

UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA

RIGORÓZNÍ PRÁCE

Ochrana osobnosti nezletilých v kyberprostoru

The Protection of Personality Rights of Minors in Cyberspace

Konzultant: prof. JUDr. Jan Dvořák, CSc.

Zpracovatel: Mgr. Veronika Křížová, LL.M.

duben 2013

„Prohlašuji, že jsem předkládanou rigorózní práci vypracovala samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.“

V Praze dne 5.4. 2013

Mgr. Veronika Křížová, LL.M.

Poděkování

Ráda bych na tomto místě poděkovala prof. JUDr. Janu Dvořákovi, CSc. za odborné vedení a cenné připomínky při zpracování této práce. Ráda bych také poděkovala právnické fakultě UC Berkeley a Berkeley School of Information za zázemí poskytnuté při shromažďování podkladů pro vypracování této práce.

Obsah

Obsah	3
Seznam použitých zkratk.....	5
Úvod.....	6
Historický vývoj práva na ochranu osobnosti v kontextu kyberprostoru	8
Vymezení základních pojmů.....	12
1. Ochrana osobnosti a kyberprostor: některé z běžných služeb způsobilých ohrožení či zásahu do osobnostních práv uživatele	21
1.1. Web 2.0: Sdílení uživatelských dat v kyberprostoru.....	21
1.2. Anonymita služeb na Internetu.....	25
1.2.1. Případová studie <i>Moreno v. Hartford Sentinel, Inc.</i>	26
1.3. Problematika sociálních sítí.....	28
1.3.1. Právní závaznost a vymahatelnost Podmínek užívání	29
2. Nezletilý na Internetu.....	34
2.1. Úvod	34
2.2. Přejít k virtuálním hodnotám	35
2.2.1. Virtuální peníze.....	36
2.2.2. Virtuální přátelství	37
2.3. Sporná otázka závislosti	38
2.4. Narušení sociálních vazeb	39
2.4.1. Případová studie: <i>Minnesota v. Melchert-Dinkel</i>	39
2.5. Právní definice osobnosti a její specifika v kyberprostoru.....	41
3. Formy ohrožení či zásahu do osobnostních práv nezletilého v kyberprostoru....	42
3.1. Zneužívání nezletilé osoby	42
3.2. Kyberšikana	46
3.2.1. Případová studie <i>U. S. v. Drew</i>	46
3.2.2. Případová studie: <i>New Jersey v. Ravi</i>	48
3.3. Zasahování do soukromí.....	51
3.3.1. Případová studie: <i>Catsouras v. DCHP</i>	52
3.4. Difamace.....	53
3.4.1. Zásah do pozitivní složky práva na informační sebeurčení nezletilé osoby - případová studie <i>Alexa Dell</i>	54
3.4.2. Zásah do negativní složky práva na informační sebeurčení nezletilé osoby při užívání výchovných prostředků v kyberprostoru	57
3.5. Dokazování v rodinném právu a Internet	59
4. Právní úprava ochrany nezletilých v kyberprostoru	61
4.1. Úvod: Sporné otázky právní regulace	61
4.1.1. Otázka kvalifikované ochrany osobnostních práv nezletilých osob.....	62
4.1.2. Subjektivní stránka újmy na osobnostních právech nezletilé osoby.....	64
4.1.3. Změna poměrů a otázka promlčení.....	66
4.2. Právní úprava ochrany osobnosti nezletilých v České republice	69
4.3. Právní úprava ochrany osobnosti nezletilých v EU.....	97
4.3.1. Platná právní úprava v EU	97
4.3.2. Návrh reformy právní ochrany uživatelů internetu v EU	100
4.3.3. Závěr	107
4.4. Právní úprava ochrany osobnosti nezletilých v USA.....	107

4.4.1. Vývoj a povaha amerického práva na ochranu osobnosti s důrazem na ochranu soukromí nezletilých v kyberprostoru	107
4.4.2. Právní rámec ochrany osobnosti nezletilých v kyberprostoru v USA	108
4.4.3. Závěr	113
5. Úvahy <i>de lege ferenda</i> : Výběr některých návrhů regulace ochrany osobnosti v kyberprostoru	114
5.1. Technické zneschopnění počítače	114
5.2. Model zeleného a červeného Internetu	115
5.3. Ověřování věku uživatele	116
5.4. Vzdělávání	116
5.5. Regulace sociálními normami	117
5.6. Ústava pro sociální síť	118
5.7. Úvaha autorky	119
5.7.1. Otázka uživatelského průkazu	120
6. Závěr	122
Summary	123
Seznam použité literatury	125
Abstrakt	141
Abstract	141
Klíčová slova / Keywords	143

Seznam použitých zkratek

OZ – Zákon č. 40/1964 Sb., Občanský zákoník

TZ - Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů

OSŘ – Zákon č. 99/1963 Sb., Občanský soudní řád

NZMPS - Zákon č. 91/2012 Sb., o mezinárodním právu soukromém

COPPA - Children's Online Privacy Protection Act of 1998

PSIS – poskytovatel služeb informační společnosti

PSISs – poskytovatelé služeb informační společnosti

SIS – služba informační společnosti

OSN – sociální síť (Online Social Network)

EFF- Electronic Frontier Foundation

FTC – Federal Trade Commission

ÚOOÚ – Úřad pro ochranu osobních údajů

Úvod

Díky rychlému rozvoji nových technologií tyto zásadním způsobem ovlivňují všechny oblasti veřejného i soukromého života člověka, od politiky přes ekonomiku až po lékařství, kulturu či budování sociálních vazeb. Vymahatelnost práva v kyberprostoru se však střetává s mnoha překážkami. Důvodem je především nesnadná aplikovatelnost klasických právních principů z „off-line¹ světa“, ať již pro relativní anonymitu uživatelů, častý mezinárodní prvek právních vztahů v kyberprostoru, virtuální povahu některých hodnot, jež mají být předmětem ochrany nebo nezachytitelnost internetových entit a volnost, s jakou se mohou rychle přemisťovat a měnit svou povahu v reálném čase. Je zřejmé, že aplikace obecné právní odpovědnosti známé z „off-line světa“ na on-line² prostředí není dost dobře možná bez zohlednění specifik internetu³, ale i jeho uživatelů, kde zvláště aktivními, a tedy i ohroženými jsou právě nezletilí.

Právní ochranou nezletilých uživatelů internetu se zabývá především trestní právo, na poli prevence, osvěty a omezené samoregulace jsou činné organizace ISP⁴ neboli PSIS⁵, ve spolupráci s veřejnou správou a výkonnými orgány veřejné moci. Pro tyto je však typická jistá neutříbenost⁶. V současné době neposkytuje plnohodnotnou ochranu nezletilým v kyberprostoru platná právní úprava česká, evropská ani právní regulace dnes nejvýznamnější velmoci na poli nových technologií - Spojených států amerických. V evropském právním prostředí zůstává nevyužit zejména občanskoprávní institut ochrany osobnosti.

Jedním z hlavních cílů této práce je poskytnout ucelený úvod do aktuální problematiky uživatelských aktivit nezletilých osob v kyberprostoru a přehled forem

¹ (ang.), mimo připojení/mimo internet, stav absence připojení, více Federal Standard 1037C (aktualizovaná verze *Telecom Glossary 2000*). Dostupný z WWW: <<http://www.its.bldrdoc.gov/projects/telecomglossary2000>>

² (ang.) v síti, indikuje stav připojení, více Federal Standard 1037C (aktualizovaná verze *Telecom Glossary 2000*). Dostupný z WWW: <<http://www.its.bldrdoc.gov/projects/telecomglossary2000>>

³ MAREŠ, D. 81280 K limitaci odpovědnosti providera v prostředí internetu – 1. část. *Epravo* [online]. 16.3 2012 [cit. 2012-12-11]. Dostupný z WWW: <<http://www.epravo.cz/top/clanky/k-limitaci-odpovednosti-providera-v-prostredi-internetu-1-cast-81280.html>>

⁴ Internet Service Provider neboli poskytovatel služeb internetu v oblasti ICT (ang. Information and Communication Technology, tedy informační a komunikační technologie). Příklady ISP: Seznam, Google, Facebook, Amazon.

⁵ Českým ekvivalentem označení a akronymu bude „poskytovatel služeb informační společnosti“ neboli (PSIS), pro plurál bude pro účely práce užito akronymu PSISs.

