014-08-26]. Dostupné z: http://www.crime-scene-investigator.net/swgde_swgit_glossary_v2-4.pdf

Sylaby a moduly. [2014]. *ECDL Czech Republic* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ecdl.cz/zakladni_moduly.php

Školy. [2014]. *Městská knihovna Litomyšl* [online]. Litomyšl: Městská knihovna Litomyšl [cit. 2014-08-28]. Dostupné z: http://www.litomysl.cz/knihovna/skoly

The SCONUL Seven Pillars of Information Literacy: Core Model For Higher Education. 2011. In: *SCONUL* [online]. April 2011 [cit. 2014-08-28]. Dostupné z: http://www.sconul.ac.uk/sites/default/files/documents/coremodel.pdf

Tor: Overview. [b.r.]. *Tor* [online]. [cit. 2014-08-28]. Dostupné z: https://www.torproject.org/about/overview

VÁLEK, Jiří. 2009. Elektronizace zdravotnictví (e-Health). *Zdraví a Zdravotnictví* [online]. [cit. 2014-08-26]. Dostupné z: http://www.zdrav.cz/modules.php?op=modload&name=News&file=article&sid=8963

Využití internetu dětmi ve věku od 12 do 17 let: Safeinternet-Gemius Ad-hoc. 2006. In: *Národní centrum bezpečnějšího internetu* [online]. Praha: Národní centrum bezpečnějšího internetu [cit. 2014-08-26]. Dostupné z: www.ncbi.cz/category/5-dokumenty?download=21

Výzkum rizikového chování českých dětí v prostředí internetu 2013. 2013. In: *Bezpečný internet* [online]. [cit. 2014-08-28]. Dostupné z: http://www.bezpecnyinternet.cz/ke-stazeni/bezpecny_internet_prezentace.pdf

Vzorový knihovní řád. 2014. In: *Portál Knihovnického institutu Národní knihovny ČR* [online]. Praha: Národní knihovna ČR, Knihovnický institut, 29. 8. 2014 [cit. 2014-08-26]. Dostupné z: knihovnam.nkp.cz/docs/VKR_def_1.rtf

Web 2.0 suicide machine [online]. [b.r.]. [cit. 2014-08-28]. Dostupné z: http://suicidemachine.org/

What is a digital footprint?. c2010. *Dear librarian* [online]. [cit. 2014-08-28]. Dostupné z: http://www.dearlibrarian.com/2010/11/what-is-a-digital-footprint/

Windows 8 ztratily podíl na trhu: naopak rostly Windows 7 a XP. 2014. In: *Technet* [online]. Praha: MAFRA, 3. 7. 2014 [cit. 2014-08-28]. Dostupné z: http://technet.idnes.cz/windows-8-ztraci-na-ukor-windows-7-dqo-/software.aspx?c=A140703_171026_software_vse

ZAŤKO, Igor. 2014. Zkušenosti s informačním vzděláváním na ZŠ Gorkého v Havířově v předmětu Informatika. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR , 24. 4. 2014 [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/Informacni_vzdelavani_na_ZS_Gorkeho.pdf

ZAZANI, Eleni. 2013. Lesson plan: Who am I? In: My digital footprint. In: *Birkbeck University of London* [online]. 25. 10. 2013 [cit. 2014-08-28]. Dostupné z: http://eprints.bbk.ac.uk/8667/3/8667.pdf

11.4 Právní dokumenty (všechny ve znění k 31. 8. 2014)

Commission staff working paper impact assessment: Accompanying document to the Proposal for a Council Recommendation on the validation of non-formal and informal learning. 2012. SWD/2012/0252 final. 5. 9. 2012. Dostupný z: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:52012SC0252&qid=1404421869196

Communication from the Commission of the European communities: Making a European Area of Lifelong Learning a Reality. 2001. Brussel, COM(2001) 678 final. 21. 11. 2001. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0678:FIN:EN:PDF

DELORS, Jacques. 1996. Learning: The treasure within: Report to UNESCO of the International Commission on Education for the Twenty-first Century. Dostupné z: http://unesdoc.unesco.org/images/0010/001095/109590eo.pdf

Dlouhodobý záměr vzdělávání a rozvoje vzdělávací soustavy ČR (2011-2015). 2011. Dostupné z: http://www.vzdelavani2020.cz/images_obsah/dokumenty/knihovna-koncepci/dlouhodoby-zamer-reg/dzcr_2011.pdf

Federal Trade Commission Decision and Order from Dec. 14, 2011, Docket No. C-4344, File No. 102-3185. Dostupné z: http://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutdo.pdf

Koncepce rozvoje knihoven ČR na léta 2011 - 2015 včetně internetizace knihoven: Knihovny pro EVROPU 2020. 2012. Dostupné z: http://www.mkcr.cz/assets/literatura-a-knihovny/Koncepce_rozvoje_knihoven_2011-2015.pdf

Koncepce rozvoje knihoven v České republice na léta 2004 – 2010. 2004. Dostupné z: http://knihovnam.nkp.cz/docs/Koncepce04_10.doc

Metodický pokyn Ministerstva kultury k zajištění výkonu regionálních funkcí knihoven a jejich koordinaci na území České republiky. 2011. Dostupné z: knihovnam.nkp.cz/docs/MetPokynMK05.doc

Nález Ústavního soudu ze dne 22. 3. 2011, spis. zn. N 52/60 SbNU 625. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1

Rozsudek Soudního dvora (velkého senátu) ze 13. května 2014, spis. zn. C-131/12. Dostupný z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=cs

Směrnice Evropského parlamentu a Rady 2009/136/ES, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02009L0136-20091219

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:01995L0046-20031120

Stanovisko Úřadu pro ochranu osobních údajů č. 2/2002, revize srpen 2009, zpracování osobních údajů v souvislosti s činností knihovny. 2009. Dostupné z: http://www.uoou.cz/files/stanovisko_2002_2.pdf

Státní informační politika – cesta k informační společnosti. 1999. Dostupné z: http://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/

Státní politika v elektronických komunikacích Digitální Česko v. 2.0 - Cesta k digitální ekonomice. 2013. Dostupné z: http://www.vlada.cz/assets/media-centrum/aktualne/Digitalni-Cesko-v--2-0_120320.pdf

Struktury systémů vzdělávání a odborné přípravy v Evropě: Česká republika 2009/10. 2009. Praha: Ministerstvo školství, mládeže a tělovýchovy [cit. 2014-08-29]. Dostupné z: http://www.msmt.cz/uploads/VKav_200/Eu_CZ_2010/educz_0910.pdf

Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=40453

Velká Británie. Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. Dostupné z: http://www.legislation.gov.uk/uksi/2011/1208/made

Zákon č. 101/2000 Sb., o ochraně osobních údajů. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49228

Zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon). Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=51517

Zákon č. 273/2008 Sb., o Policii České republiky. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67272

Zákon č. 561/2004 Sb., o předškolním, základním středním, vyšším odborném a jiném vzdělávání (školský zákon). Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=58471

11.5 Použité zdroje v navrhované metodice

Terminologie a základní funkce internetu

HLAVENKA, Jiří. 2004. *Vyhledávání na Internetu*. 2. vyd. Brno: Computer Press, ISBN 80-722-6759-0.

HOCK, Randolph. 2010. *The extreme searcher's Internet handbook: a guide for the serious searcher*. 3rd ed. Medford (NJ): CyberAge Books. ISBN 09-109-6584-6.

PROCHÁZKA, David. 2011. *Nebojte se počítače - pro Windows 7 a Office 2010*. 1. vyd. Praha: Grada, 126 s. Snadno a rychle (Grada). ISBN 978-80-247-3717-1.

Ochrana osobních údajů v internetové komunikaci

ATKINS, Lucy. 2007. Can u speak teenager? Today's teenagers live and breathe the wired world of the Internet, using it for sex, rebellion and creativity. Lucy Atkins offers a parental guide to Bebo, MoSoSo and more ;-). *The Daily Telegraph*, March 24, 2007, s. 001.

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. 2012. *Nebezpečí internetové komunikace III*. Olomouc: Univerzita Palackého v Olomouci, Pedagogická fakulta, ISBN 978-80-244-3087-4. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

KRÁL, Mojmír. 2006. Bezpečnost domácího počítače: Prakticky a názorně. 1. vyd. Praha: Grada, 334 s. ISBN 80-247-1408-6.

LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG a Kjartan ÓLAFSSON. 2011. *EU Kids Online: Final report*. LSE [online]. Sept 2011 [cit. 2013-07-20]. Dostupné z: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf

ZEMÁNEK, Jakub. 2004. *Slabá místa Windows aneb jak se bránit hackerům*. Computer Media, 156 s. ISBN 80-86686-11-6.

Sociální inženýrství a silná hesla

HOFFMAN, Sandra K a Tracy G MCGINLEY. [2010]. *Identity theft: a reference handbook*. Santa Barbara (Calif.): ABC-CLIO, c2010, xiii, 262 s. Contemporary world issues. ISBN 15-988-4144-0.

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. 2012. *Nebezpečí internetové komunikace III*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, Pedagogická fakulta, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

KRÁL, Mojmír. 2006. Bezpečnost domácího počítače: Prakticky a názorně. 1. vyd. Praha: Grada, 334 s. ISBN 80-247-1408-6.

LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG a Kjartan ÓLAFSSON. 2011. *EU Kids Online: Final report*. LSE [online]. Sept 2011 [cit. 2013-07-20]. Dostupné z: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf

Typy internetových hrozeb pro dospívající

BARTOSZ, Jakub. 2009. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. *IDnes* [online]. Praha: MAFRA [cit. 2013-07-28]. Dostupné z: http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba

Jessica Logan (18) hanged herself after her boyfriend circulated a nude photo of her. 2009. *Mydeathspace.com* [online] [cit. 2012-02-29]. Dostupné z: http://mydeathspace.com/article/2009/03/07/Jessica_Logan_%2818%29_hanged_herself_after_her_boyfriend_circulated_a_nude_photo_of_her

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. 2012. *Nebezpečí internetové komunikace III*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, Pedagogická fakulta, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

KRÁL, Mojmír. 2006. Bezpečnost domácího počítače: Prakticky a názorně. 1. vyd. Praha: Grada, 334 s. ISBN 80-247-1408-6.

LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG a Kjartan ÓLAFSSON. 2011. *EU Kids Online: Final report* [online]. London: The London School of Economics and Political Science, Sept 2011 [cit. 2013-07-20]. Dostupné z: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf

NEJEZCHLEBOVÁ, Lenka. 2009. SMS pro hnidu a video ze záchoda. Tak vypadá kyberšikana. *IDnes* [online]. Praha: MAFRA, 5. března 2009 [cit. 2013-07-21]. Dostupné z: http://zpravy.idnes.cz/sms-pro-hnidu-a-video-ze-zachoda-tak-vypada-kybersikana-p1l-/domaci.aspx?c=A090304_130312_domaci_nel

Případy kybergroomingu I. 2009. *E-bezpečí* [online] [cit. 2013-07-28]. Dostupné z: http://e-bezpeci.cz/index.php/temata/kybergrooming/33-112

Sedmnáctiletou oběť si našel na Facebooku, znásilnil ji a zavraždil. 2010. *Novinky.cz* [online]. Praha: Borgis [cit. 2012-02-28]. Dostupné z: http://www.novinky.cz/zahranicni/evropa/194196-sedmnactiletou-obet-si-nasel-na-facebooku-znasilnil-ji-a-zavrazdil.html

VEDROVÁ, Petra. 2011. Stalker ženu sledoval doma i na cestě do práce. *Policie České republiky* [online]. Praha: Policie České republiky, 24.11.2011 [cit. 2012-05-14]. Dostupné z: http://www.policie.cz/clanek/stalker-zenu-sledoval-doma-i-na-ceste-do-prace.aspx

WYNTER, Nadia. 2009. Parents of Holly Grogan, 15, blame Facebook for teen's suicide. *The New York times*. Monday, September 21, 2009. ISSN 0362-4331. Dostupné z: http://articles.nydailynews.com/2009-09-21/news/17933131_1_facebook-social-networking-bully

11.6 Odkazované zdroje

Akce – kyberšikana. 2014. *Základní škola Dačice: Komenského 7* [online]. 24. 4. 2014 [cit. 2014-08-28]. Dostupné z: http://www.zsdacice.eu/fotogalerie.php?typgalerie=99&typakce=1436

Barevný svět poznání. 2014. *Masarykova veřejná knihovna Vsetín* [online]. 9. 6. 2014 [cit. 2014-08-28]. Dostupné z: http://www.mvk.cz/knihovna/vsetin/barevny-svet-poznavani/

BAUEROVÁ, Marta. 2014. Kyberšikana. *Městská knihovna ve Svitavách* [online]. 11. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://www.booksy.cz/?p=2099

Dětské oddělení. [b.r.]. *Městská knihovna Pelhřimov* [online]. Pelhřimov: Městská knihovna Pelhřimov [cit. 2014-08-28]. Dostupné z: http://www.knih-pe.cz/index.php/detske-oddeleni

HOCH, Ivo. 2012. Diskusní konference. *Portál Knihovnického institutu Národní knihovny ČR* [online]. [cit. 2012-03-19]. Dostupné z: http://knihovnam.nkp.cz/sekce.php3?page=02_diskusni_konference.htm

CHRÁSTKOVÁ KNÍŘOVÁ, Michaela. 2013. Kyberšikana v dětských kolektivech. *Město Březová u Sokolova* [online]. 23. 5. 2013 [cit. 2014-08-28]. Dostupné z: http://mu-brezova.cz/?article_id=11846

IFLA/UNESCO Public Library Manifesto. 1994. In: *IFLA* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ifla.org/publications/iflaunesco-public-library-manifesto-1994

KOVÁŘOVÁ, Pavla a Gabriela ŠIMKOVÁ. 2014. Evidence-Based Learning Approach in Evaluation of Information Literacy Education. In: KURBANOĞLU, Serap, Esther GRASSIAN, Diane MIZRACHI, Ralph CATTS a Sonja ŠPIRANEC (eds.). *Information Literacy: Lifelong Learning and Digital Citizenship in the 21st Century, Ecil 2014, Dubrovnik, Croatia, October 20-23, 2014.* Revised selected papers. Switzerland: Springer, s. 560-569. ISBN 978-3-319-14136-7. DOI: 10.1007/978-3-319-14136-7. Dostupné z: http://link.springer.com/chapter/10.1007%2F978-3-319-03919-0_14

Kurz první pomoci záchrany života. 2013. *Městská knihovna v Praze* [online]. [cit. 2014-08-28]. Dostupné z: http://www.mlp.cz/cz/akce/e10812-kurz-prvni-pomoci-zachrany-zivota./

LATTA, Sara L. 2011. *Cybercrime: data trails do tell tales*. Berkeley Heights (NJ): Enslow, 104 s. True forensic crime stories. ISBN 15-984-5361-0.