⁶ např. zaměření na nejmarkantnější aktivity naplňující často skutkovou podstatu trestného činu

jednání PSISs a třetích osob způsobilých ohrožení nebo zásahu do osobnostních práv těchto uživatelů. Tato práce se dále bude zabývat některými spornými otázkami v oblasti ochrany osobnosti nezletilých s ohledem na zvláštní požadavky na právní úpravu jednání v kyberprostoru, jako je otázka konkludentního souhlasu v kontextu nových technologií a služeb informační společnosti, otázka kvalifikované ochrany nezletilých, problém re-identifikace⁷ osobních údajů, sporná otázka přirozeného vývoje společnosti a posunu jejího vztahu k tradičním osobnostním hodnotám, obsahová jednota internetu bez ohledu na věk uživatelů anebo právní odpovědnost poskytovatelů služeb informační společnosti.

V této práci budou dále v rámci úvah *de lege ferenda* představeny a vyhodnoceny některé z úvah odborníků v oblasti práva na ochranu osobnosti a kybernetického práva, hledající nové alternativy pro vymezení právních prostředků ochrany soukromí a dalších osobnostních práv v kyberprostoru. Práce se také pokusí o výklad některých základních pojmů z oblasti práva informační společnosti relevantních pro dané téma, objasní vybrané trendy v užívání služeb informační společnosti nezletilými a to také za využití případových studií a příkladů z praxe, a to s cílem poskytnout nejen sumarizaci možných zásahů do osobnostních práv nezletilých v kyberprostoru ale také jejich důsledků.

Ve své práci by se autorka ráda dále zaměřila na specifika pojmu osobnost z jeho definice⁸ v kontextu aktuálního vývoje nezletilých v informační společnosti, a změn v přístupu nezletilých k ochraně soukromí, jejich znalosti internetu a jednání v kyberprostoru. Tato práce je zaměřena na nezletilé, kteří představují hlavní kupní sílu mnoha odvětví e-commerce⁹, jejíž přístup k osobnostním hodnotám, především k soukromí, je hodnocen velmi nejednotně, a to zejména s ohledem na skutečnost, že se jedná o první generaci, která vyrůstá v otevřené informační společnosti.

⁷ Tedy situace, kdy spojením s dalšími daty informace neumožňující identifikaci subjektu dat tuto identifikaci umožní a získává tak vlastnosti osobního údaje. Osobní údaje definuje ustanovení § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů jako jakékoli údaje týkající se určeného nebo určitého subjektu údajů. Pojmu indetifikovaných, identifikovatelných a nově re-identifikovatelných dat se zabývá také P. Schwartz a D. Solove.

⁸ Mimo jiné v českém občanském právu definice z rozhodnutí Nejvyššího soudu ČR ze dne 8. srpna 2007 č. 30 Cdo 2782/2007

⁹ (ang.), označení veškerých obchodních transakcí realizovaných za pomoci internetu a dalších elektronických prostředků. Zdroj: Adaptic, Praha, Česká republika [cit. 2012-09-18]. Dostupný z WWW: <<http://www.adaptic.cz/znalosti/slovnicek/e-commerce/>>

Jedním ze zásadních cílů této práce je najít odpověď na otázku, jakým způsobem lze v kyberprostoru nastavit právní rámec vymahatelnosti práva na ochranu osobnosti této skupiny, a to i s ohledem na tento mezioborový spor o to, jakou hodnotu nebo cenu nezletilí v současnosti tomuto právnímu nároku přiřkládají. Tato skupina je nejvíce formována, vzdělávána, ale také postižena vlivy kyberprostoru a informačních a komunikačních technologií (IKT)¹⁰.

Více než dvě miliardy uživatelů využívá pravidelně služeb Internetu¹¹ a tento počet je stále rozšiřován, poněvčas právě nezletilými dětmi stále mladšího věku. Právní jistotu nemají v současné době ani nezletilí ani plnoletí uživatelé internetu. Problematika s tímto stavem spojená patří k těm nejsložitějším a nejrozvrstvenějším v oblasti moderního práva.

Historický vývoj práva na ochranu osobnosti v kontextu kyberprostoru

Vývoj osobnostních práv v České republice, Evropské unie (přesněji v evropských zemích) a USA, byl podmíněn velmi odlišným historickým, kulturním, společenským, ale i technologickým vývojem. Na formování právní úpravy ochrany osobnosti v USA, zejména pak na hledání cesty k právu na soukromí, měly zásadní vliv filozofické, politické a právní koncepty odlišné od těch, které měly být dále rozvíjeny v Evropě. Jedním z nosných pilířů amerického práva se mimo jiné stal eminentní zájem společnosti na vytvoření právní pojistky, která by chránila jedince před postihem za veřejnou kritiku, zejména pak kritiku vlády. Až do současnosti zůstává v právní regulaci soukromí v USA znatelných několik, z pohledu evropského právního myšlení, ochranu ztěžujících, právních principů. Je to například absence ústavou přímo chráněného práva na soukromí. Toto právo bylo zakotveno především judikaturou např. ve věci *Wheaton v. Peters*¹², *Olmstead v. U.S.*¹³, *Roe v. Wade*¹⁴, *Eisenstadt v. Baird*¹⁵ nebo *Griswold v. Connecticut*¹⁶. Oproti Evropě jsou také odlišně regulována, či spíše neregulována,

¹⁰ (ang.) ICT (Information and Communication Technologies) pojem, který se v České republice uplatňuje velice často pro informatiku obecně

¹¹ Usage and Population Statistics. *Internet World Stats* [online] [cit. 2012-10-06]. Dostupný z WWW: <www.internetworldstats.com>

¹² *Wheaton v. Peters*, 33 U.S. 591, 634 (1834)

¹³ *Olmstead v. United States*, 277 U.S. 438 (1928)

¹⁴ *Roe v. Wade*, 410 U.S. 113 (1973)

¹⁵ *Eisenstadt v. Baird*, 405 U.S. 438 (1972)

¹⁶ *Griswold v. Connecticut*, 381 U.S. 479 (1965)

média ve svých zásazích do soukromí fyzických osob a zásadní důraz je kladen na ochranu osobnostních práv občana před zásahy státní moci. Co se důrazu na ochranu domova, jako zásadní nepřekročitelné hranice soukromí týče, americké pojetí se však evropskému přístupu do značné míry blíží. Tento pojem je stále jedním z nejzákladnějších co do regulace soukromé sféry občana, především však jako místo, kde vládní moc nesmí bezdůvodně zasáhnout, a proto se se změnou životního stylu obyvatel USA a rozvojem technologií, setkáváme v judikatuře s problematikou interpretace tohoto pojmu právě ve vztahu k těmto změnám. Ačkoli se v právní úpravě soukromí evropských zemí (a nejen těch) také setkáváme s důrazem na pojem domova, lze tvrdit, že role tohoto pojmu v americkém právu je srovnatelná s evropským historickým právním zájmem na zachování „dobré pověsti“ občana, na záruce vzájemného respektu a slušného jednání, který se odráží nejen v právu ústavním a dokonce trestním nebo pracovním, ale i v právu občanském. Shrnutí základního rozdílu ve formování a v přístupu k ochraně osobnosti v USA a v Evropě se věnuje Jamese Q. Whitman ve své práci „The Two Western Cultures of Privacy: Dignity versus Liberty“¹⁷, kde mimo ochrany anonymního projevu a dalších práv, shrnuje, že zatímco důstojnost je v Evropě přetrvávajícím zájmem hodným ochrany, v USA je tímto svoboda slova.

V Evropě se moderní právo ochrany osobnosti začalo rozvíjet v 17. století, vycházejí z osvícenství, rozvoje racionalismu a přirozenoprávní teorie¹⁸. Nově byl tedy tento právní nárok založen na principu rovných práv člověka a občana. Toto je zásadní rozdíl oproti předchozímu konceptu přiznávajícímu reputaci, ale také právo na domáhání se svých práv před soudem v návaznosti na společenskou třídu. Co se přijetí myšlenky rovných práv člověka a občana týče, šly ještě Spojené státy ruku v ruce s rozvinutou Evropou, protože patřily k jedněm z prvních, které ji přijaly, a tato se stala základním stavebním kamenem amerického práva, např. při tvorbě Deklarace nezávislosti. Komplexní právní úpravu ochrany osobnosti vycházející z potřeb nastalého stavu musely postupně přijmout všechny rozvinuté evropské státy. Prvenství

¹⁷ WHITMAS, James Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, *Yale Faculty Scholarship Series*, 2004, Vol. 113, No. 6. (2004) s. 1151. Dostupný také z WWW: <<http://www.yalelawjournal.org/pdf/113-6/WhitmanFINAL.pdf>>

¹⁸ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 41 ISBN 80-7201-484-6

v tomto směru neslo v Evropě Švýcarsko, které definovalo právo na soukromí v občanském zákoníku z roku 1907¹⁹.