Library lessons calendar. c2002-2014. *C.S. Porter Middle School* [online]. [cit. 2014-08-28]. Dostupné z: http://www.mcpsmt.org/Page/6273

LLOYD, Annemaree. 2010. *Information literacy landscapes: information literacy in education, workplace and everyday contexts*. 1st pub. Oxford: Chandos Publishing, xvi, 192 s. Chandos information professional series. ISBN 978-184-3345-077.

MACKNESS, Jenny, Sui Fai John MAK a Roy WILLIAMS. 2010. The ideals and reality of participating in a MOOC. In: DIRCKINCK-HOLMFELD, L., V. HODGSON, C. JONES, M. DE LAAT, D. MCCONNELL, a T. RYBERG. *Handbook and abstracts for the seventh International Conference on Networked Learning 2010: a research based conference on networked learning in higher education and lifelong learning*. Lancaster: University of Lancaster. ISBN 978-186-2202-252. Dostupné z: http://eprints.port.ac.uk/5605/1/The_Ideals_and_Realilty_of_Participating_in_a_MOOC.pdf

Manifest IFLA pro digitální knihovny. 2010. In: *Portál Knihovnického institutu Národní knihovny ČR* [online]. Prosinec 2010 [cit. 2014-08-26]. Dostupné z: http://knihovnam.nkp.cz/docs/IFLA/IFLA_Manifesto_for_Digital_Libraries_201012cz.pdf

Městská knihovna Přerov - březen 2014. 2014. *Přerov* [online]. Březen 2014 [cit 2014-08-28]. Dostupné z: http://prerov.nejlepsi-adresa.cz/akce-kalendar/mista/Mestska-knihovna-Prerov-Zerotinovo-namesti-36-Prerov/2014/3/31

Na internetu bezpečně. 2014. *Tišnovské noviny: příloha Tišnovských novin* [online]. Roč. 24, č. 4, s. 6 [cit. 2014-08-30]. Dostupné z: http://tisnov.cz/soubor/tisnovske_noviny_2014-04_web_priloha-kam.pdf

Nabídka knihovnických lekcí a besed na školní rok 2012 – 2013. 2012. In: *Regionální knihovna Karviná* [online]. Karviná: Regionální knihovna Karviná [cit. 2014-08-28]. Dostupné z: http://www.rkka.cz/KVC/KVC2013.pdf

Nabídka pro školy. [2014]. *Knihovna města Plzně* [online]. Plzeň: Knihovna města Plzně, Obvodní knihovna Doubravka [cit. 2014-08-28]. Dostupné z: http://www.knihomol.wz.cz/skoly.php

Nabídka tematických besed pro školy pobočka Jungmannova 2014/2015 pro 1. stupeň ZŠ. c2009 – 2014. *Knihovna města Olomouce* [online]. [cit. 2014-08-28]. Dostupné z: http://www.knihomol.wz.cz/skoly.php

Nabídka vzdělávání pro střední školy a gymnázia. [2014]. *Městská knihovna Prostějov* [online]. Prostějov: Městská knihovna Prostějov [cit. 2014-08-28]. Dostupné z: http://knihovnapv.webnode.cz/pro-skoly/ss/

Nástrahy v online světě: beseda pro 6. - 9. třídy ZŠ. 2014. *Knihovna města Ostravy* [online]. Ostrava: Knihovna města Ostravy [cit. 2014-08-28]. Dostupné z: http://cms.kmo.cz/www/cl-900/297-knihovnicke-lekce-a-besedy/?akce=240

OGROCKÁ, Eva. 2013. Nebezpečný internet aneb Co dělají vaše děti právě teď? *Inflow* [online]. 30. 11. 2013 [cit. 2014-08-30]. Dostupné z: http://www.inflow.cz/nebezpecny-internet-aneb-co-delaji-vase-deti-prave-ted

PC učebna. 2013. *Městská knihovna Litvínov* [online]. Litvínov: Městská knihovna Litvínov, 18. 2. 2013 [cit. 2014-08-28]. Dostupné z: http://www.knihovna-litvinov.cz/sluzby/pc-ucebna

PINTÉR, Josef. V havířovské Městské knihovně o hororové literatuře. 2014. *Karvinský deník* [online]. 18. 2. 2014 [cit. 2014-08-30]. Dostupné z: http://karvinsky.denik.cz/kultura_region/v-havirovske-mestske-knihovne-o-hororove-literature-20140218.html

Plán ZŠ Aloisina výšina na měsíc říjen 2012. *Základní škola, Liberec: Aloisina výšina* [online]. Liberec: Základní škola Aloisina výšina [cit. 2014-08-28]. Dostupné z: http://www.zs-aloisinavysina.cz/?D=186

PORS, Niels Ole. [2002]. The Public Library in the Electronic World: Veřejné knihovny v digitálním světě. In: *Portál Knihovnického institutu Národní knihovny ČR* [online]. Praha: Národní knihovna ČR, Knihovnický institut [cit. 2014-08-26]. Dostupné z: knihovnam.nkp.cz/docs/VerKnyDS.doc

Preventivní programy. c2014. *ZŠ Blansko Erbenova* [online]. Blansko: ZŠ Blansko, Erbenova [cit. 2014-08-28]. Dostupné z: http://www.erbenova.cz/detail-historie-clanky/560.html

Přednáškový blok: Digitální stopy (25. 2. 2014). 2014. *Novinkový systém SR FF UK* [online]. 22. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://sml.strada.ff.cuni.cz/novinka/629/

RÁBLOVÁ, Romana. 2014. Lapeni v síti. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/rablova_prezentace.pdf

Rámcové vzdělávací programy. c2013-2014. *Ministerstvo školství, mládeže a tělovýchovy* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy [cit. 2014-08-28]. Dostupné z: http://www.msmt.cz/vzdelavani/skolstvi-v-cr/skolskareforma/ramcove-vzdelavaci-programy

REID, Kate. 2014. Digital Citizenship – What does it mean to you?. *The Hutchins school library lions* [online]. 12. 5. 2014 [cit. 2014-08-28]. Dostupné z: http://blogs.hutchins.tas.edu.au/librarylions/2014/05/12/digital-citizenship-what-does-it-mean-to-you/

Scope & Sequence. 2012. *Common Sense Media* [online]. [cit. 2014-08-28]. Dostupné z: https://www.commonsensemedia.org/educators/scope-and-sequence

SEIDELIN, Susanne a Stuart HAMILTON (eds.). 2005. *Libraries, national security, freedom of international laws and social responsibilities*.. Copenhagen: IFLA/FAIFE Office, 406 s. World Report Series, vol. v. ISBN 87-988-0136-8. Dostupné z: http://www.ifla.org/files/assets/faife/publications/world-report-2005.pdf

STOWER, Helen. 2013. Online = Public…a lesson for students in taking care of your digital footprint. *EduBlogs* [online]. 16. 1. 2013 [cit. 2014-08-28]. Dostupné z: http://sallytilley.edublogs.org/2013/01/16/online-public-a-lesson-for-students-in-taking-care-of-your-digital-footprint/

SULLIVAN, Nancy. [b.r.]. iPad Lessons. *Madison High School Library* [online]. [cit. 2014-08-28]. Dostupné z: https://sites.google.com/site/madisonhslibrary/class-connections/ipad-lessons

The Role of Libraries in Lifelong Learning: Final report of the IFLA project under the Section of Public Libraries. 2003. In: *IFLA* [online]. [cit. 2014-08-28]. Dostupné z: http://archive.ifla.org/VII/s8/proj/Lifelong-LearningReport.pdf

XNOTION. 2010. How to Unblock Facebook. In: *HubPages* [online]. 7. 6. 2010 [cit. 2014-08-28]. Dostupné z: http://xnotion.hubpages.com/hub/How-to-Unblock-Facebook

ZADEMBSKÁ, Marika a Martin ČADRA. 2014. V pavučině sítí. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/zadembska_cadra_prezentace.pdf

ZVONKOVÁ, Lenka. 2009. Lekce děti upozorní na nebezpečí internetu. *Region Valašsko* [online]. 31. 3. 2009 [cit. 2014-08-28]. Dostupné z: http://www.regionvalassko.cz/aktuality_zobraz.php?lang=1&id=198&akt=2552&page=4

12 Seznam obrázků

13 Seznam tabulek

14 Seznam grafů

III. Přílohy

Příloha 1. Použité výzkumné nástroje

Příloha 1.1. Vzdělávání dětí v knihovnách k bezpečnosti na internetu

a) Představení

Vážené kolegyně a vážení kolegové,

jmenuji se Pavla Kovářová a jsem doktorandka na ÚISK FF UK a odborná pracovnice na KISK FF MU, kde se mj. zabývám informační bezpečností. Ráda bych Vás tímto požádala o spolupráci formou vyplnění krátkého dotazníku, jehož cílem je zmapování vzdělávání na téma bezpečnosti na internetu, především v knihovnách a se zaměřením na děti, ale i souvisejícího širšího kontextu. Výsledky dotazníku poslouží i k přizpůsobení několika plánovaných seminářů pro knihovníky na obdobná témata. Dále budou představeny na mezinárodní konferenci EU Kids Online (http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Conference.aspx) i v českých odborných periodikách.

Dotazník je složen z 10 otázek. Pokud je u některé možný výběr více odpovědí, budete na toto u ní upozorněni. Vyplnění by Vám nemělo zabrat déle než 10 minut.

Děkuji za spolupráci Pavla Kovářová

1. V jaké jste zaměstnán/a instituci (vyberte nejkonkrétnější možnost)? *

- školní knihovna
- akademická knihovna
- veřejná knihovna, která podle knihovního zákona není specializovaná knihovna
- jiná knihovna
- instituce školství mimo školní knihovnu
- instituce veřejné správy
- soukromá firma

2. Organizuje tato instituce vzdělávací aktivity (ne pro zaměstnance samotné instituce)? *

- ano
- ne (přejděte na otázku č. 8)

b) Vzdělávací aktivity v instituci

3. Jaké je obsahové zaměření vzdělávacích aktivit Vaší instituce? (možno více odpovědí)

   - zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
   - zkvalitnění práce s tradičními informačními zdroji
   - zkvalitnění práce s elektronickými informačními zdroji
   - kulturní akce
   - jiné (uveďte jedno nejvýznamnější)

4. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)

   - ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ne, ale podle mého názoru by měly
   - ne, podle mne to nemá smysl
   - pokud ano, jak často

5. Považujete děti za jednu z klíčových primárních cílových skupin vzdělávacích aktivit ve Vaší instituci (tj. vzdělávací akce pořádáte přímo pro ně a to minimálně 6 v roce)?

   - ano
   - ne (přejděte na otázku č. 8)

c) Vzdělávací aktivity pro děti

6. Jaké je obsahové zaměření vzdělávacích aktivit orientovaných na děti jako primární cílovou skupinu? (možno více odpovědí)

   - zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
   - zkvalitnění práce s tradičními informačními zdroji
   - zkvalitnění práce s elektronickými informačními zdroji
   - čtenářství
   - kulturní akce
   - doplnění výuky ve škole bez zaměření na aktivity knihovny (např. kreslení, fyzikální experimenty…)

- jiné (uveďte jedno nejvýznamnější)

7. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)

   - ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ne, ale podle mého názoru by měly
   - ne, podle mne to nemá smysl
   - pokud ano, jak často

d) Doplňující informace

8. Myslíte si, že by se knihovny měly v rámci svých vzdělávacích aktivit věnovat bezpečnosti dětí na internetu? *

   - ano
   - ne

9. Jaké znáte online vzdělávací projekty k tématu bezpečnosti dětí na internetu (nejsou myšleny jednorázové kampaně)? (možno více odpovědí) *

   - Bezpecne-online.cz
   - E-Bezpečí
   - E-Nebezpečí
   - Internet Hotline
   - Nebuď oběť
   - Pomoconline.cz
   - Protišikaně.cz
   - Saferinternet CZ
   - Žádný
   - Jiný (uveďte jeden nejvýznamnější)

10. Chcete k tématům v dotazníku něco dodat? Pokud chcete být informováni o umístění publikovaných výsledků tohoto dotazníku, uveďte kontaktní e-mailovou adresu.

Vaše odpovědi byly úspěšně odeslány, děkuji za vyplnění dotazníku.

Příloha 1.2. Rozšiřující deskripce vzdělávání

Dobrý den, jsme projekt iNeBe - informační (ne)Bezpečí, podporovaný Kabinetem informačních studií a knihovnictví Masarykovy univerzity v Brně. Chtěli bychom Vás požádat o vyplnění dotazníku zaměřeného na tématiku informační bezpečnosti, který nám pomůže zjistit jaký zájem mají knihovny o vzdělávání v této oblasti. Vyplnění dotazníku Vám zabere přibližně 8 minut. V případě, že máte jakýkoliv dotaz nebo zájem o spolupráci, pište na e-mail: inebe@seznam.cz. Děkujeme za Váš čas!

1. Prosím uveďte název města ve kterém se nachází Vaše knihovna: *
2. Zde prosím vyplňte název Vaší knihovny: *
3. Organizuje Vaše knihovna vzdělávací aktivity pro veřejnost? *
   - Ano
   - Ne
   - Nevím

   a) Aktivity v knihovně

4. Je některá z těchto aktivit zaměřená na počítačovou gramotnost nebo práci s počítačem/internetem? *
   - Ano
   - Ne
   - Nevím

   b) Vzdělávání v oblasti informační bezpečnosti

5. Věnujete se v rámci některé vzdělávací aktivity problematice informační bezpečnosti? *
   - Ano
   - Ne
   - Nevím

c) Vzdělávání v oblasti IB

6. Myslíte si, že je důležité vzdělávání v oblasti informační bezpečnosti? *
   - Určitě ano
   - Spíše ano
   - Spíše ne
   - Určitě ne
   - Nevím / nemohu odpovědět
7. Chtěli byste se vy osobně vzdělávat v oblasti informační bezpečnosti? *
   - Určitě ano
   - Spíše ano
   - Spíše ne
   - Určitě ne
   - Nevím
8. Měli byste zájem o přednášku či kurz na téma informační bezpečnosti ve Vaší knihovně?*
   - Určitě ano
   - Spíše ano
   - Spíše ne
   - Určitě ne
   - Nevím / nemohu odpovědět
9. Pokud by vám byla nabídnuta možnost vzdělávat se v problematice informační bezpečnosti, jaká forma výuky by Vám vyhovovala?

	Vyhovovala	Spíše vyhovovala	Spíše nevyhovovala	Nevyhovovala
E-learningový kurz *				
Klasické přednáškové lekce v rozsahu 5-10 lekcí *				
Jednorázový intenzivní workshop ve Vaší knihovně *				
Výuka ve virtuálním světě, např. SecondLife *				
Samostudium materiálů *				
Individuální školení s lektorem (max. 3 osoby) *				

d) Cestování

10. Byli byste ochotni na výuku dojíždět? *

	Ano	Ne
Praha *		
Brno *		
nejbližší krajská knihovna *		

e) Informace o kurzu

11. Kolik času týdně byste byli ochotni věnovat takovému kurzu? *

- Maximálně hodinu
- 1 - 2 hodiny
- 2- 3 hodiny
- 3- 4 hodiny
- 4 hodiny a více

12. Vyberte témata, která by Vás zajímala v kurzu: * Můžete vybrat z více možností

- problematika sociálních sítí
- nevyžádané zprávy (spam)
- malware (viry, červy, trojské koně…)
- zneužití osobních informací (vč. kyberšikany)
- autorské právo
- pornografie
- nevhodný a nelegální obsah (agresivita a násilí)
- specifičtí uživatelé (děti, firmy, stát…)
- šifrování (hesla, elektronický podpis…)
- prevence (jak svá data chránit)
- jiné (napište prosím jaké)

13. Měli byste zájem o metodické materiály, které by vám umožnily orientaci v problematice tak, abyste sami mohli ve Vaší knihovně přednášet na téma informační bezpečnosti? *

- Ano
- Ne

f) Typy materiálů

14. Jakou formu výukových materiálů preferujete? *

- podcasty (zvukové nahrávky)
- teoretické texty
- brožurky/letáčky
- videa
- zábavná forma (hry, komixy, křížovky…)
- teorie s možností ověření znalostí (test)
- jiné (napište prosím jaké)

g) Závěrečné otázky

15. V případě, že máte zájem o spolupráci, výukové nebo propagační materiály, vyplňte prosím Vaši e-mailovou adresu:

16. Místo pro Vaše vyjádření nebo připomínky a to ať už k dotazníku nebo problematice:

Děkujeme za Váš čas strávený s vyplňováním dotazníku!

Příloha 1.3. Didaktické testování

Dobrý den,

prosím o vyplnění dotazníku, jehož cílem je porovnat znalosti studentů oboru informační studia a knihovnictví a knihovníků o problematice digitálních stop. Výsledky budou použity pro tvorbu dizertační práce.

Vzhledem k cíli šetření prosím netipujte odpovědi, ale vyberte variantu „nevím“, pokud danou znalost nemáte. Vyplnění může být časově náročnější (přibližně 20 minut), výsledky ale budou o to přínosnější nejen pro publikování, ale také pro to, jaké vzdělávací aktivity Vám budou v budoucnu v souvisejících tématech nabízeny. Proto věřím, že vynaložený čas bude prospěšný i pro Vás.

Velmi děkuji za ochotu se tímto šetřením zabývat.

Pavla Kovářová
Kabinet informačních studií a knihovnictví, FF MU
Ústav informačních studií a knihovnictví, FF UK

1. Co jsou digitální stopy? (více možných odpovědí)*

   - *Historie vyhledávání, záznamy e-komerce (registrace, objednávky)*
   - *Informace s vypovídací hodnotou, uložená či přenášená v digitální podobě, tedy dokumenty, „otisky" činností technologického zařízení pracujícího s daty, metadata obsahující informace o daném souboru apod.*
   - *Informace zpřístupněné vědomým nahráváním a sdílením samotným uživatelem i zpřístupněné online bez záměrného přičinění uživatele*
   - *Jakákoliv digitální data, která mohou prokázat spáchání trestného činu nebo mohou poskytnout vazbu mezi trestným činem a jeho obětí či jeho pachatelem*
   - *Profily, které reklamním společnostem umožňují doručovat personifikovaná reklamní sdělení, vytvořené nejčastěji na základě sledování klíčových slov zadávaných do vyhledávačů a sledování pohybu napříč navštívenými webovými stránkami*
   - *Soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během využití informačních technologií*
   - *Záznamy komunikace přes mobil, tablet i GPS a podobná zařízení*
   - Nevím

2. Ve které oblasti si dokážete představit legální využití a ve které nelegální zneužití digitálních stop?*

	využití	zneužití	bez vlivu	nevím
hacking		X		
kriminalistika	X			
management (kontrola a monitoring)	X	X		
marketing	X	X		
mezilidská komunikace, např. zprávy i zeď na Facebooku	X	X		
personalistika	X	X		
správa informačních systémů a sítí	X	X		
státní správa	X			

3. Jak silně zneužitelné jsou informace, které je za určitých okolností možné zjistit z digitálních stop? (označte jednu možnost pro každý řádek)* (1 silně zneužitelné - 5 samostatně nezneužitelné)

	1	2	3	4	5	Nevím
cestovní plány		X				
citlivé údaje s potenciálem diskriminace (náboženství, přestupky proti zákonu…)	X					
číselné identifikátory a autentizací údaje (rodné číslo, uživatelské jméno a heslo…)	X					
dokumenty k osobě (vlastní i oblíbené cizí výtvory, fotky s ním…)			X			
identifikační údaje pro stát či firmy (jméno, příjmení, datum a místo narození, adresa trvalého pobytu…)	X					
informace o denní rutině (pravidelný dopravní spoj, zájmová sdružení, rozvrh…)		X				
navštívené webové stránky			X			

osobní informace možná za hranicí soukromí (podrobnosti přátelství a partnerství, nahé fotky v kojeneckém věku…)		X				
podrobnosti o movitém či nemovitém majetku			X			
povolání					X	
přibližná výše platu					X	
telefonní číslo, e-mailová adresa			X			
věk				X		
zájmy (koníčky, zdroje, názory…)			X			
zaměstnavatel, vzdělání				X		

4. Co je výsledkem deaktivace účtu na Facebooku? Vyberte jednu nejpřesnější odpověď.*

   - Informace vyprodukované uživatelem, který účet deaktivuje, budou odstraněny
   - *Účet bude neaktivní, ale vše zaznamenané na Facebooku zůstane, dokud nebudou podniknuty komplexnější kroky ke smazání*
   - Účet nebude přístupný, dokud ho uživatel znovu neaktivuje přes daný postup (např. potvrzení e-mailem, když byl účet deaktivován kvůli prozrazení přístupových údajů)
   - Všechny informace spojitelné s uživatelem budou odstraněny
   - Nevím

5. Jaké nástroje jsou využívány pro automatický pasivní (bez uživatelovy aktivity) sběr digitálních stop? (více správných odpovědí)*

   - CAPTCHA
   - *cookies*
   - crawler
   - *historie v prohlížeči*
   - hotspot
   - link farma
   - PageRank
   - *plugin v prohlížeči*
   - *sociální síť*
   - *vyhledavač*
   - *webbug (pixelový tag)*
   - jiný (doplňte)

6. Zhodnoťte upotřebení digitálních stop v problémech uvedených v tabulce. Pokud je pro realizaci digitální stopu nezbytné využít, zatrhněte pole „vyžaduje“. Pokud digitální stopa jen přispívá k úspěšnosti, ale není nezbytná, zatrhněte pole „podporuje“. Pokud problém s digitální stopou nepracuje, zatrhněte „bez vlivu“. Pokud pojem neznáte, zatrhněte „nevím“. (označte jednu či více možností)*

	Vyžaduje	Podporuje	Bez vlivu	Nevím
Krádež identity	X			
Kyberšikana		X		
Kyberstalking	X			
Kybergrooming	X			
Sexting	X			
Vydírání	X			
Malware		X		
Spam			X	
Scam		X		
Hoax			X	
Phishing		X		
Prolamování hesel		X		

7. Jaká varování mohu předznamenávat to, že se Vás někdo snaží zmanipulovat? (více možných odpovědí)*

   - *„ohánění se“ autoritou (nadřízený, známá organizace…) a znalostí bez kontextu*
   - *časový limit, naléhavost*
   - *formální (jazykové, typografické) chyby*
   - *napodobení očekávaného vzhledu (např. webu, adresy, vizuálu…)*
   - *nebezpečí (finanční či jiné)*
   - *nemožnost či omezení ověření*
   - *symboly pro zvýšení pozornosti (velká písmena, vykřičníky, $$$…)*
   - *útok na emoce (vina, soucit, ego přes flirtování či lichocení…)*
   - *vybuzení zájmu (zvědavost, finanční či jiný zisk s malými náklady)*
   - nic z uvedeného
   - jiné

8. Jaká preventivní opatření ve vlastním chování proti vytváření a využití digitálních stop znáte a které používáte?*

	znám a používám	znám, ale nepoužívám	neznám
Bezpečné používání silných hesel			
Čtení certifikátů, licenčních podmínek, varování, potvrzení…			
Egosurfing (vyhledání informací o konkrétním člověku)			
Nedůvěra k deklarované identitě (uvědomění si možností změny identity, např. spoofing, falešné údaje v registraci…)			
Nezjednodušování si práce na úkor bezpečnosti (např. pamatování hesel v prohlížeči)			
Prověřování aplikacemi typu antivir všeho staženého z internetu (soubory, e-maily…)			
Při neobvyklé žádosti (o informace, činnost…) ověřit oprávněnost			
Sledování aktuálních problémů a bezpečnostních řešení			
Šifrování (e-mailů, spojení…) či elektronický podpis, kde je to možné			
Uvážlivá práce s uživatelskými účty, především v operačním systému			
Uvážlivé publikování fotografií, videí a osobních údajů			
Vhodné nastavení soukromí u všech služeb, zejména sociálních sítí (např. nastavení aktualizací)			
Vhodné nastavení prohlížeče (např. správa cookies)			
Nejsou navštěvovány weby a stahovány soubory s nevhodným a nelegálním obsahem			
Využití více přihlašovacích jmen (přezdívek)			
Zamýšlení se nad možnými negativními i pozitivními důsledky a jejich zhodnocení před aktivitou			

9. Co znamená anonymní mód (InPrivate apod.) v prohlížeči? Vyberte jednu nejpřesnější odpověď.*

- Nejsou ukládány nikam žádné informace o uživateli a zařízení, které využívá
- Nejsou ukládány informace spojitelné s konkrétním uživatelem, ale jen obecné (např. preferovaný jazyk)
- *Jsou ukládány informace jako při běžném použití prohlížeče, ale po ukončení jsou smazány záznamy (historie, cookies apod.), kromě stažených souborů*
- Nevím

10. Jakou anonymizaci umožňují webové proxy servery? Vyberte jednu nejpřesnější odpověď.*

- Úplné skrytí veškerých technických informací o uživatelově zařízení, díky čemuž webové stránky mohou zjistit jen technické informace o proxy serveru
- Úplné skrytí IP adresy za adresu proxy serveru, o zařízení uživatele mohou weby zjistit jen obecné technické informace (např. rozlišení obrazovky pro správné zobrazení)
- *Skrytí IP adresy, které je ale neúčinné, pokud nejsou blokovány HTTP hlavičky nebo není důvěryhodný správce*
- Nevím

11. Jak fungují služby založené na onion routingu (např. TOR, JonDonym)? Vyberte jednu nejpřesnější odpověď.*

- *IP adresa a další údaje jsou skryty za údaji několika proxy serverů, navíc lze přenos šifrovat a použít pluginy pro šifrovaný přenos a blokování Flash a Java skriptů*
- Dostatečná anonymizace je zajištěna skrytím veškerých technických informací o uživatelově zařízení několikanásobným zašifrováním (jako vrstvy cibule), jiné funkce by službu nevhodně zpomalovaly
- Různé pakety jsou přes různé uzly sítě (rating), proto žádný uzel nezíská kompletní informaci o uživatelově zařízení či osobě
- Nevím

12. Co se stane při zablokování cookies s úmyslem zamezit vzniku digitální stopy? Vyberte jednu nejpřesnější odpověď.*

- *Některé služby nebudou správně fungovat, zejména pokud jsou spojeny s uživatelským účtem.*
- Služby nebudou moci shromažďovat žádné informace o uživateli, takže mu nebudou moci zasílat cílenou reklamu.
- Nezobrazí se některé části stránky (např. interaktivní, Flash videa apod.).
- Zvýší se bezpečnost uživatele, ale použití internetu to neovlivní, je to pro něj transparentní opatření.
- Nevím.