Za první významnou odbornou práci zabývající se ochranou osobnosti a soukromí lze ve Spojených státech amerických považovat článek autorů Samuela Warrena a Louise D. Brandeise²⁰ „The Right to Privacy“²¹, který vyšel v *Harvard Law Review* v zimě roku 1890. Ve Spojených státech amerických se tak v 19. století, i přes důraz kladený na ochranu svobody projevu rozvinula diskuze o uznání práva na soukromí. Warren a Brandeis ve své práci vnesli významnou myšlenku, že není podstatné, jaká metoda vyjádření je pro komunikaci užita, tedy že ochrany by měl pojímat i prostý deníkový záznam nebo nevýznamný dopis. Právo na ochranu soukromí považovali za pouhý příklad obecnějšího zaručeného práva člověka nebýt rušen²², tedy být šetřen zásahů do své životní sféry bez svého souhlasu. Toto právo náležející osobnostním projevům, tedy znakům individuální mentální a duševní integrity, Warren a Brandeis staví na roveň právu na ochranu proti zásahu do tělesné integrity, jako je právo nebýt bezdůvodně uvězněn nebo podroben fyzickému útoku. Warren a Brandeis se také pokoušejí nastavit základní nepřekročitelnou hranici soukromí i pro osoby veřejně činné. „Zatímco některé skutečnosti lze považovat za soukromé pouze u osob, které se nerozhodli zastávat pozici takové povahy, která činí jejich činnost legitimní záležitostí veřejného šetření²³, některé skutečnosti je oprávněn chránit před módní lidovou zvědavostí každý bez rozdílu, bez ohledu na to, zda je jeho osoba součástí veřejného života či nikoli.“, píší ve svém článku.

Evropské prostředí bylo, během 20. století vystaveno četným tragédiím, v nichž hrálo setrvale významnou roli zneužívání osobních údajů a porušování práva na ochranu osobnosti totalitními režimy. To vedlo k poválečným iniciativám na mezinárodní i národní úrovni k revizi právních prostředků k ochraně osobnostních práv a jejich vymahatelnosti. Vzhledem k politické situaci v zemi nedocházelo v tomto směru

¹⁹ Více KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 44 ISBN 80-7201-484-6

²⁰ Louis D. Brandeis byl partnerem v advokátní kanceláři spolu se Samuelem Warrenem. Od roku 1916 působil jako ústavní soudce. Brandeis byl potomkem českých emigrantů, kteří odešli z Prahy po roce 1848.

²¹ WARREN, S. a BRANDEIS, Louis D. *The Right to Privacy. Harvard Law Review*. 1890, IV, 15. Dostupný také z WWW:

<http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.htm>

²² COOLEY, T.M.; *A Treatise on the Law of Torts* (2d ed. 1888). s. 29

²³ Nikoli ve smyslu procesního práva ale ve smyslu dělby veřejné moci, tedy jakéhosi dohledu občanů - veřejného zájmu či veřejné kontroly.

v Československu k zásadnímu rozvoji. Pro české právo má však význam občanský zákoník z roku 1964 a zejména jeho porevoluční novela č. 87/1990 Sb., zavádějící náhradu nemajetkové újmy v penězích, a dále pak rozvoj práva na soukromí a na ochranu osobních údajů související s pozdější implementací evropského práva.

Co se EU týče, významný posun legislativní snahy Komise směrem k aktualizaci regulace práva na soukromí²⁴ vzhledem k rozvoji uživatelských aktivit v kyberprostoru představovala významný posun Smlouva o fungování Evropské unie (SFEU), jejíž Článkem 16 zakládá právo každého na ochranu osobních údajů a respektování soukromého života. To znamená, že každý má právo na stejný standard ochrany, a to platí pro všechny subjekty zpracování dat. Ochrana dat je také zmíněna jako jedno ze základních práv v Článku 8 Listiny základních práv EU²⁵. Mimoto je EU smluvní stranou Úmluvy o ochraně lidských práv a základních svobod Rady Evropy²⁶, která také právo na soukromí ustavuje²⁷. Tato práce se blíže bude věnovat návrhu Komise na novou jednotnou právní úpravu ochrany osobních údajů uživatelů internetu (dále také jen jako Návrh Komise nebo Návrh), která by měla zásadním způsobem rozšířit ochranu poskytovanou směrnicí 95/46/EC, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále také jen jako Datová směrnice)²⁸. Dojde-li k přijetí Návrhu, bude mít tento zásadní význam pro právní záruky soukromí a ochrany osobních údajů, jak pro nezletilé tak zletilé uživatele a, jak lze doufat, také částečně postihne problematiku neexistující formální „globální jurisdikce“ a složité vymahatelnosti práv uživatelů ze zemí EU na subjektech ze třetích zemí, zejména USA. Vzhledem k dynamičnosti odvětví a prostředí, jehož se úprava týká, však Návrh bude muset v budoucnu dostat dalších změn. Vizi Viviane Reding, která prohlásila, že Návrh Komise představuje právní regulaci, která bude schopná beze změny platit po příštích třicet let²⁹ lze považovat za velice odvážnou.

²⁴ EU. Proposal for a Regulation of the European Parliament and of the Council COM(2012) 11 final, of 25.1 2012, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Dostupný také z:

<http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

²⁵ Srov. Listina základních práv EU (2007/C 303/01)

²⁶ Článek 8 Úmluvy zaručuje právo na respektování soukromého a rodinného života.

²⁷ KUNER, Ch.; The European Commission's Proposed Data protection Regulation“ A Copernical Revolution“ in European Data Protection Law. *Bloomberg Privacy and Security Law Report*. 2012, 11, PVLR 215. ISSN 1538-3431

²⁸ Postavení ochrany osobních údajů ve vztahu k ochraně osobnosti se bude autorka práce věnovat dále.

²⁹ WARMAR, M.; EU Privacy regulations subject to „unprecedented lobbying“ [online] *The Telegraph*. 8. únor 2012 [cit. 2012-07-12] Dostupný z WWW:

Jedním z důvodů, které do budoucna mohou způsobit zásadní problémy v obchodních vztazích v oblasti e-commerce mezi USA a Evropou, je právě rozdílný pohled na nároky právní ochrany soukromí uživatelů. Zatímco v Evropě je toto téma považováno za významnou agendu EU a zásadní zodpovědnost členských států, ve Spojených státech bylo donedávna soukromí uživatelů regulováno výrazněji trhem³⁰.

Z praktického aplikačního hlediska je ještě důležité připomenout podstatné specifikum evropských právních režimů, spočívající v tom, že tyto státy odděleně upravují ochranu osobních údajů a právo na soukromí, zatímco ve většině ostatních světových právních řádů jsou tyto upraveny jednotně. Ačkoli česká právní teorie podčleňuje osobní údaje pod soukromí, jejich ochrana spadá v praxi spíše do oblasti správního práva, zatímco ochrana soukromí do práva občanského. Je však myslitelné domáhat se nápravy zásahu do osobnostního práva závažným zásahem do osobních údajů občanskoprávní žalobou, stejně jako je souběžně možné tuto užít na některé extrémní formy zásahů do práva na ochranu osobnosti v kyberprostoru, naplňující skutkovou podstatu trestného činu.

Vymezení základních pojmů

Kyberprostor

Jedním ze základních problémů, se kterými se potýká česká právnícká literatura, je nejednotnost terminologie a chybějící jasné definice tak zásadních pojmů, jako je kyberprostor. Jedním z podstatných témat Kulatého stolu pro bezpečnější internet³¹ bylo právě připomenutí závažnosti této nejednotnosti³².

Jak uvádí Radim Polčák již ve své disertační práci z roku 2005, přesné vymezení pojmu kyberprostor není ani možné ani žádoucí.³³ R. Polčák ve své disertační práci kyberprostor definuje jako specifické a existenčně autonomní sociální prostředí

<<http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.htm>>

³⁰ SOLOVE, Daniel J., SCHWARTZ, Paul M.; *Information privacy law*. 4. vyd., Aspen Elective Series, Wolters Kluwer Law and Business, 2011. s. 1116. ISBN 0735510407

³¹ Ten byl u příležitosti Evropského týdne kybernetické bezpečnosti 2012 v České republice uspořádán Národním Centrem pro bezpečnější internet.

³² Jasná definice kyberprostoru by se měla objevit v novém Zákoně o kybernetické bezpečnosti.