13. Jaké specializované nástroje proti vytváření a využití digitálních stop znáte a které používáte? (označte jednu možnost pro každý řádek)*

	znám a používám	znám, ale nepoužívám	neznám
Anonymizér			
Antiphishingový nástroj			
Antirootkit			
Antispam			
Antispyware			
Antivirus			
Filtry obsahu (whitelisty, blacklisty, indikátory slov, ruční hodnocení)			
Firewall			

14. Co jsou osobní údaje, které chrání český zákon a jeho evropské obdoby díky směrnici EU? Vyberte jednu nejpřesnější odpověď.*

- *Informace, které jednoznačně identifikují konkrétní fyzickou osobu ve fyzickém prostření (např. jméno, příjmení, adresa trvalého pobytu, datum narození)*
- Informace, které jednoznačně identifikují konkrétní osobu ve fyzickém i v elektronickém prostření (např. přístupové údaje)

- Informace, které jednoznačně identifikují konkrétní fyzickou nebo právnickou osobu (např. IČO, vedení organizace)
- Informace, které chce konkrétní člověk uchovat v soukromí (např. společenské vztahy, sociální vazby)
- Nevím

15. Když někdo přinese počítač na opravu, může se technik legálně podívat na data v počítači? Vyberte jednu nejpřesnější odpověď.*

- Ano, pokud je jeho úkolem i zálohovat data
- Ano, protože co mu zákon nezakazuje, to má povoleno a toto mu zákon nezakazuje
- Ne, pokud by musel nějak neoprávněně proniknout do systému (uhodnout heslo, využít bezpečnostní mezery informačního systému atp.); v opačném případě ano
- Ne, ale musí mu to zákazník výslovně zakázat
- *Ne, jde o narušení soukromí zákazníků a to není legálně možné*
- Nevím

16. Jste:*

- muž
- žena

17. V jaké fázi vysokoškolského vzdělávání v oboru informační studia a knihovnictví se nacházíte? (jedna odpověď)*

- studuji bakalářský stupeň
- studuji navazující magisterský stupeň
- studuji doktorský stupeň
- studuji jiný obor než informační studia a knihovnictví
- mám již dostudován obor informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- mám již dostudován jiný obor než informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- jiné

18. Jak byste popsal/a svůj zájem o téma digitálních stop? Vyberte jednu nejpřesnější odpověď.*

- vůbec mne to nezajímá a myslím, že nemá smysl tomu věnovat čas
- nezajímá mne to, ale myslím, že má smysl v této oblasti vzdělávat
- zajímá mne to jako běžného uživatele
- zajímá mne to a chci se této problematice věnovat hlouběji než běžný uživatel nebo o ní chci vzdělávat ostatní

19. Přiřaďte rozsah vzdělávání v tématu digitálních stop (nebo obecněji informační bezpečnosti), který jste absolvoval/a. (označte ve vybraném řádku jednu či více možností)*

	Žádné vzdělání	1-3 přednášky	Více přednášek	Samostatný předmět či seminář
před vysokou školou				
na vysoké škole mimo obor informační studia a knihovnictví				
na vysoké škole v rámci oboru informační studia a knihovnictví				
po vysoké škole mimo akce určené pro knihovníky a informační pracovníky				
po vysoké škole v rámci akce určené pro knihovníky a informační pracovníky				

20. Přiřaďte varianty vyjadřující Váš názor, jak by se mělo vzdělávat o digitálních stopách na ZŠ, VŠ a v knihovně. Vzdělávat by se…

a) nemělo.

b) mělo několika přednáškami nezaměřenými na informační bezpečnost, ale související.

c) mělo několika přednáškami o digitálních stopách v předmětech/vzdělávacích cyklech nezaměřených na informační bezpečnost.

d) mělo celým předmětem zaměřeným na inf. bezpečnost.*

Základní škola _____

Vysoká škola _____

Knihovna _____

Příloha 2. Pracovní listy pro koncepci vzdělávání v knihovnách

Příloha 2.1. K čemu je internet?

Příloha 2.1.1 Funkce internetu

I. Instalace softwaru, např. hry, Skype

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš.

Do adresního řádku nahoře napíšeš **URL adresu** služby, která zprostředkovává různý **software** a nabízí o něm informace. Když URL adresu neznáš, napíšeš do **vyhledávače** (např. Google) „software ke stažení“, vyhledávač ti v několika prvních výsledcích nabídne službu, kde je možné software stahovat. Kliknutím na název vybrané **webové stránky** se na ni dostaneš.

Do pole pro hledání napíšeš název (např. Skype) nebo typ softwaru (např. slovník), který chceš.

Ze seznamu si vybereš software, který se ti líbí, je zadarmo ke stažení a má dobré hodnocení (**recenze**). Na název vybraného software klikneš a pomocí tlačítka „stáhnout“ uložíš **soubor** z **internetu** do svého počítače.

Na stažený soubor dvakrát klikneš, tím ho otevřeš a pokračuješ podle pokynů, které se ti postupně ukazují.

Po nainstalování se ti objeví nová **ikona** na **Ploše** nebo pod tlačítkem „**Start**“, když na ni dvakrát klikneš, spustíš program, který máš nainstalovaný.

II. Komunikace přes software, např. Skype

Na počítači dvakrát klikneš na **ikonu softwaru**, pomocí kterého se chceš s někým bavit přes **internet**, tedy psát nebo povídat. Na tabletu na ikonu klepneš jednou.

Při prvním spuštění si vytvoříš **profil** tak, že vyplníš povinná pole ve formuláři registrace. Pro heslo a e-mail k registraci zavolej svou knihovnici.

Po vytvoření profilu nebo při dalším využívání se přihlásíš zadáním **přihlašovacího jména** (přezdívky) a **hesla**, které je nutné chránit, aby někdo nemohl používat tvůj profil za tebe.

V seznamu uživatelů si můžeš vybrat kamarády a známé, které si chceš přidat do **seznamu kontaktů**, abyste se spolu mohli bavit přes tento software. Obvykle si je vyhledáš pomocí jejich přihlašovacího jména po kliknutí na „hledat“, přidat kontakt“ a podobně.

Když si chceš s někým začít psát nebo povídat, klikneš na jeho jméno v seznamu kontaktů. Někdy ještě musíš vybrat způsob komunikace, tedy jestli mu třeba chceš poslat zprávu, zavolat nebo se bavit jinak.

Pokud už se s nikým v tu chvíli nechceš bavit, klikneš na „**odhlásit se**“, aby tvoji kamarádi viděli, že už nejsi na příjmu.

III. Komunikace přes internetový nástroj, např. e-mail, Facebook

Spustíš **internetový prohlížeč** (např.  ), že na něj dvakrát klikneš.

Do adresního řádku nahoře napíšeš **URL adresu** nástroje, přes který se chceš s někým bavit. Když URL adresu neznáš, napíšeš do **vyhledávače** (např. Google) název (např. Facebook) nebo typ nástroje (např. sociální síť), který hledáš. Vyhledávač tě na správnou URL adresu **webové stránky** posune kliknutím na vybraný výsledek hledání.

Při prvním použití nástroje si vytvoříš **profil** tak, že vyplníš povinná pole ve formuláři registrace. Pro heslo a e-mail k registraci zavolej svou knihovnici.

Po vytvoření profilu nebo při dalším použití se přihlásíš zadáním **přihlašovacího jména** (přezdívky) a **hesla**, které je nutné chránit, aby někdo nemohl používat tvůj profil místo tebe.

V seznamu uživatelů si můžeš vybrat kamarády a známé, které si chceš přidat do **seznamu kontaktů**, abyste se spolu mohli bavit přes tento nástroj. Obvykle si je vyhledáš pomocí jejich přihlašovacího jména po kliknutí na „hledat“, přidat kontakt“ a podobně.

Když si chceš s někým začít psát nebo povídat, klikneš na jeho jméno v seznamu kontaktů. Někdy ještě musíš vybrat způsob komunikace, tedy jestli mu třeba chceš poslat zprávu, zavolat nebo se bavit jinak.

Pokud už se s nikým v tu chvíli nechceš bavit, klikneš na „**odhlásit se**“, aby tvoji kamarádi viděli, že už nejsi na příjmu.

IV. Hraní online, např. Shakes & Fidget, Farmerama

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš. Na tabletu na ikonu prohlížeče klepneš jednou.

Do adresního řádku nahoře napíšeš **URL adresu** hry, která tě zajímá. Když URL adresu neznáš, napíšeš do **vyhledávače** (např. Google) název hry (např. Shakes & Fidget) nebo název služby, která odkazuje na různé hry (např. Good Game Studio) nebo jen „online hra". Vyhledávač ti zobrazí mnoho výsledků, ze kterých si vybereš, co tě zaujme. Klikneš na název vybraného výsledku a vyhledávač tě posune na správnou URL adresu **webové stránky.**

Při prvním použití hry si vytvoříš **profil** tak, že vyplníš povinná pole ve formuláři registrace. Pro heslo a e-mail k registraci zavolej svou knihovnici.

Po vytvoření profilu nebo při dalším použití se přihlásíš zadáním **přihlašovacího jména** (přezdívky) a **hesla**, které je nutné chránit, aby někdo nemohl používat tvůj profil místo tebe.

Ve hře je obvykle možné nějakou část hrát ve spolupráci s dalšími hráči, třeba v týmu. Dorozumívat se nejčastěji můžete psaním zpráv, přes **chat**, který vidí všichni nebo jen členové skupiny (cechu, klanu, gangu…).

Pokud už v tu chvíli nechceš hrát, klikneš na „**odhlásit se**", aby tvoji kamarádi viděli, že už nejsi na příjmu.

V. Vyhledávání informací, např. článků na vybrané téma do školy

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš. Na tabletu na ikonu prohlížeče klepneš jednou.

Do adresního řádku nahoře napíšeš **URL adresu** vybraného **vyhledávače** (např. Google).

Do rámečku, který ukazuje pole pro vyhledávání, napíšeš **klíčová slova**, ne otázku nebo větu. Když třeba hledáš vyjmenovaná slova, napíšeš do pole jen „vyjmenovaná slova", ne „Jaká jsou vyjmenovaná slova?". S výběrem klíčových slov ti může pomoct **našeptávač**, který ti ukazuje, co bys mohl chtít napsat, ještě než to dopíšeš.

Klikneš na tlačítko pro spuštění hledání („hledej“, obrázek lupy, „hledat Googlem“…) nebo na **klávesu** Enter.

Zobrazí se ti **webová stránka**, kde je seznam výsledků. Každý výsledek se skládá z nadpisu, kousku textu a URL adresy. Pomocí těchto ukázek se můžeš rozhodnout, jestli tě výsledek bude zajímat, nebo ne.

Pokud si nejsi jistý, nebo tě výsledek zajímá, klikneš na název výsledku nebo URL adresu a vyhledávač tě posune na vybranou stránku.

Pokud se ti stránka nelíbí, vrátíš se zpátky pomocí tlačítka v prohlížeči vlevo nahoře, kde je šipka doleva. A pak zkusíš jiný výsledek, který tě zajímá, dokud nenajdeš, co hledáš nebo nezkusíš jiná klíčová slova.

VI. Vyhledávání obrázků

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš. Na tabletu na ikonu prohlížeče klepneš jednou.

Do adresního řádku nahoře napíšeš **URL adresu** vybraného **vyhledávače** (např. Google).

V horní části zobrazené stránky klikneš na „Obrázky“. Do rámečku, který ukazuje pole pro vyhledávání, napíšeš **klíčová slova**, ne otázku nebo větu. Když třeba hledáš vyjmenovaná slova, napíšeš do pole jen „pes“, ne „Jak vypadá pes?“. S výběrem klíčových slov ti může pomoct **našeptávač**, který ti ukazuje, co bys mohl chtít napsat, ještě než to dopíšeš.

Klikneš na tlačítko pro spuštění hledání (např. „hledej“, ) nebo na **klávesu** Enter.

Zobrazí se ti **webová stránka**, kde je seznam výsledků, tedy jeden obrázek vedle druhého.

Když klikneš na vybraný obrázek, může se ti zvětšit s popiskem, kde je i URL adresa stránky, odkud je obrázek. Na ni se dostaneš tak, že klikneš na název výsledku nebo URL adresu. Někdy tě vyhledávač po kliknutí na obrázek rovnou posune na stránku, odkud obrázek vzal.

Pokud se ti stránka nelíbí, vrátíš se zpátky pomocí tlačítka v prohlížeči vlevo nahoře, kde je šipka doleva. A pak zkusíš jiný výsledek, který tě zajímá, dokud nenajdeš, co hledáš nebo nezkusíš jiná klíčová slova.

VII. Vyhledávání videí

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš. Na tabletu na ikonu prohlížeče klepneš jednou.

Do adresního řádku nahoře napíšeš **URL adresu** vybraného **vyhledávače** (např. Google).

V horní části zobrazené stránky klikneš na „Videa“ nebo „YouTube“. Do rámečku, který ukazuje pole pro vyhledávání, napíšeš **klíčová slova**, ne otázku nebo větu. Když třeba hledáš vyjmenovaná slova, napíšeš do pole jen „pes“, ne „Jak běhá pes?“. S výběrem klíčových slov ti může pomoct **našeptávač**, který ti ukazuje, co bys mohl chtít napsat, ještě než to dopíšeš.

Klikneš na tlačítko pro spuštění hledání („hledej“,  nebo na **klávesu** Enter.

Zobrazí se ti **webová stránka**, kde je seznam výsledků. Uvidíš **náhled** videa, název výsledku a nějaké další informace o videu.

Když klikneš na vybraný náhled nebo název, posune tě vyhledávač na stránku, odkud obrázek vzal.

Pokud se ti stránka nelíbí, vrátíš se zpátky pomocí tlačítka v prohlížeči vlevo nahoře, kde je šipka doleva. A pak zkusíš jiný výsledek, který tě zajímá, dokud nenajdeš, co hledáš nebo nezkusíš jiná klíčová slova.

VIII. Nahrávání souborů z počítače na internet

Spustíš **internetový prohlížeč** (např. ), že na něj dvakrát klikneš. Na tabletu na ikonu prohlížeče klepneš jednou.

Do adresního řádku nahoře napíšeš **URL adresu** služby, která umožňuje sdílení obrázků a videí s dalšími lidmi, buď hned, nebo po zadání přihlašovacího jména a **hesla**. Když URL adresu neznáš, napíšeš do **vyhledávače** (např. Google) název (např. Rajče) nebo typ nástroje (např. sdílení **souborů**), který hledáš. Vyhledávač tě na správnou URL adresu **webové stránky** posune kliknutím na vybraný výsledek hledání.

Někdy je nutné přihlášení. Při prvním použití si vytvoříš **profil** tak, že vyplníš povinná pole ve formuláři registrace. Po vytvoření profilu nebo při dalším použití se přihlásíš zadáním **přihlašovacího jména** (přezdívky) a **hesla**, které je nutné chránit, aby někdo nemohl používat tvůj profil místo tebe. Pro heslo a e-mail k registraci zavolej svou knihovnici.

Nástroj ti někde na hlavní stránce zobrazuje možnost „nahrát soubor“, „upload“, nebo „nahrát“ se slovem ukazujícím na typ souboru (např. video, obrázek, fotka…). Klikneš na místo, kde je toto napsané.

Zobrazí se ti okno podobné tomu, když otevřeš **složku** v počítači. Je v něm seznam souborů, vlevo je seznam složek. Pro nahrání musíš vědět, kde je uložený a proklikat se k němu, jako když ho hledáš pro otevření na počítači. Až se k němu dostaneš, jednou na něj klikneš a v okně dole potvrdíš tlačítkem „nahrát soubor“. Někdy takto můžeš vybrat více souborů.

Chvíli počkáš, než se vybraný soubor nahraje, někdy k němu doplníš nějaký popisek, nebo se ti ukáže **náhled** obrázku nebo videa. Většinou ti nástroj ukáže také URL adresu, kterou můžeš poslat tomu, s kým chceš soubory sdílet.

Jestli bylo pro nahrání souborů nutné se přihlásit, po skončení nahrávání zase klikni na tlačítko „**odhlásit se**“, aby ti někdo na tvém profilu nenahrával nebo nemazal soubory.

Příloha 2.1.2 Pětilístek

Kolik slov	Obsah	Ukázka	Můj pětilístek
1	Téma	e-mail	_____
2	Jaký je	potřebný, nepoužívaný	_____ _____
3	Co (se s tím) dělá	registruje, informuje, ukládá	_____ _____ _____
4	Co je pro tebe	nudná cesta k zajímavějšímu	_____ _____ _____ _____
1	Synonymum	pošta	_____

Příloha 2.2. Kdo je za monitorem?

Příloha 2.2.1 Mapa komunikace

Červená (text)

- světle (užší spojení s konkrétní osobou): E-mail
- středně (lze komunikovat s jedním i více lidmi současně): Instant Messaging
- tmavě (komunikace dostupná i veřejně, a to záznam či chat): Chat, Onlinovky, Shakes & Fidget, World of Warcraft, Farmerama, BiteFight

Žlutá: Telefonování

Oranžová (text a telefonování)

- tmavě (i veřejná; způsoby závislé na konkrétním herním serveru, některé komunikaci přímo ve hře neumožňují, jiné nabízí chat či telefonní hovor): Minecraft
- světle (možný Instant Messaging i telefonní hovor, světlá barva, protože komunikace nikdy není zcela veřejná): Skype, ICQ

Hnědá (všechny výše uvedené možnosti):

- Sociální sítě, Facebook, Twitter, Lidé, Google+

Modrá tmavě (komunikace necílená na konkrétní osobu a veřejná):

- Blog, Diskuzní fórum

Bílá (není komunikace):

- Google, Seznam

Příloha 2.2.2 Tabulka zjištěných identit

Moje číslo:

Moje jméno:

Na druhé straně:

	Jméno	Body
A		
B		
C		
D		
E		
F		
G		
H		
I		
J		
K		
L		
	Celkem odhaleno spolužáků	
	Minusové body za odhalení	
	Celkem	

Moje písmeno:

Moje jméno:

Na druhé straně:

	Jméno	Body
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
	Celkem odhaleno spolužáků	
	Minusové body za odhalení	
	Celkem	

Příloha 2.2.3 Když se mě někdo zeptá

Když se mě někdo, koho znám jen online, zeptá:...

http://us.123rf.com/400wm/400/400/candyman/candyman0706/candyman070600089/1158082-do-not-speak.jpg

Co dělá tvůj tatínek?
Co máš na sobě?
Co rád (ráda) posloucháš za hudbu?
Dáš si mne do přátel na Facebooku?
Chodíš na nějaké kroužky?
Jak vypadáš?
Jaká je tvoje oblíbená barva?
Jaké je tvoje číslo na mobil?
Jakou máš e-mailovou adresu?
Jakou onlinovku teď hraješ?
Jsi doma sám (sama)?
Jsi kluk nebo holka?
Kam chodíš do školy?
Kam chodíš na kroužky?
Kde bydlíš?
Kde máš počítač?
Kolik máš sourozenců?
Máš doma nějaké zvíře?
Nechceš se potkat?
Pošleš mi svou fotku?

http://static5.depositphotos.com/1002927/449/i/450/dep_4490852-Communication-Problem.jpg

… nepovím mu to.

… tak mu to řeknu.

Příloha 2.3. Mnoholičný lektvar na internetu

Příloha 2.3.1 Tabulka pravosti identit

Moje číslo:
Moje jméno:

Na druhé straně:

	Uváděné jméno	Pravda √	Lež ×	Body
A				
B				
C				
D				
E				
F				
G				
H				
I				
J				
K				
L				
M				
N				
O				
P				
Celkem odhaleno spolužáků				
Minusové body za odhalení				
Celkem				

Moje písmeno:
Moje jméno:

Na druhé straně:

	Uváděné jméno	Pravda √	Lež ×	Body
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
Celkem odhaleno spolužáků				
Minusové body za odhalení				
Celkem				

Příloha 2.3.2 Hesla

Typy útoků na hesla

Typ útoku	**Rychlost**	**Přibližná úspěšnost**
Útok uhodnutím (přenesením)	Minuty	30%
Slovníkový útok	Hodiny	70%
Útok hrubou silou	Až tisíce let	100%

Délka prolomení hesla (testování 100 hesel za sekundu, s ohledem na pravděpodobnost zjištění v 1. polovině obvykle interval dělen dvěma)

Počet znaků	**4**	**5**	**6**	**7**	**8**
0-9	2 minuty	16 minut	3 hodiny	1 den	11 dní
0-9, a-z	5 hodin	7 dní	8 měsíců	25 let	900 let
0-9, a-z, A-Z	2 dny	3 měsíce	18 let	1 000 let	70 000 let
0-9, a-z, A-Z, @*!	6 dní	1 rok	120 let	10 000 let	800 000 let

Formát bezpečného hesla

- více než 8 znaků, ideálně 12
- velká i malá písmena, číslice a speciální znaky (např. *+)
- nerozeznatelné smysluplné slovo (ani s vloženým písmenem či zvláštním znakem)
- není posloupností (např. 123456 nebo „asdfgh“ - písmena vedle sebe na klávesnici)

Bezpečné používání hesla

- žádná shoda se zjistitelnou informací (např. datum narození, jméno domácího mazlíčka, ani shoda s přihlašovacím jménem)
- neopakují se v různých službách
- pravidelně měněno, na důležitých místech do 90 dní, na běžných do půl roku
- nikomu neprozrazovat (ani nejlepšímu kamarádovi, stejně jako nepůjčíte kartáček na zuby), nezapisovat

Automatizace správy hesel

- správce hesel: Sticky Password, Password Depot, Password Corral, KeyWallet, Aha Password, Správce hesel, lastpass, a další
- náročnost hesla podle významu služby
- stejný postup, jiné heslo, např. Toto je moje heslo, které mám na Facebooku v lednu. => „Tjmh,kmnFv1.“ (první písmeno z každého slova, ponechána čárka a tečka ve větě, leden jako první měsíc nahrazen číslicí 1)

Kontrola bezpečnosti hesla

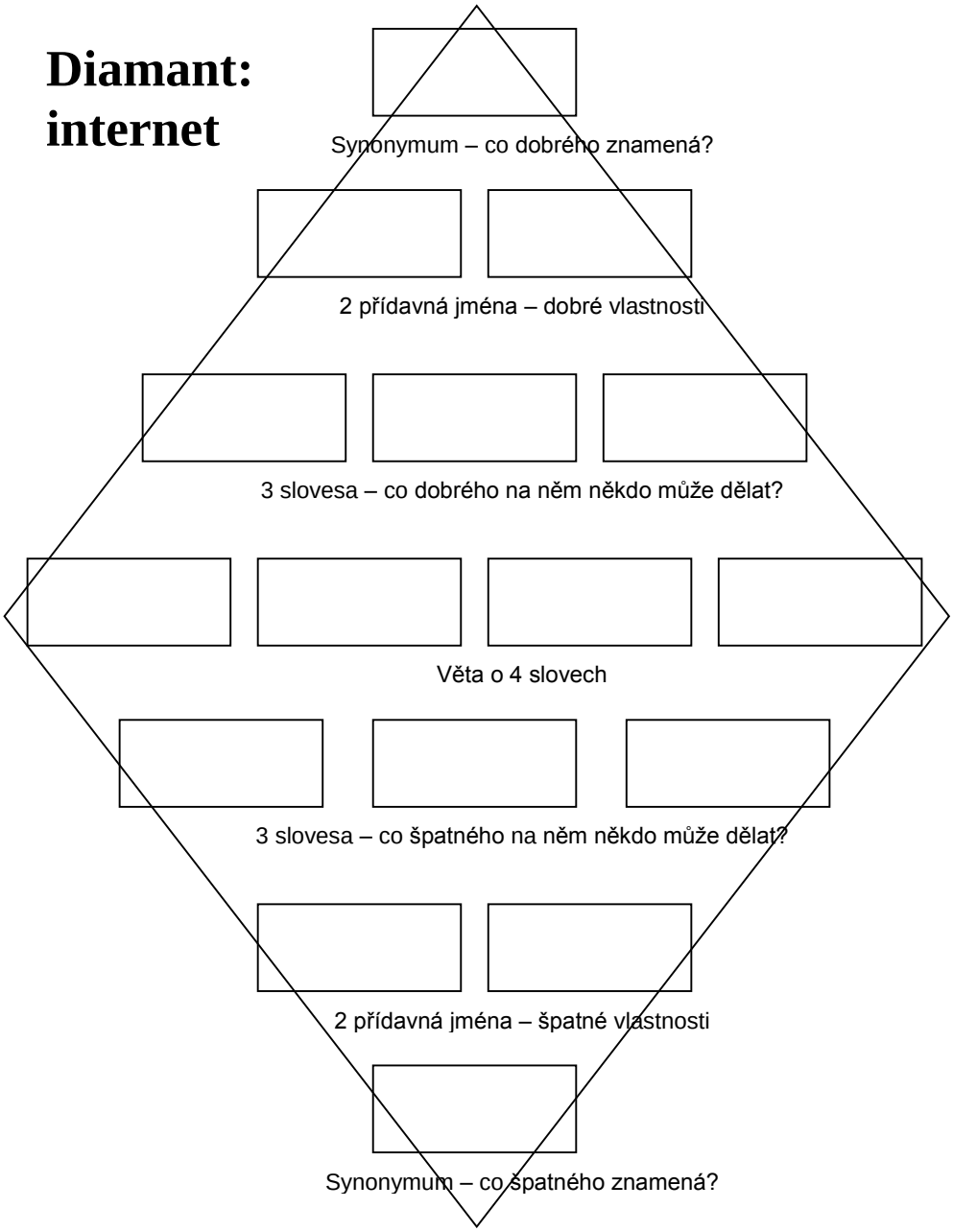
- Test Your Password (http://www.testyourpassword.com/) – v angličtině, ale velmi jednoduché, heslo se zadá do levého sloupce a čím víc vyskočí pod tím, tím lepší
- Tester síly hesla Password meter (http://www.paracom.cz/password.html) – poví všechno, kde jsou silné a slabé stránky hesla
- Změření odolnosti hesla (https://security.ics.muni.cz/kontrola-hesla) – hodně informací i to, za jak dlouho by bylo heslo prolomeno

Pro mne bezpečné heslo

……..

Příloha 2.4. Detektivky na Facebooku

Příloha 2.4.1 Diamant



Příloha 2.4.2 Čtení s předvídáním

Martina se smutně rozhlédla po pokoji. Na stěnách viděla fotky, kde se smála se svou nejlepší kamarádkou, pár obrázků z posledního třídního výletu, kytku, co si naposled natrhala u přehrady, když s pár dalšími lidmi chtěli využít teplého letního večera. Pak dala do kufru posledních pár kousků oblečení a zaklapla ho. Ten zvuk jí ukázal, že stěhování už je tady a celý její život končí a bude muset začít jinde znovu. Jak ji asi vezmou v půlce školního roku?

S přicházejícím jarem už odpověď na otázku při stěhování znala, ale byla horší, než si kdy představovala i v nejhorších snech. Pošťuchování, kterým to začalo, ještě čekala. Navzájem se s ostatními tipovali, co jsou zač. Postupně to ale začalo přecházet v něco, co už nemohla označit jako pošťuchování, protože jí to bylo nepříjemné. Neustálé narážky na její původ na vesnici, nemoderní oblečení, nenamalovaný obličej nabývaly na agresivitě i sprostosti.