³³ POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí*, Brno, 2006. 221 s. Doktorandská práce. Masarykova Univerzita, Právnická fakulta, Katedra obchodního práva. Vedoucí práce Petr Hajn. Dostupný také z WWW: <http://is.muni.cz/th/21177/pravf_d/disertacni_prace_-_text.pdf>

charakterizované mimo jiné i zvláštním étosem.³⁴ Je nutné připustit, že s postupujícím přesunem velké části aktivit lidské společnosti do prostředí kyberprostoru, se utváří jisté normy chování žádané praktickou nutností. Tyto lze dělit na obecné a zvláštní. Obecné se budou týkat běžného pohybu v kyberprostoru a běžného jednání, jako je např. komunikace maily nebo na chatu apod. Tento typ étosu však není, až na výjimky³⁵, široce obecně prosazován a často není dodržován. Jeho spektrum je také poměrně úzké. Zvláštní normy jsou pak typické pro zvláštní skupiny uživatelů, jako je např. komunita hráčů MMORPG³⁶. Zde jsou již normy chování výrazně propracovanější a komunitou je často dbáno na jejich dodržování zúčastněnými fyzickými osobami.

Jak dále říká Polčák, pojetí kyberprostoru jako technologicky determinovaného síťového informačního prostředí³⁷ je vytvořeno na základě praktických zkušeností s vývojem digitálních informačních sítí, jejichž prvky a uzly jsou osobní počítače. Polčák dále uvádí, že výraz internet není nutné vnímat jako synonymum pro pojmy kyberprostor či informační síť, ale jako výraz pro formu jejich aktuálního naplnění.³⁸ Z toho také vyplývá inklinace této práce právě k termínu kyberprostor. Jedná se o pojem širší než je internet a obsahově pod něj mohou tedy spadat také jiná komunikační rozhraní občanskoprávních vztahů, jejichž účastníky jsou poskytovatelé služeb informační společnosti a fyzické osoby – jejich uživatelé.

Dalším důvodem ke kladení důrazu na pojem kyberprostor v této práci je jeho historie. V roce 1984 byl tento pojem poprvé použit spisovatelem Williamem Gibsonem

³⁴ POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí*, Brno, 2006. 221 s. Doktorandská práce. Masarykova Univerzita, Právnická fakulta, Katedra obchodního práva. Vedoucí práce Petr Hajn. Dostupný také z WWW: <http://is.muni.cz/th/21177/pravf_d/disertacni_prace_-_text.pdf>

³⁵ STRAWBRIDGE, M., *Netiquette - Internet etiquette in the age of the blog*, Software Reference Ltd., 2006; *Business Know-how*, Five Rules of Twitter Etiquette, Dostupný z WWW: <<http://www.businessknowhow.com/internet/twitter-etiquette.htm>>

³⁶ MMORPG (ang. Massive(ly)-Multiplayer Online Role-Playing Game) je počítačová hra, (zpravidla, pozn. autorky) na hrdiny o více hráčích (tzv. Multiplayer), která umožňuje tisícům hráčů po celém světě být duchem v jeden čas a na jednom místě - ve zpravidla fiktivním virtuálním světě skrze Internet (a prostřednictvím alter-ega, které hráč sám vygeneruje, ovládá, a kterým komunikuje s dalšími hráči, ať již písemně nebo verbálně, pozn. autorky). Zdroj: <<http://www.mmorphry.estranky.cz/clanky/co-je-to-vubec-mmorpg-hra---.htm>>

³⁷ Jak o nich referuje MACEK, J.; POLČÁK, R.; ŠKOP, M.; *Normativní systémy v kyberprostoru* (úvod do studia). Brno: Masarykova univerzita v Brně, 2005, s. 5

³⁸ POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí*, Brno, 2006. 221 s. Doktorandská práce. Masarykova Univerzita, Právnická fakulta, Katedra obchodního práva. Vedoucí práce Petr Hajn. Dostupný také z WWW: <http://is.muni.cz/th/21177/pravf_d/disertacni_prace_-_text.pdf>

v jeho futuristickém románu „Neuromancer“.³⁹ V jeho definici lze postřehnout nejen základ pozdější skutečné reality kyberprostoru, což je globálnost tohoto prostředí a jeho vliv na rozvoj technologií, ale také zásadní fakt, že ústředním prvkem tohoto prostředí je člověk, tedy jeho podstata redukována na jeho osobnost a osobnostní projevy realizované přeneseně prostřednictvím technologie. Podle Václava Jirkovského z ČVUT má kyberprostor několik základních znaků, jako je jeho globálnost, necentralizovanost, otevřenost, řízenost pouze uživateli nebo interaktivnost. Komunikace v prostředí kyberprostoru se dále podle něj vyznačují pocitem bezpečí a intimitu⁴⁰. To je způsobeno podle autorky této práce jednak anonymitou uživatelů, technologickým zprostředkováním komunikací, neexistujícím přímým kontaktem (pohledem, často chybějící možnosti sledování nonverbálních projevů komunikátora), ale také vědomím nízké možnosti legislativní kontroly tohoto prostoru. Právě tento pocit však stál na počátku problematiky porušování práv v kyberprostoru. Nejzásadněji se pak projevil v oblasti porušování osobnostních práv nezletilých.

Informační sebeurčení

Jak odborná literatura, tak judikatura⁴¹ uvádějí právo na informační sebeurčení v kontextu práva na ochranu osobnosti jako jeho rozšířenou povahu judikovanou také Evropským soudem pro lidská práva v podobě interpretace Čl. 8 odst. 1 Úmluvy o ochraně lidských práv a základních svobod v tom smyslu, že respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Tuto myšlenku lze argumentačně užít pro požadavek ochrany pozitivní (aktivní) složky osobnostních práv nezletilé osoby, kterou se tato práce bude podrobněji zabývat dále.

³⁹ „Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky (...) Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyšlitelná komplexnost. Linie světla seřazené v neprostoru myslí, shluky a souhvězdí dat. Jako světla města, (...)“ Zdroj: GIBSON, W. *Neuromancer*. New York: Ace Books, 1984. s. 69. ISBN 0-441-56956-0

⁴⁰ JIROVSKÝ, V.; *Společnost ve virtuálním světě* [online prezentace]. 2010 [cit. 2012-12-19]. Dostupný z WWW: <<http://www.slideshare.net/TUESDAY/jirovsky-tisk-3735598>>

⁴¹ Nález Ústavního soudu ze dne 1. března 2000 sp.zn. II ÚS 517/99

Jak vyplývá z odborné literatury⁴², právo na ochranu osobního soukromí lze vymezit jako právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupňovány jiným (pozitivní složka práva) a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob s rovným právním postavením (negativní složka práva). Pojem práva na informační sebeurčení je tak principem osobnostních práv jako kontroly nad okruhem osob, se kterými svá soukromá data/informace subjekt sdílí nebo, se kterými jsou tato sdílena.⁴³ Díky tomuto výkladu je možné považovat za porušení práva na soukromí také rozšiřování informace, kterou subjekt s určitou skupinou osob již sdílel. Představitelná, a právní teorií popsaná, je situace, kdy subjekt sdílí informaci se skupinou osob s předpokladem uchování její důvěrnosti, a to v závislosti na povaze informace, okolnostech sdílení a dále v závislosti na principu důvěry, ne pouze profesní, jakou nalézáme např. pro lékaře nebo advokáty, ale obecné, předpokládané a konkludentně přijaté vzhledem ke kontextu informace. Zjednodušeně řešeno, např. i informaci, o které se od samotného subjektu dozvěděl okruh např. třiceti osob, lze stále vnímat jako soukromou, a její další šíření za nezákonné, a to i přes relativně vysoký počet osob, kterým byla sdělena. V tomto smyslu poskytuje z oblasti amerického práva zajímavou definici soukromí rozhodnutí kalifornského odvolacího soudu ve věci *M.G. v. Time Warner, Inc.*⁴⁴ z roku 2001, ve kterém právo na soukromí není definováno prostřednictvím povahy skutečností, které lze považovat za soukromé resp. intimní, ale jako právo na kontrolu.⁴⁵ Například pokud osoba sdělí terapeutické skupině pro osoby nakažené virem HIV o 20ti lidech, že je nositelem viru, z povahy skupiny a informace vyplývá, že se stále jedná o informaci soukromou, spadající dokonce do jeho intimní sféry.

⁴² Srov. KNAP, K.; ŠVESTKA, J.; Jehlička, O.; Pavlík, P.; Plecítý, V.: *Ochrana osobnosti*. 3. vydání. Praha: Linde, 1996, s. 288. Zdroj: K právu na soukromí a rodinný život (II. ÚS 517/99). *Soudní rozhledy: Z aktuálních nálezů Ústavního soudu*. 3/2000

⁴³ Více v nálezů Ústavního soudu č. I. ÚS 453/03 ze dne 11. II. 2005 a nálezů Ústavního soudu č. IV. ÚS 23/2005 ze dne 17. 7. 2007

⁴⁴ *M.G. v. Time Warner, Inc.* 89 Cal. App. 4th 623, 632 (Cal. Ct. App. 2001)

⁴⁵ Právo na soukromí je právem definovat intimní okruh osob, se kterými bude osoba soukromé informace sdílet. Informace, která je sdělena několika osobám, je stále informací soukromou. Zdroj: *M.G. v. Time Warner, Inc.*, 89 Cal. App. 4th 623, 632 (Cal. Ct. App. 2001)

Dítě

Pro účely této práce vychází autorka zejména z definice dítěte z Čl. 1 Úmluvy o právech dítěte, podle které se dítětem rozumí každá lidská bytost mladší 18ti let. Úmluva o právech dítěte však říká, že „dítě znamená kterákoli lidská bytost mladší 18ti let, pokud podle práva, které se na dítě vztahuje, není plnoletost určena dříve.“, v SRN je tak ale např. dítě z právního hlediska pouze osob mladší 14ti let. Podle výsledků mezinárodní analýzy právní úpravy soukromí a ochrany osobních údajů, kterou provedla advokátní kancelář Baker & McKenzie, lze usuzovat, že vzhledem k tomu, že nezletilému dítěti staršímu 15 let je podle OZ za určitých okolností udělována způsobilost k některým závažným právním úkonům, jako je například pořízení poslední vůle, rodič nebo zákonný zástupce má kontrolu nad aktivitami nezletilého v kyberprostoru teoreticky pouze do dovršení 15 roku. Mnoho PSISs poskytujících služby ve značné míře nezletilým, nastavilo minimální uživatelskou věkovou hranici. Tato však často i vůči evropským uživatelům vychází z hranice, kterou původně nastavil americký federální zákon na ochranu soukromí dětí na internetu - Children's Online Privacy Protection Act (COPPA). Motivem PSISs pro univerzální zákaz užívání osobám mladším 13ti let je snaha vyhnout se právní odpovědnosti za sběr osobních údajů pro komerční účely o osobách mladších 13ti let bez souhlasu zákonného zástupce, jak právě COPPA zakazuje. Autorka této práce se domnívá, že by tento, sám o sobě stále spíše mírný důraz na ochranu nezletilých před behaviorálním marketingem měl být rozšířen na subjekt „dítěte“ jak jej jasně definuje Návrh Komise obecně, tedy osobu mladší 18 let.

Důvodem spornosti dosavadní samoregulační hranice 13ti let je skutečnost, že právě období mezi 13 – 18 rokem je dobou, kdy je nezletilý technologicky nejaktivnější, nejcitlivější co se sociálního statutu a svobodného osobnostního sebeurčení týče, a kdy je zároveň pod největším tlakem jak k dosažení obecně uznávaného sociálního obrazu, tak pod tlakem vrstevníků, kteří právě v tomto věku nejčastěji mohou užívat technologií a internetu pro kyberšikanu, difamaci a pronásledování, ale také podnikají amatérské data-miningové aktivity, to znamená, že vyhledávají informace o svých vrstevnících, spolužácích a jejich rodinách i učitelích na internetu, a s těmito dále pracují, někdy za účelem výše uvedené šikany nebo vydírání spolužáků. Častý je pro tyto také zásah do soukromí pořizováním foto a video záznamů, které jsou následně vloženy na internet, bez souhlasu subjektu. Podrobněji se pojmem nezletilého coby uživatele služeb

informační společnosti a jeho způsobilosti být smluvní stranou autorka zabývá dále v této práci.

Z Čl. 3 Úmluvy o právech dítěte vyplývá, že zájem dítěte musí být předním hlediskem při jakékoli činnosti týkající se dětí, ať už uskutečňované veřejnými nebo soukromými zařízeními sociální péče, soudy nebo, správními nebo zákonodárnými orgány. Toto je podstatné jak pro rozhodování soudů při složitém vyvažování proti sobě stojících základních práv, tak pro tvorbu případné nové legislativy poskytující nezletilým možnost efektivně se domáhat právní ochrany před zásahy do jejich osobnostních práv v kyberprostoru. Dále v této práci však také autorka předloží alternativní argumentaci pro vytvoření pouze taxativně vymezeného spektra prostředů kvalifikované právní ochrany nezletilých, kteří jsou v dnešní době vybaveni rozsáhlými znalostmi z oblasti informatiky, kterými nezdědka překonávají průměrného zletilého uživatele.

Na tomto místě lze pouze shrnout, že dítě je v kontextu ochrany osobnosti v kyberprostoru potřeba vnímat jako postmoderní osobnost vyvíjející se již zcela v informační společnosti, a v tomto smyslu vybavenou jedinečnými znaky oproti generaci předchozí.

Informační společnost

Informační společnost je charakterizována rozsáhlým využíváním digitálního zpracovávání, uchovávání a přenosu informací. Ze zpracovávání informací se stává významná ekonomická aktivita, která jednak prostupuje tradičními ekonomickými či společenskými aktivitami a jednak vytváří zcela nové příležitosti a činnosti, které podstatně ovlivňují charakter společnosti.⁴⁶ Termín "informační společnost" má zdůraznit fakt, že vedle technických otázek zde musí být řešeny i důležité otázky z oblasti etiky, morálky, politiky, práva apod., obecně celé široké spektrum možných dopadů na lidskou společnost.^{47, 48}

⁴⁶ ZLATUŠKA, J.; Informační společnost. *Zpravodaj ÚVT MU*. 1998, roč. VIII, č. 4, s. 1-6. ISSN 1212-0901 Dostupný také z WWW: <<http://www.ics.muni.cz/bulletin/articles/122.html>>

⁴⁷ PETERKA, J.; *Slovník Jiřího Peterky* [online]. Praha [cit. 2012-08-24]. Dostupný z WWW: <<http://www.earchiv.cz>>

⁴⁸ JANÁK, M.; Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu. online]. *IT Právo*, 2009 [cit. 2012-11-19]. Dostupný z WWW: <[http://www.itpravo.cz/index.shtm?l?AA_SL_Session=8bab7c81254d3179ff720eb355e677c0&sh_itm=556af04eed0edd7e3a87506bec5481a0&sel_ids=1&ids\[xd78ee7f117f5f1dd84e8898647203834\]=1#disc](http://www.itpravo.cz/index.shtm?l?AA_SL_Session=8bab7c81254d3179ff720eb355e677c0&sh_itm=556af04eed0edd7e3a87506bec5481a0&sel_ids=1&ids[xd78ee7f117f5f1dd84e8898647203834]=1#disc)>

Služba informační společnosti

Pojem služby informační společnosti se objevuje ve směrnici Evropského parlamentu a Rady 2001/31/ES⁴⁹ o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, a podle této směrnice jde o služby poskytované zpravidla za úplat, na dálku, prostřednictvím elektronického zařízení pro zpracování a ukládání dat a na individuální žádost příjemce služby. Taková služba např. zahrnuje on-line prodej zboží, poskytování služeb vyhledávačů a přístupu k datům, přenos informací po síti, poskytování připojení k síti, ukládání informací atd. Službou informační společnosti se dále rozumí jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky.

Data

K obecně známé povaze dat je pro účely této práce namísto doplnit definici, kterou přinesl Jason Schultz z právnické fakulty kalifornské univerzity Berkeley, tedy, že „Informace je zároveň ekonomickou komoditou a základem pro přístup k lidskému vědění, budování demokracie a prosazování vývoje společnosti.“⁵⁰

Poskytovatel služeb informační společnosti

Služby informační společnosti lze rozdělit do několika kategorií. Pro potřeby této práce budou definovány pouze skupiny poskytovatelů služeb informační společnosti (dále také jen jako PSISs), kteří jsou poskytovateli volného prostoru, neboli webhostingových služeb nebo provozovateli kybernetických „platform“, jak je podle Electronic Frontier Foundation (EFF)⁵¹ označována většina PSISs, poskytujících a spravujících především sociální sítě. PSISs se tato práce bude zabývat okrajově ve vztahu ke správě a zpracování osobních údajů jako typické činnosti cloud

⁴⁹ Konkrétně ustanovení čl. 2 písm. a)

⁵⁰ SCHULTZ, J., *Profil vyučujícího* [online], UC Berkeley School of Law [cit. 2012-06-18] Dostupný z: <<http://www.ischool.berkeley.edu/people/faculty/jasonschultz>>

⁵¹ Electronic Frontier Foundation (EFF): Free Speech is Only as Strong as the Weakest Link [online] [cit. 2012-10-08]. Dostupný z WWW: <<https://www.eff.org/free-speech-weak-link>>

computingu⁵² a dále v části věnované otázce právní odpovědnosti PSIS za zásah do osobnostních práv subjektu, ať již vlastním jednáním nebo třetí osobou.