Pak přišel konec školního roku a Martina doufala, že dvouměsíční pauza situaci uklidní. Ale po začátku školního roku to vypadalo spíš na to, že ostatní chtěli dohnat, co zameškali. Smáli se jí, když byla před tabulí. Zesměšňovali ji. Útoky zesilovaly. Vyvrcholilo to tím, že natočili shora kabinku záchodu, když měla průjem. A video kolovalo třídou… všichni se svíjeli smíchy, až na Martinu. Už nevěděla jak dál, tak se svěřila učitelce. Ta jí ale nevěřila a říkala, že to k jejich věku patří, že občas „rýpnou“. A že to je určitě jen jednorázový problém. Styděla se to říct doma, tak svůj problém jen naznačovala a doufala, že se objeví pomoc. Ta nepřicházela, proto jednou napsala na Facebook, že takový život nezvládne a musí ho skončit.

Stěhování ale nezabilo její předchozí přátelství, takže za pár minut zvonil Martinině mamce telefon a nejlepší kamarádka její dcery jí řekla, co Martina chystá. Martina to myslela vážně, ale včasný příchod její maminky zajistil včasnou pomoc.

Martina změnila školu, ale tím její starost neskončila. Už je sice neviděla ve škole, ale něco je stále spojovalo. Když se přihlásila na Facebook, opět se na ni vyřítila dávka sprostých slov spolu s odpornými obrázky, do kterých byla vložena její fotka. Mezi mnoha byla na její zdi básnička od „vzorné žačky“ z bývalé třídy: „Vypadá jako hnida/ ale je velká pinda/anglicky umí jen I miss you, I love you/ Ale na to jí říkám jen Fuck you.“ Vyvrcholilo to na Nový rok, kdy dostala „přání“: „Přeju ti vše nejhorší do nového roku. Smrt, mor, syfilis, tuberu, láskou nezamaskuješ žádný hemeroidy, hnidy. A dostaneš přes hubu hned na Nový rok.“ Ta hrůza z ponížení před milióny lidí pro ni byla nesnesitelná. Martina se zhroutila. Odmítala jíst.

Naštěstí opět zasáhla máma. Šla do Martininy bývalé školy a přesvědčovala učitelku, že je nutné něco udělat. Když se jí to stále nedařilo, obrátila se na policii, která případ začala řešit a došlápla si na ty, kdo Martině ubližovali. Skončilo to záznamem do prospěchu v chování a pokáráním. Snad to postačí, aby stejný zájem nevěnovali někomu dalšímu, když Martina už jejich cílem být nemohla.

Kyberšikana

Skutečnost: NEJEZCHLEBOVÁ, Lenka. SMS pro hnidu a video ze záchoda. Tak vypadá kyberšikana. IDnes [online]. 5. března 2009 [cit. 2013-07-21]. Dostupné z: http://zpravy.idnes.cz/sms-pro-hnidu-a-video-ze-zachoda-tak-vypada-kybersikana-p1l-/domaci.aspx?c=A090304_130312_domaci_nel

WYNTER, Nadia. Parents of Holly Grogan, 15, blame Facebook for teen's suicide. The New York times. Monday, September 21, 2009. ISSN 0362-4331. Dostupné z: http://articles.nydailynews.com/2009-09-21/news/17933131_1_facebook-social-networking-bully

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. Nebezpečí internetové komunikace III. 1. vyd. Olomouc: Pedagogická fakulta, 2012, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

Když se Monika zaregistrovala na internetové seznamce, těšila se, že tu konečně najde vhodného partnera. Když si vzpomněla na své spolužáky a kluky z turisťáku, věděla, že ve svém okolí hledat nemůže, nikdo z nich nebyl ten, o kom by mohla snít a s kým by si chtěla propsat celou noc. Ale na netu je přece dneska každý, tak se tam určitě musí najít i nějaký ON, který by jí ukázal, co znamená cítit to, o čem četla jen v knížkách a snila po svých oblíbených filmech.
Jednou se ozval zvuk oznamující novou zprávu. „Ahoj. Vím, že holce, jako jsi ty už muselo přijít hodně podobných zpráv, ale když jsem viděl tvou fotku, nemohl jsem si pomoct to nezkusit. Někoho tak hezkého jsem viděl jen v televizi. Nemám okolo sebe nikoho, s kým bych si mohl povídat tak, aby mi rozuměl. Z toho, co jsi o sobě ale napsala myslím, že bych konečně mohl najít spřízněnou duši. Mohli bychom se zkusit poznat, abychom nezahodili naději, že potkáme toho, o kom sníme?“
A tak si řekla, proč ne. Tím začaly týdny romantických zpráv a souznění v zájmech i tužbách. ON, se kterým se seznámila na internetu, ji okouzlil. Byl sice o nějaký rok starší, ale to nevadilo. Věkový rozdíl nebyl tak obrovský a pár let navíc mu dodávalo na zajímavosti. Měl tolik zkušeností, nějakou i špatnou za sebou, o to víc bylo jasné, jak si váží toho, co spolu mají. Mohla s ním zažívat jen a jen krásnější věci.
Zdál se tak milý. Nejspíš však ranila jeho ego, když mu oznámila, že to sice bylo hezké, ale že jsou mladí a chce poznat i někoho jiného, tak bude lepší, když zůstanou kamarádi. On to neunesl a začal ji bombardovat škaredými smskami, e-maily a neustále ji nutil, aby svůj názor změnila. Věci došly tak daleko, že zablokoval její mail, ze kterého začal posílat ošklivé a sexuálně laděné maily jejím rodičům a kamarádkám. Snažil se, aby trpěla tak, že podlehne, bude to chtít ukončit a vrátí se k němu.
Monice se podařilo smsky i maily zastavit a získat kontrolu nad schránkou. Ale on nepolevil. Začal ji sledovat, doprovázel ji ze školy, nechával výhružné vzkazy a několikrát jí dal před dveře mrtvé zvíře. Když před ním prchala temnou ulicí z kroužku, kde na ni opět čekal, se ho tak strašně bála, že na jednom rohu málem uklouzla a zvrtla si kotník.
Byla z toho už tak vyděšená, že když ji ten večer pronásledoval z práce, tak se rozhodla zavolat policii. Při bližším zkoumání vyšlo na povrch, že ten stejný mladík již byl několikrát řešen kvůli podobnému obtěžování jiných holek. Z tohoto důvodu se policie rozhodla zasáhnout a využít paragrafu Nebezpečné pronásledování v trestním zákoníku. Monika svůj profil na seznamce zrušila a raději se začala víc dívat okolo sebe na známé svých přítel, kteří jí mohli dopředu říct, o koho se zajímá.

Stalking

Skutečnost: VEDROVÁ, Petra. Stalker ženu sledoval doma i na cestě do práce. *Policie České republiky* [online]. 24.11.2011 [cit. 2012-05-14]. Dostupné z: http://www.policie.cz/clanek/stalker-zenu-sledoval-doma-i-na-ceste-do-prace.aspx

Petra se dívala z mostu na západ slunce a přemýšlela o posledním půlroce svého života. Když vzpomínala na nejšťastnější chvíle svého života, usmívala se, i když byly dávno pryč. Jak vše vypadalo růžové, jako ty červánky dneska. Kamarádky jí záviděli pěknou postavu a tvář, pozorného kluka, na kterého měla dost času, protože škola jí šla sama a tak ji úkoly neodváděly od pomalu, ale jistě se rozvíjejícího vztahu.

Ale rozvíjel se pomalu, nebo až moc rychle? Byli spolu, jak to šlo, ale chtěli ještě víc, proto si každý večer psali přes Facebook. Chatovali, posílali si odkazy na písničky a svoje fotky z telefonu. Obrázky posílání polibků jim brzo přestaly stačit a potom, co Petra poslala fotku ze sprchy, kde byla nahá, ale se zakrytými částmi těla, které ještě neviděl, Michal ztratil ostych a poprosil ji, jestli by mu ukázala něco víc, když s dotýkáním chce jít pomaleji.

Petra váhala, ale když jí napsal, jestli už nechce pokračovat v rozvoji jejich vztahu, tak se lekla, že by o něj mohla přijít. A fotky přece nic neudělají, jen bude mít radost a stejně je to ten, s kým chce jednou prožít všechno. Proto nakonec souhlasila pod podmínkou, že je nesmí nikomu ukázat. Michal souhlasil a tak si navzájem začali posílat čím dál odvážnější fotky.

Po dvou měsících už všechno nebylo tak růžové. Michala už fotky i Petra omrzeli a začal se dívat po jiných, ale zároveň jí vždycky udělal scénu, když jen stála vedle jiného. Těch mraků mezi nimi bylo čím dál víc, až mu Petra řekla, že by to raději měli skončit a žít si každý sám, když ji omezuje, ale nebere na ni ohled. Michal zuřil a křičel na ni, že je coura a že má určitě stejně někoho jiného. A když je coura, tak ať to vidí každý, když už to všichni vědí.

Po pár dnech Petra zjistila, jak to myslel. Založil na Facebooku diskusní skupinu na její jméno s podtitulem „mladé a chutné maso“ a nahrál tam fotky, které mu dřív posílala, doplněné o její označení a sprostý text. Ostatní je pak veřejně a nechutně komentovali, jindy ji označovali za děvku. Už po těch pár dnech bylo ve skupině víc než 500 lidí. A aby toho nebylo málo, do diskuze se zapojili i její spolužáci. Projevovali to nejen na Facebooku, ale i na chodbách a na ulici, kde za ní pokřikovali třeba „ukaž, že ty fotky nejsou montáž“ nebo „máš je menší než ta moje, ale na ty tvoje zas můžu koukat, kdy chci“. Petru to rychle začalo dohánět k šílenství.

Po dvou týdnech si řekla, že tak to dál nejde. Šla se projít a došla k mostu, kde začala vzpomínat. A když došla až k tomu, co má následovat, viděla jen málo cest, kam dál. Jedna z nich vedla přes zábradlí mostu. Přehodila jednu nohu a zhluboka se nadechla. V tom zafoukal vítr a jako by jí přinesl do hlavy druhou variantu. Nebylo to sice příjemné a jednoduché, ale mohla poprosit rodiče a linku pomoci, aby s ní našli cestu z problému, do kterého spadla. Vždyť máma jí vždycky říkala, že pro ni udělá všechno a taťka žas, že spolu všechno zvládnou. Teď čeká tyto tvrzení těžká zkouška, ale most nezmizí, a když to nepůjde, tak se sem vrátí. Zkusit to ale musí, vždyť ví, co je štěstí a chce ho ještě zažít.

Sexting

Skutečnost: Jessica Logan (18) hanged herself after her boyfriend circulated a nude photo of her. Mydeathspace.com [online]. 2009 [cit. 2012-02-29]. Dostupné z: http://mydeathspace.com/article/2009/03/07/Jessica_Logan_%2818%29_hanged_herself_after_her_boyfriend_circulated_a_nude_photo_of_her.

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. Nebezpečí internetové komunikace III. 1. vyd. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2012, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

Petr seděl u počítače a sám si gratuloval, že se dostal na level, který se mu ještě nikdy nepodařil. Zároveň děkoval ještě tomu, kdo mu s tím mohl. Sombrero byl dobrý spoluhráč, ještě že ho potkal a že zrovna oba potřebovali někoho ke spojení svých sil, aby se dostali dál. Už 14 dní spolu paří a vzájemně si pomáhají dostat své postavy tam, kde jim to samotným nešlo. A při jednání o postupech si občas prohodí pár informací o svém životě mimo počítač.

Jednou Sombrero Petrovi napsal, že by chtěl vidět, kdo mu pomohl projít přes bosse, jestli by mu to ukázal spřátelením na Facebooku. Petr neváhal a se zájmem se díval na docela chudý profil, který k jeho překvapení patřil docela pěkné holce. Překvapení přestal řešit, když mu Sombrero napsala, že je to jen proto, aby ji neignorovali všichni ve hře, že je holka, že i on by se s ní možná nespojil, kdyby to věděl. Od té doby spolu byli víc v kontaktu přes Facebook než přes onlinovku, takže i jejich povídání bylo spíš o nich než o strategii postupu. Bylo to s ní fajn a Petra občas napadlo, že by nebylo špatné ji poznat blíž, což jí taky jednou napsal.

Sombrero odpověděla, že není proti, ale trošku se seznamování na internetu bojí, tak jestli by jí neposlal další fotky. A aby věděla, jestli stojí za to, že by mohl zkusit odvážnější než jako z výletu s rodiči. Petr se sice zarazil, ale bál se, aby nevypadal jako mazánek, který si nic netroufne, tak si stoupl v koupelně před zrcadlo jen ve slipech a vyfotil se. Pak ještě chvíli váhal nad „enter“, ale nakonec ji zmáčkl. Za monitorem se přece nemusí červenat.

Petra ani nenapadlo, že by ho mohlo potkat, co následovalo. Přítelkyně se proměnila ve fúrii. Hrozila, že když jí nebude posílat odvážnější, pustí o něm po Facebooku, že je na kluky, a zveřejní nahé fotky, kde se pozná. Po fotkách přišlo video, kde musel ukazovat, jak si sám se sebou „hraje“. Ani to jí nebylo dost a jednou se Petrovi objevil ve schránce požadavek, že se chce potkat. A opět nechybělo pár poznámek, co bude následovat, když se mu to nebude líbit. Co mu zbývalo. Doma řekl, že se jede učit ke spolužákovi, protože potřeboval dost času a pravdu říct nemohl. Pak se vydal na zastávku autobusu, která ho měla dovést na místo.

Petr čekal na lavičce v parku. Když se jeho společnice neobjevovala, začal se procházet. Přešlapoval sem a tam, když za jeho zády zapraskala větev. Než se stačil ohlédnout, cizí ruce ho popadly a někdo ho surově vláčel k autu. Vše se seběhlo tak rychle, že se ani nestačil bránit. Dotyčný ho svázal ruce a nacpal do pusy roubík. Když auto zastavilo, byl zavlečen do staré barabizny. Dotyčný ho začal svlékat, a když se bránil, surově ho uhodil. A pak už to šlo ráz na ráz. Petr křičel bolestí. Ale přes roubík to nebylo slyšet. Připadalo mu to jako věčnost a když s ním skončil, celé jeho tělo se třáslo v nastalém šoku. Muž beze slova odešel.