Poskytovatel volného prostoru

„Poskytovatelem volného prostoru (hosting providerem) se rozumí právnická nebo fyzická osoba, která na základě smlouvy poskytuje na Internetu datový prostor jiným subjektům a tak zpřístupňuje cizí obsah prostřednictvím počítačové sítě Internet, případně poskytuje další služby s tím spojené. (...) Volným prostorem se pak rozumí datový prostor na Internetu, kde může být na základě smlouvy tento obsah zpřístupněn.“⁵³ Nejčastěji tak v praxi půjde o prostor pro tvorbu stránek uživatelů⁵⁴.

Kybernetické platformy

„Druhou skupinou (...) tvoří například poskytovatelé veřejných emailových adres, poskytovatelé SMS bran, poskytovatelé komunikačních programů na bázi ICQ, Skype, atp. Do jisté míry zde budou zahrnuti i poskytovatelé internetových stránek zprostředkující přenos určitých informací poskytnutých uživatelem dále. Typicky tedy půjde o různé online formuláře, popřípadě privátní diskusní zprávy, které jsou dále přeposílány.“⁵⁵ Podobně, jako obsah vytvořený klientem poskytovatele volného prostoru webovými stránkami nespadá takovýto obsah potenciálně závadné povahy, který na těchto stránkách dále vytvoří jiný uživatel či návštěvník stránek klienta, *per se* do právní odpovědnosti poskytovatele kybernetické platformy. V obou případech se jedná o tzv. „cizí obsah“, jehož výklad předkládá článek Martina Janáka v článku „Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu“ takto: „Za cizí obsah je v tomto smyslu třeba považovat elektronická data sítě Internet, náležící jinému subjektu než poskytovateli volného prostoru, která lze přenášet

⁵² (Označení pro) využití externích služeb pro uchování a správu elektronických dat mimo subjekt, jemuž data patří nebo který s nimi na základě určitého právního důvodu nakládá. Zdroj: CÍSAŘOVÁ, Z.; *Elektronická data a cloud computing z pohledu autorského práva a ochrany osobních údajů*. Univerzita Karlova v Praze, Právnická fakulta (2012), s. 32

⁵³ MATEJKA, J.; ČERMÁK, J; Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah [online] *ITPrávo*. 2001 [cit. 2012-09-23]. Dostupný z WWW: <<http://www.itpravo.cz/index.shtm?x=48792>>

⁵⁴ Pro téma této práce zejména blogů, humoristických stránek nebo amatérského bulváru.

⁵⁵ JANÁK, M., Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu [online] *IT Právo*. 2009 [cit. 2012-11-19]. Dostupný z WWW: <http://www.itpravo.cz/index.shtm?l?AA_SL_Session=8bab7c81254d3179ff720eb355e677c0&sh_itm=556af04eed0e>

prostředky pro elektronickou komunikaci a v některých případech též uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou (jde např. o webové stránky ve formátu HTML, formátovaný text z libovolného textového editoru, fotografie, hudbu, animace a zvuky, apod.).⁵⁶ Jak ale bude osvětleno v části této práce věnované právní odpovědnosti PSISs, v některých případech zvláštní zákon⁵⁷ dovozuje právní odpovědnost také PSIS – poskytovatele kybernetické platformy za tzv. cizí obsah.

K dalším podstatným pojmům, které je pro účely této práce nezbytné osvětlit patří pojem **správce osobních údajů**, kterým je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Za správce osobních údajů jsou např. považováni provozovatelé sociálních sítí.⁵⁸ Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.⁵⁹ Dále pojem **zpracovatel** osobních údajů, kterým je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.⁶⁰ a pojem **příjemce**, kterým je každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).⁶¹ Dále je potřeba připomenout zákonnou definici souhlasu se zpracováním osobních údajů, který je v ustanovení § 4 zákona o ochraně osobních údajů označován jako „souhlas subjektu údajů“, tedy, rozumějme uživatele, fyzické osoby, jejíž osobní údaje jsou v kyberprostoru zpracovávány, a který je svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů⁶².

⁵⁶ MATEJKA, J.; ČERMÁK, J.; Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah [online]. *ITPrávo*. 2001 [cit. 2012-09-23]. Dostupný z WWW:<<http://www.itpravo.cz/index.shtm?x=48792>>

⁵⁷ Srov. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

⁵⁸ Pracovní skupina pro ochranu údajů zřízená podle článku 29; *Stanovisko č. 5/2009 k internetovým sociálním sítím*. 12. červen 2009

⁵⁹ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. § 4 j

⁶⁰ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. § 4 k

⁶¹ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů., § 4 o

⁶² Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. § 4 n

1. Ochrana osobnosti a kyberprostor: některé z běžných služeb způsobilých ohrožení či zásahu do osobnostních práv uživatele

1.1. Web 2.0: Sdílení uživatelských dat v kyberprostoru

Pojem Web 2.0 označuje přelomové období v historii internetu, revoluci v přístupu uživatelů k internetu jako takovému. Celý přechod lze zjednodušeně popsat, jako odklon od původního záměru internetu, který měl být sítí propojených uložišť, která by zejména poskytovala neustále dostupné informace, které by doplňovali, kontrolovali a prověřovali správci. Uživatelé však po čase přestali vnímat internet jako jednostranné médium a vznikl velký tlak jejich zájmu podílet se na jeho obsahu interaktivně a v reálném čase. To vedlo k přerodu internetu do podoby Webu 2.0, který se datuje do roku 2004. Lze tvrdit, že nyní se nacházíme v rokokové fázi Webu 2.0, neboť interaktivní internet je tvořen z velké části právě uživateli a hlavním cílem užívání internetu generace nezletilých již není čerpat informace, ale komunikovat, a především sdílet, vkládat, doplňovat a tvořit. Uživatelský obsah⁶³ přibývá na internetu mimořádným tempem. Tato skutečnost je jedním z hlavních liberačních argumentů PSISs: i pokud by měli některé skupiny PSISs právní odpovědnost za obsah platform, mohou pro toto množství dat jen těžko fakticky jejich obsah kontrolovat. Je tedy iluzí se domnívat, že internet je pod kontrolou nebo, že je, v současné podobě zcela kontrolovatelný. Jak řekl Laurence Lessig: „Kyberprostor je nevyhnutelný a přece neregulovatelný. Žádný národ bez něj nemůže žít, a přece, žádný národ nebude nikdy schopen kontrolovat chování v něm.“⁶⁴ Toto tvrzení experta na právo IP a technologií může působit poněkud fatalisticky, a je navíc jistě ovlivněno jeho liberálními postoji a cíleno je tak spíše proti snahám jednotlivých států o kontrolu prostoru poskytujícího teoreticky absolutní osobní, společenskou a politickou svobodu občanům, je ale také nezbytným výchozím bodem pro jakékoli úvahy o možné právní regulaci kyberprostoru v demokratické společnosti.

Na tomto místě práce budou představeny nejběžnější služby Webu 2.0, které nezletilí využívají, a právní problematika s nimi spojená. Jedná se např. o blogy, tedy internetové deníky, na které uživatel umísťuje především články a komentáře, ale také

⁶³ často užíván ang. termín User Generated Content (UGC)

⁶⁴ LESSIG, L.; *The Laws of Cyberspace* [prezentace na konferenci, video] *Taiwan Net '98*, 1998.

např. fotografie, videa a hypertextové odkazy⁶⁵. Právní problematika blogu spočívá nejen v povaze blogu, který poskytuje velký prostor pro difamací, ale dále v možnosti jeho tvorby anonymně, a faktu, že každý příspěvek může být kterýmkoli čtenářem v diskuzi anonymně komentován. Nejčastěji jsou to právě tzv. vlákna diskuzí, kde se difamační obsah objevuje.

Další službou jsou sociální sítě, kterým se budeme věnovat více dále v této práci. Rozeznáváme sociální sítě obecné a se zvláštním zaměřením. Nejznámější světovou sociální sítí je v současné době Facebook. Sociální síť představuje interaktivní komunikační informační servis ze života uživatele kombinovaný v posledních letech s prvky zpravodajství, reklamního katalogu, plánovače, e-mailu, lokalizátoru, nebo také např. herní platformy. Cílem uživatele sociální sítě je zůstat v kontaktu s okolím. Informovat o svém životě a být informován o životě druhých. Sociální sítě představují ideální platformu, na které může docházet k mnoha formám zásahů do osobnostních práv nezletilých, od zneužívání nezletilého, přes kyberšikanu až po pronásledování nebo difamací.

Podobná nebezpečí, ačkoli nikoli v takovém rozsahu, skýtají veřejná uložení médií, jako jsou fotografie – např. Flickr nebo Instagram. Nebezpečí těchto uložení spočívá v možnosti „re-identifikace“ „de-identifikované“ informace z kontextu ostatních dostupných dat v kyberprostoru. Např. pokud zašle uživatelka pouze fotografii ze svého obývacího pokoje, nezveřejňuje příliš, ale pokud její přítelkyně/kontakt zašle ještě další fotografie, ze kterých je evidentní umístění domu, kde dívka bydlí, např. podle známých staveb v okolí, bude uživatelka vystavena nebezpečí. Mimoto fotografie některých služeb mohou obsahovat jako metadata⁶⁶ přesné geolokační údaje o pořízené fotografii, která jsou prohlížečím přístupná.

Podobně lze upozornit na platformy pro sdílení videí, jako je YouTube nebo Vimeo. Tyto jsou velice oblíbené mezi nezletilými, mimo jiné protože jim umožňují umělecké sebevyjádření. Nezřídka se však na službách video sdílení objevuje závadný obsah např. násilného charakteru. Jsou zde umístěny také videozáznamy šikany. Je častým jevem, že nezletilý umístí na takovou platformu video, kterým se chce svěřit

⁶⁵ Část interaktivního textu, po jehož zakliknutí je čtenář přesměrován na jinou stránku se souvisejícím obsahem.

⁶⁶ Informace neoddělitelně spjatá se souborem, resp. data o datech, zde GPS údaje o přesném místě a čase pořízení fotografie.

anonymním diváků s osobním problémem v naději na podporu. Protože tato videa mohou opět ve vláknu komentovat i zcela neznámí uživatelé užívající přezdívky, obsah komentářů bývá často útočný, nenávistný a vulgární. Objevují se i výhrůžky, nadávky s rasistickým, sexistickým nebo homofobním podtextem anebo obscénní reakce. Takové texty mohou mít zcela devastující účinky na dítě, a představují zásadní zásah do jeho osobnostních práv. Další zásadní nebezpečí skýtají služby online video projekcí nebo video hovorů orientované na komunikaci uživatelů, jako je Skype nebo BlogTV. Uživatel si často neuvědomuje, že ačkoli se z videopřenosu nepořizuje záznam, uživatel může pořídit bez vědomí druhého komunikátora fotografický záznam toho, co vidí, a to přímo v počítači. Tímto pak může být uživatel vydírán. Jedná se tak často o případy, kdy neznámá osoba vybízí nezletilou osobu, aby se obnažila, a z tohoto posléze pořídí fotografii, kterou dítě vydírá. Na výše jmenované BlogTV bylo takto jedním uživatelem vydíráno více než 100 dětí, které posléze v některých případech tento uživatel pohlavně zneužil⁶⁷. Platforma BlogTV byla také zneužita mužem, který na základě nevědomě pořízeného záznamu později dlouhodobě pronásledoval a vydíral nezletilou Kanadanku Amandu Todd, která pod vlivem tohoto nátlaku v 16 letech spáchala sebevraždu. Ke zveřejnění informací o incidentu a jeho závažných několikaletých destruktivních následcích na svou psychiku a život použila dívka předtím, než spáchala sebevraždu, video platformu YouTube.

Další službou potenciálně způsobilou zásahu do osobnostních práv nezletilého jsou internetové seznamky. Charakterem je lze přirovnat k sociálním sítím, problematické jsou však zejména z toho důvodů, že ze své povahy vybízejí nezletilé ke kontaktování neznámých osob a ke sdílení intimních údajů. Nezletilí navíc nezřídka experimentují se sexuálně explicitními vzkazy pro ostatní uživatele nebo s pořizováním a vykládáním či zasíláním vlastních eroticky laděných fotografií⁶⁸.

Také pro tyto služby platí, že jakýkoli obsah je anonymně kopírovatelný. Mírnější variantou zásahu je, pokud např. fotografie budou použity bez uvedení jména nebo přezdívky nezletilého na stránkách shromažďující trapné snímky neznámých osob pro pobavení veřejnosti, v horším případě se může opakovat výše uvedený scénář

⁶⁷ MORRIS, K.; BlogTV and the sad, avoidable path to Amanda Todd's suicide. *The Daily Dot* [online] 15. říjen 2012 [2012-12-27] Dostupný z WWW: <<http://www.dailymdot.com/news/blogtv-amanda-todd-suicide/>>

⁶⁸ Více viz. dále v této práci a také dokument Seznam se bezpečně]. *Seznam.cz* [cit. 2012-10-18]. Dostupný také z WWW: <<http://www.youtube.com/watch?v=9bDFe5as5HA>>

odhalení, vydírání, zneužití. Ačkoli PSISs provozující seznamky mají snahu jejich obsah regulovat, tato místa zůstávají stále rizikovými oblastmi internetu. Mohou také mít negativní vliv na hodnotový růst nezletilého dítěte. Mimo seznamky určené pouze pro osoby určitého náboženství či rasy, existuje také úspěšná mezinárodní seznamka pouze pro krásné osoby⁶⁹. Pokud se na posledně jmenovanou seznamku Beautiful People nezletilý přihlásí, bude jeho fotografie kolovat mezi již „přijatými“ uživateli a ti na čtyřstupňové škále vyhodnotí krásu osoby. Pouze pokud bude uchazeč shledán atraktivním, smí se do seznamky připojit. Dalším, z hlediska osobnostních práv lépe postižitelným, problémem této stránky je možnost dalšího nakládání provozovatele s fotografiemi odmítnutých uchazečů.

V souvislosti s osobními údaji lze krátce zmínit také rizika vyhledavačů, které sbírají, spolu s dalšími PSISs data uživatele, se kterými je dále nakládáno. Do soukromí nezletilého dítěte může zasahovat také behaviorální marketing⁷⁰ a obdobné obchodní praktiky.

Další potenciálně ohrožující službou jsou herní platformy, které mohou v některých případech zasahovat do práva nezletilého na rodinný život. Více se tímto tématem bude práce zabývat v kapitole věnované otázce závislosti na službách informační společnosti.

Nebezpečná jsou také chatová fóra a podobné komunikační platformy. Tyto sice mohou pomoci nezletilé osobě ve složité životní situaci, a to anonymní komunikací s lidmi s podobným problémem a jejich prospěšnost je nepopiratelná v podpoře nezletilých osob vyrovnávajících se např. se svou sexuální orientací, rodinnými spory nebo šikanou, skupiny mohou ale také podporovat negativní jevy, jako je sebepoškozování, poruchy příjmu potravy, organizované násilí, užívání drog nebo prostituce. Také pro nezletilé se zájmem o tato témata existují dostupné komunikační skupiny, kde mohou anonymně a bez kontroly získat veškeré potřebné informace a nebezpečné kontakty.

⁶⁹ Srov. stránky seznamky BeautifulPeople.com, Dostupný z WWW: <<http://www.beautifulpeople.com/en-CZ>>

⁷⁰ Behaviorální targeting / advertising, tedy online behaviorální reklama (také známa jako zájmově orientovaná reklama) je způsob zobrazování reklamy na navštívených internetových stránkách tak, aby reklama více odpovídala zájmům uživatelů a byla tak pro ně relevantní a vhodná. Zájmy jsou založeny na předchozí internetové aktivitě (návštěvnosti). Zdroj: Your online choices: Průvodce on-line behaviorální reklamou. Dostupný z WWW: <<http://www.youronlinechoices.com/cz/o-behavioralnim-cileni-reklamy>>