Petr se ztěžka doplazil z domu k silnici, kde ho našel neznámý řidič a dovezl ho do nemocnice. Pak už nešlo nic tajit. Případu se okamžitě ujala policie a po prošetření je stopy zavedly k již několikrát trestanému násilníkovi. Zjistilo se, že podobnou komunikaci na Facebooku vedl s několika chlapci. Soud ho uznal vinným celkem ze sedmi případů pohlavního zneužívání, třinácti případů vydírání. Byl odsouzen na 8 let vězení.

Grooming

Skutečnost: Sedmnáctiletou oběď si našel na facebooku, znásilnil ji a zavraždil. Novinky.cz [online]. 2010 [cit. 2012-02-28]. Dostupné z: http://www.novinky.cz/zahranicni/evropa/194196-sedmnactiletou-obet-si-nasel-na-facebooku-znasilnil-ji-a-zavrazdil.html.

Případy kybergroomingu I. E-bezpečí [online]. 2009 [cit. 2013-07-28]. Dostupné z: http://e-bezpeci.cz/index.php/temata/kybergrooming/33-112

BARTOSZ, Jakub. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. IDnes [online]. 2009 [cit. 2013-07-28]. Dostupné z: http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba

Mirek seděl opřený před monitorem a přemýšlel, proč se nemůže přihlásit ke svému účtu na Facebooku. Překlep to být nemůže, zkoušel to pětkrát a vždycky neúspěšně, zkontroloval i klávesy Caps Lock a Num Lock, že má českou a ne anglickou klávesnici, prostě všechno. A heslo má všude stejné, takže omyl taky nehrozil. Tak co se proboha mohlo stát? Přemýšlel, kde mohl vzniknout problém.
Heslo si nikam nepsal, ale občas ho řekl někomu, od koho něco potřeboval. Třeba poslat mail do školy, aby si to přiřadili k jeho jménu, ale nebyl včas u počítače, tak poprosil kamaráda. A pak jednou zapomněl v knihovně odškrtnout „zapamatovat si heslo“, když se tam přihlašoval. Uhodnout ho asi nikdo nemohl, koho by napadlo, že používá „2hokejky“. No tak zkusí si poslat nové heslo při zapomenutí. To ale dlouho nepřicházelo…
Druhý den přišel do školy a všichni se od něho otáčeli. Pak za ním přiběhl jeho kamarád Adam a začal křičet, jak si mohl něco takového dovolit, že si to škaredě odskáče, kdo ho bude tak urážet. Mirek se ho snažil zastavit a zjistit, co se děje. Adam stále křičel, že snad ví, co píše na Facebooku a odešel. Byl to nekonečný den plný zlých pohledů i slov. Když Mirek přiběhl domů, poprosil svou sestru, kterou měl v přátelích, aby se podívala na jeho profil na Facebooku.
Přestože se Mirek na svůj profil nemohl celý den přihlásit, z jeho účtu bylo zveřejněno a odesláno pěkných pár zpráv. A asi se dostaly k mnoha z jeho skoro 300 přátel. Na jeho profilu bylo také mnoho nahých fotografií s vloženým obličejem Mirka. Zároveň bylo jasné, že se útočník prostřednictvím krádeže profilu Mirka dostal také do neveřejných částí profilů jeho virtuálních přátel, začal je obtěžovat, psal jim vulgární vzkazy, nevhodně komentoval jejich fotografie atd. Vše pod jménem Mirka.
Trvalo dlouhou dobu, než alespoň nejdůležitější přátele Mirek přesvědčil, že jeho profil neovládá on sám a někdo mu ho ukradl. Zároveň jim dal najevo, že si kvůli tomu založí nový profil a tím problém vyřeší, zatím, že starý profil mají zablokovat nebo odstranit z přátel. To se asi stalo tak hromadně, že si toho útočník všimnul a rozhodl se pro novou strategii. Vytvořil na Facebooku nový profil s Mirkovým jménem, vyvěsil na něm Mirkovy fotografie, ale i jméno, skutečné telefonní číslo, adresu školy, kterou Mirek navštěvoval a další citlivé údaje. Mnoho přátel si ho přidalo, protože očekávali Mirkův nový profil. Po krátké době opět jménem Mirka anonymní útočník vstupoval do internetových diskusí, kde obtěžoval ostatní, urážel je, napadal, vyhrožoval jim. Mirek se o existenci profilu dozvěděl od své spolužačky, která jej náhodou objevila.
Po těchto dvou zkušenostech už Mirek nevěděl, co dál. Nejdřív chtěl fungovat úplně bez Facebooku, ale brzo zjistil, že to nejde, že by tak nevydržel, když se tak spolu baví všichni, jen on je vyloučený. Nakonec se rozhodl pro poslední pokus využívat Facebook, alespoň na minimální úrovni se zcela falešnými údaji, spojením jen na pár nejbližších přátel a velmi silně nastavenými pravidly pro ochranu soukromí, které stále kontroloval nejen u sebe, ale i u svých přátel, aby tím chránil je i sám sebe a jeho pronásledovatel ho opět nenašel a neukradnul mu jeho identitu a sociální síť.

Krádež identity

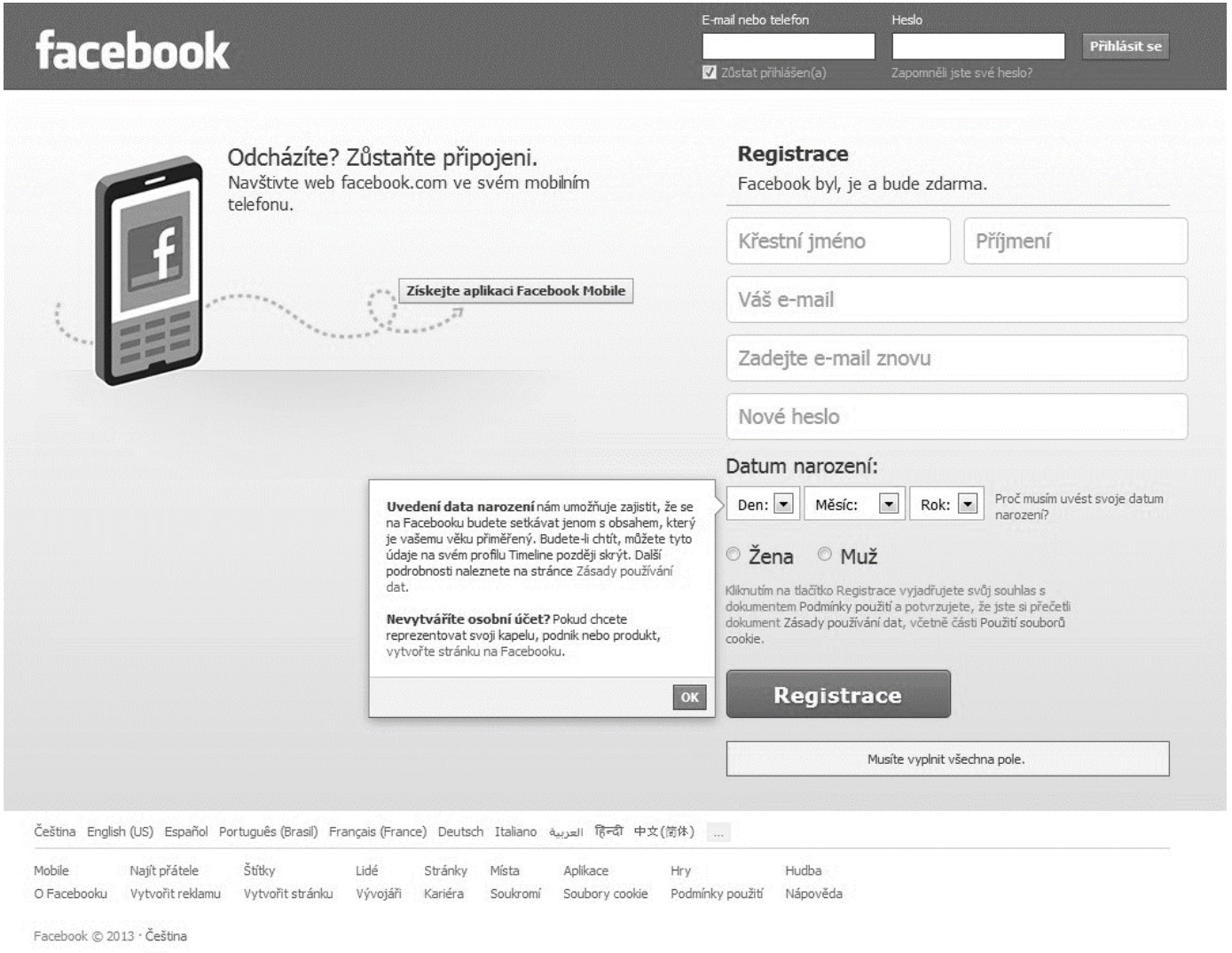
Skutečnost: KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. Nebezpečí internetové komunikace III. 1. vyd. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2012, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

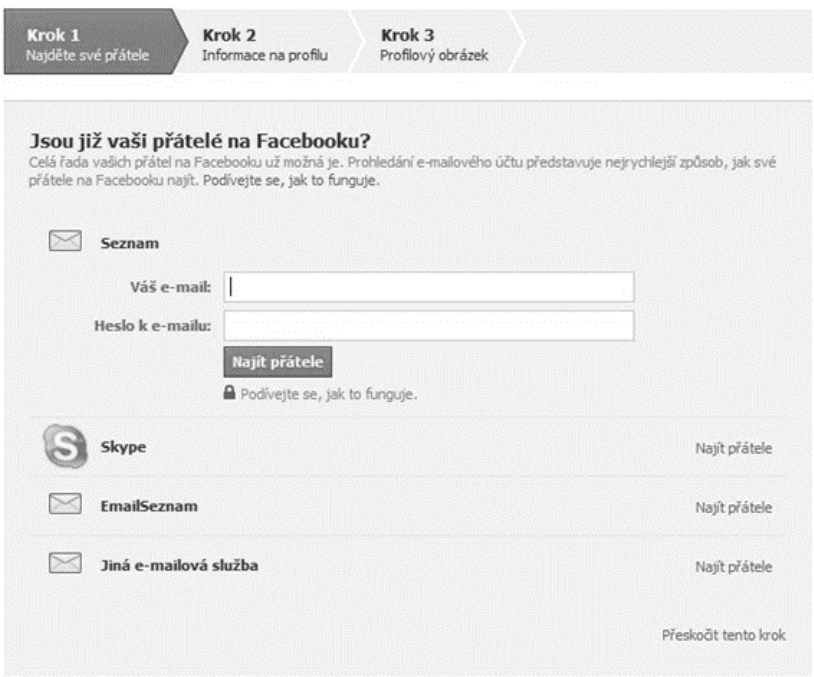
Příloha 2.4.3 Tabulka pro předvídání

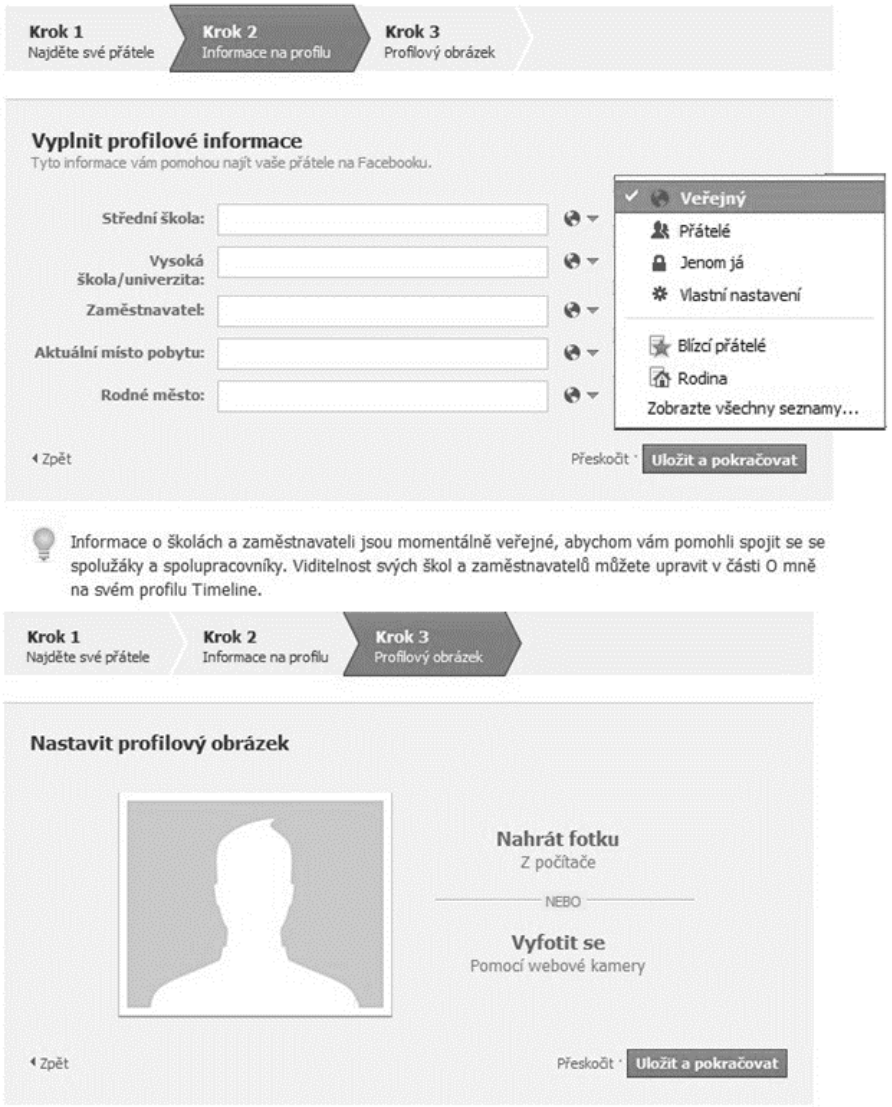
Tabulka předpovědí Jména..... čtený text..... datum.....

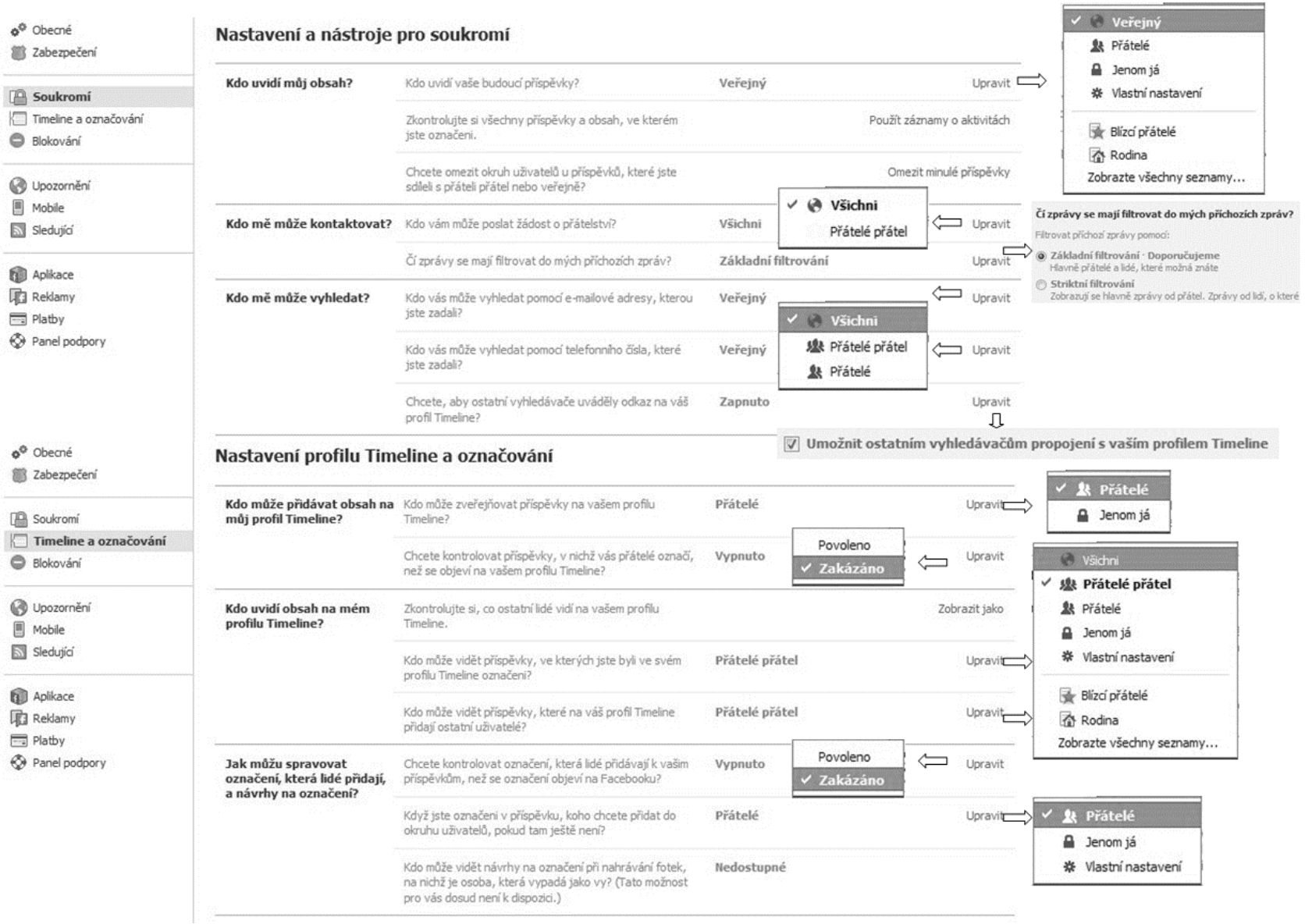
Část textu	**Jak se podle vás bude příběh vyvíjet? (Pište v celých větách)**	**Proč si to myslíte?**	**Co se opravdu dosud stalo? (Pište v celých větách)**
Po 1. části textu			
Po 2. části textu			
Po 3. části textu			
Po 4. části textu			
Po 5. části textu			
Po 6. části textu + skutečnost			

Příloha 2.4.4 Registrace na Facebook




Krok 1
Najděte své přátele
Krok 2
Informace na profilu
Krok 3
Profilový obrázek
Jsou již vaši přátelé na Facebooku?
Celá řada vašich přátel na Facebooku už možná je. Prohledání e-mailového účtu představuje nejrychlejší způsob, jak své přátele na Facebooku najít. Podívejte se, jak to funguje.
Seznam
Váš e-mail:
Heslo k e-mailu:
Najít přátele
Podívejte se, jak to funguje.
Skype
Najít přátele
EmailSeznam
Najít přátele
Jiná e-mailová služba
Najít přátele
Přeskočit tento krok
Facebook za vás uloží seznam kontaktů, abychom vám pomohli oslovit další lidi a spojit se s přáteli.
Další informace


Krok 1
Najděte své přátele
Krok 2
Informace na profilu
Krok 3
Profilový obrázek
Vyplnit profilové informace
Tyto informace vám pomohou najít vaše přátele na Facebooku.
Střední škola:
Vysoká škola/univerzita:
Zaměstnavatel:
Aktuální místo pobytu:
Rodné město:
Veřejný
Přátelé
Jenom já
Vlastní nastavení
Blízcí přátelé
Rodina
Zobrazte všechny seznamy...
Zpět
Přeskočit
Uložit a pokračovat
Informace o školách a zaměstnavateli jsou momentálně veřejné, abychom vám pomohli spojit se se spolužáky a spolupracovníky. Viditelnost svých škol a zaměstnavatelů můžete upravit v části O mně na svém profilu Timeline.
Krok 1
Najděte své přátele
Krok 2
Informace na profilu
Krok 3
Profilový obrázek
Nastavit profilový obrázek
Nahrát fotku
Z počítače
NEBO
Vyfotit se
Pomocí webové kamery
Zpět
Přeskočit
Uložit a pokračovat
Profilové obrázky a úvodní fotky jsou veřejné. U ostatních fotek, které na Facebook nahráváte, si můžete okruh uživatelů vybrat.


Obecné
Zabezpečení
Soukromí
Timeline a označování
Blokování
Upozornění
Mobile
Sledující
Aplikace
Reklamy
Platby
Panel podpory
Nastavení a nástroje pro soukromí
Kdo uvidí můj obsah?
Kdo uvidí vaše budoucí příspěvky?
Veřejný
Upravit
Veřejný
Přátelé
Jenom já
Vlastní nastavení
Blízcí přátelé
Rodina
Zobrazte všechny seznamy...
Zkontrolujte si všechny příspěvky a obsah, ve kterém jste označeni.
Použít záznamy o aktivitách
Chcete omezit okruh uživatelů u příspěvků, které jste sdíleli s přáteli přátel nebo veřejně?
Omezit minulé příspěvky
Kdo mě může kontaktovat?
Kdo vám může poslat žádost o přátelství?
Všichni
Upravit
Všichni
Přátelé přátel
Čí zprávy se mají filtrovat do mých příchozích zpráv?
Základní filtrování
Upravit
Čí zprávy se mají filtrovat do mých příchozích zpráv?
Filtrovat příchozí zprávy pomocí:
Základní filtrování · Doporučujeme
Hlavně přátelé a lidé, které možná znáte
Striktní filtrování
Zobrazují se hlavně zprávy od přátel. Zprávy od lidí, o které
Kdo mě může vyhledat?
Kdo vás může vyhledat pomocí e-mailové adresy, kterou jste zadali?
Veřejný
Upravit
Všichni
Přátelé přátel
Přátelé
Kdo vás může vyhledat pomocí telefonního čísla, které jste zadali?
Veřejný
Upravit
Chcete, aby ostatní vyhledávače uváděly odkaz na váš profil Timeline?
Zapnuto
Upravit
Umožnit ostatním vyhledávačům propojení s vaším profilem Timeline
Obecné
Zabezpečení
Soukromí
Timeline a označování
Blokování
Upozornění
Mobile
Sledující
Aplikace
Reklamy
Platby
Panel podpory
Nastavení profilu Timeline a označování
Kdo může přidávat obsah na můj profil Timeline?
Kdo může zveřejňovat příspěvky na vašem profilu Timeline?
Přátelé
Upravit
Přátelé
Jenom já
Chcete kontrolovat příspěvky, v nichž vás přátelé označí, než se objeví na vašem profilu Timeline?
Vypnuto
Povoleno
Zakázáno
Upravit
Kdo uvidí obsah na mém profilu Timeline?
Zkontrolujte si, co ostatní lidé vidí na vašem profilu Timeline.
Zobrazit jako
Kdo může vidět příspěvky, ve kterých jste byli ve svém profilu Timeline označeni?
Přátelé přátel
Upravit
Kdo může vidět příspěvky, které na váš profil Timeline přidají ostatní uživatelé?
Přátelé přátel
Upravit
Všichni
Přátelé přátel
Přátelé
Jenom já
Vlastní nastavení
Blízcí přátelé
Rodina
Zobrazte všechny seznamy...
Jak můžu spravovat označení, která lidé přidají, a návrhy na označení?
Chcete kontrolovat označení, která lidé přidávají k vašim příspěvkům, než se označení objeví na Facebooku?
Vypnuto
Povoleno
Zakázáno
Upravit
Když jste označeni v příspěvku, koho chcete přidat do okruhu uživatelů, pokud tam ještě není?
Přátelé
Upravit
Přátelé
Jenom já
Vlastní nastavení
Kdo může vidět návrhy na označení při nahrávání fotek, na nichž je osoba, která vypadá jako vy? (Tato možnost pro vás dosud není k dispozici.)
Nedostupné

Příloha 3. Rozhovory v akčním výzkumu

Příloha 3.1. Formulář poučeného souhlasu

Poučený souhlas

Tímto uděluji PhDr. Pavle Kovářové, r. č. , poučený souhlas k neanonymnímu publikování autorizovaných výsledků rozhovoru v její dizertační práci. Cílem publikovaných informací bude popsat názory a argumenty k vzdělávání v knihovnách o tématu digitálních stop a jejich zneužívání s důrazem na spolupráci škol a knihoven při tomto vzdělávání. Ke zpracování dojde na základě polostrukturovaného rozhovoru zaznamenaného ve formě videa pro potřeby vyhodnocení zjištění. Videozáznamy nebudou publikovány, po zpracování budou uchovány jen pro potřeby pozdějšího přezkoumání.

Jméno:
Pozice pro výzkum:
Podpis:

Příloha 3.2. Seznam otázek pro rozhovor

Aktuální pohled na knihovnu a informační bezpečnost

a) Povědomí o problematice a vzdělávání obecně

1. Jak byste definoval/a digitální stopy a jaké problémy jsou s nimi spojeny?
2. Má podle Vás smysl vzdělávat v oblasti digitálních stop a (proti) jejich zneužití?

b) Knihovny v problematice a názor na to

3. Jak byste popsal/a svůj aktuální názor na to, jestli knihovny mají vzdělávat v tématu digitálních stop a (proti) jejich zneužití?
4. Jak se na spojení vzdělávání o digitálních stopách v knihovnách podle Vás dívají obecně knihovníci/školy/veřejnost či její určité části?

c) Obsah vzdělávání

5. Jaká subtémata by se měla při tomto vzdělávání v knihovnách řešit?
6. Pro koho by měla být nabízena?
7. A jakou formou?
8. Při srovnání s jinými tématy, co by měla knihovna upřednostnit (knihy X internet; témata v rámci internetu; v subtématech digitálních stop)?

d) Připravenost knihovníků

9. Dokážete si Vy osobně představit, že by se toto téma řešilo v každé knihovně?
10. Co by pro to muselo být zajištěno?
11. Proč myslíte, že dnešní aktivní knihovnici jsou či nejsou připraveni vzdělávat v této problematice?
12. Vzdělávají podle Vás střední, vyšší a vysoké školy budoucí knihovníky, aby toto téma mohli řešit?
13. Co by tyto školy měly dělat, aby to jejich absolventi mohli řešit?
14. Co by měli absolventi pro to znát a jak hluboce?

e) Dřívější názory

15. Jak jste dříve pohlížel/a na to, že by knihovny vzdělávaly v problematice digitálních stop?
16. Kdy a čím se to měnilo?
17. Jakou jste měl/a představu o možnosti lekcí a jejich reálnosti?
18. Bylo nějak téma digitálních stop řešeno dřív v nějaké lekci knihovny?
19. Jak to vypadalo?
20. Jak byste popsala stav před lekcí, tj. do jakého prostředí byla implementována, co mohlo ovlivnit její realizaci?
21. Co podle Vás přesvědčilo knihovnu pustit se do realizace lekce?
22. A co přesvědčilo školu (paní učitelky)?

f) Názory k uskutečněné lekci

23. Co si myslíte o uskutečněné lekci?
24. Změnila nějak právě ona Vaše názory? V čem?
25. Mělo by se podle Vás něco v uskutečněné lekci změnit?
26. Jaké pozitivní či negativní výsledky podle Vás má a na koho?
27. Myslíte, že je rozšiřitelná na další prostředí (školy, knihovny, věk cílové skupiny…)?
28. Na jaká a za jakých podmínek?
29. Co si myslíte, že si z ní děti odnesly?
30. Myslíte si, že by se na ni mělo navázat? Jak?