1.2. Anonymita služeb na Internetu

Informace o hrozbě anonymní komunikace na internetu byly zpochybnovány, zejména argumentem, že anonymita na internetu neexistuje. Standardní anonymita je skutečně relativní – podle IP adresy⁷¹ počítače, lze dohledat, na koho je na síti registrován. Fakt, že počítač je na určitou osobu zapsán, však neznamená, že tato komunikaci vykonala. Pokud je počítač užíván celou rodinou, v kanceláři nebo dokonce v internetové kavárně, může být komunikátora velmi obtížné dohledat. PSIS je navíc data o uživateli povinen ve valné většině případů poskytnout pouze pro potřeby trestního, nikoli občanskoprávního řízení⁷². Úspěch identifikace uživatele lze zvrátit také s užitím technologií. Osoby, které chtějí své příspěvky zasílat skutečně anonymně, mohou využít proxy servery jako je WiTopia, Cryptohippie nebo Identity Cloaker, aby tak utajili IP adresu svého počítače⁷³. Ačkoli tyto metody měly za cíl zaručit každému možnost svobodně se vyjádřit bez hrozby negativních následků, především vládního postihu, tyto služby mohou být využity pro veškeré negativní aktivity na internetu, přes komunikaci týkající se trestné činnosti, či anonymní nedohledatelnou kyberšikanu až po kybergrooming.⁷⁴

Nebezpečí téměř nekontrolovatelné anonymity na internetu jsou si vědomi také zástupci PSISs. Randi Zuckerberg, bývalá ředitelka marketingu společnosti Facebook řekla, že anonymita musí z Facebooku zmizet⁷⁵. Tento svůj názor také systematicky mediálně prosazovala, a to právě s motivací ochrany dětí na internetu. Bývalý generální ředitel společnosti Google zase nazval anonymitu na internetu nebezpečnou⁷⁶. Přístup

⁷¹ Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. IP adresa je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol). Zdroj: Wikipedia contributors; IP adresa [online] *Wikipedia, The Free Encyclopedia* [cit. 2013-02-12]. Dostupný z WWW:

<http://cs.wikipedia.org/wiki/Speci%C3%A1ln%C3%AD:Co_odkazuje_na/IP_adresa>

⁷² C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, více dále v této práci.

⁷³ ROUNDS, B.; How to Make Anonymous Comments on a Website [online]. *How to Vanish*, 2. leden 2011 [cit. 2012-11-05]. Dostupný z WWW: <<http://www.howtovanish.com/2011/01/how-to-make-anonymous-comments-on-a-website/>>

⁷⁴ Falešné IP adresy jsou také užívány při porušování autorských práv pro odběr obsahu, který pro region uživatele není licencován.

⁷⁵ BOSKER, B.; Facebook's Randi Zuckerberg: Anonymity Online Has to Go Away [online] *Huffington Post* 26. září 2011 [cit. 2012-12-11]. Dostupný z WWW:

<http://www.huffingtonpost.com/2011/07/27/randi-zuckerberg-anonymity-online_n_910892.html>

⁷⁶ KIRKPATRICK, M.; Google, Privacy and the Explosion of New Data [online] *Techonomy* 4. srpen 2010 [cit. 2012-08-09]. Dostupný z WWW: <<http://techonomy.typepad.com/blog/2010/08/google-privacy-and-the-new-explosion-of-data.html>>

PSISs k anonymitě na internetu je do velké míry podobný jako přístup k nedovolenému komerčnímu sběru informací od osob mladších 13 let, za který hrozí v USA komerčnímu PSIS právní postih. Než aby museli provozovatelé stránek převzít odpovědnost za nesnadnou kontrolu věku uživatelů, často obcházejí požadavek kontroly zákazem používat službu osobám mladším 13ti let. Problematika anonymity v kyberprostoru je citlivým tématem vzhledem k funkci tohoto prostoru jako svobodné otevřené platformy nenahraditelné např. pro politickou kritiku. Rozhodnutí společnosti Facebook začít s rozsáhlým vyhledáváním a mazáním profilů podezřelých jako falešné identity či umělé profily zahrnující systém⁷⁷ bylo kritizováno mimo jiné také českými politickými aktivisty a médii. Jako problematické z právního hlediska je nahlíženo především preventivní zablokování uživatele na základě upozornění jiného uživatele. Mimo ochrany uživatelů je Facebook k výmazu těchto profilů motivován také skutečností, že protože mnoho z nich není skutečných, mohou přispět k nepřesnostem vyhodnocení reklamní kampaně zadané pro uživatele Facebooku. Negativní ohlas tak mohou způsobit jak u samotných zadavatelů, tak u akcionářů společnosti, jejíž hlavní příjem plyne právě z reklamy.

1.2.1. Případová studie *Moreno v. Hartford Sentinel, Inc.*

Vývoj ve věci *Moreno v. Hartford Sentinel, Inc.*⁷⁸ dobře ilustruje přístup amerických soudů k právní odpovědnosti jak sociálních sítí, tak platform poskytujících subjektům možnost vytváření osobních blogů s prostorem pro komentáře a příspěvky jiných, převážně anonymních uživatelů. Zároveň poukazuje na praktický rozpor přístupu, který se obecně snaží udržet výsadní postavení svobody slova, a zároveň ve svém důsledku v případech jako je tento, potlačí právo „anonymního projevu“, které má v americkém právu významné místo. Studentka UC Berkeley na sociální síť MySpace s uvedením pouze svého křestního jména zaslala ironický pamflet popisující její kritický pohled na rodné město, kam se nakrátko vrátila, aby navštívila svou rodinu. Ředitel střední školy v tomto městě s 19 tisíci obyvatel, který kritickou stať objevil, na základě dat v ní uvedených identifikoval autorku a spolu s uvedením jejího plného jména, bez jejího vědomí, pamflet zkopíroval a zaslal do redakce místních novin. I přes snahu

⁷⁷ Viz. dále v této práci

⁷⁸ *Moreno v. Hartford Sentinel, Inc.*, 172 Cl. App. 4th 1125 (Cal. Ct. App. 2009)

autorky a její rodiny byl text přetištěn spolu s následnými kritickými reakcemi rozhořčených obyvatel města. Tyto měly být jen předzvěstí pronásledování rodinných příslušníků autorky stále žijících ve městě, které vyústilo ve střelbu na dům rodičů studentky. Právníci, na které se obrátila autorka a její rodina se případem nechtěli zabývat, právě pro zainteresovanost sociální sítě ve věci. Ta se nakonec nestala ani stranou sporu. Žaloba byla, nakonec neúspěšně podána na vydavatele deníku, který pamflet přetiskl.

Do dnešních dnů zůstává realitou, že se právo jen velmi pomalu a obtížně učí vyrovnávat s existencí kybernetických informačních kanálů. Existují internetové mutace tištěných periodik, internetové informační servery bez oficiální redakční základny a další obdobné platformy. V USA je možnost podání občanskoprávní žaloby na provozovatele webové stránky značně omezena. Příčinou je zákon Communication Decency Act⁷⁹. Tento právní předpis poskytuje PSISs a zakladatelům webových stránek ochranu před právní odpovědností. „S žádným poskytovatelem nebo uživatelem interaktivní počítačové služby nemůže být jednáno jako s vydavatelem nebo mluvčím ve vztahu k jakékoli informaci, která byla poskytnuta jiným poskytovatelem obsahu.“ Znění tohoto ustanovení lze shrnout tak, že pokud informace např. na sociální síti nebo blogu pochází z jiného zdroje, nenese ani jiný uživatel ani provozovatel za tyto žádnou právní odpovědnost resp. nenese právní odpovědnost za jejich dosažitelnost v rámci služby. Někteří odborníci, jako např. Lori Andrews, se domnívají, že by měl existovat zvláštní status pro internetové stránky, u kterých lze předpokládat, že budou obsahovat potenciálně závadné příspěvky, a tyto pak učinit právně odpovědnými. Ve své knize „I know who you are and I saw what you did: Social network and the death of privacy“ vychází v tomto poměrně radikálním názoru Andrews z judikatury i názorů

⁷⁹ USA. Communication Decency Act (CDA): Ustanovení 230(c)(1) tohoto federálního zákona jasně vyjímá internetové vydavatele de facto z právní odpovědnosti v rozsahu, v jakém jsou vázáni vydavatelé tištěných periodik. Na tomto místě je však potřeba připomenout, že ani odpovědnost těchto není podle amerického práva zdaleka tak rozsáhlá, jako u vydavatelů evropských. V praxi se tato výjimka bude týkat také stránek jako je College Humor (humoristické internetové stránky cílené na nezletilé a mladé dospělé, které jsou mezinárodně dostupné a využívají také fotografie a diskuze ze sociální sítě Facebook. Dostupné z WWW: <<http://www.collegehumor.com/>> Vztahovat se bude také na sociální sítě samotné, ale i poskytovatele volného prostoru. Všichni tito nenesou odpovědnost za obsah uploadovaný na jejich službu uživatelem. Zákon však uvádí výjimku pro případy, kdy se jedná o činnost, naplňující skutkovou podstatu trestného činu. To znamená, že pokud by ve Spojených státech existoval, s ohledem na sektorální řešení této sféry, federální zákon umožňující trestněprávní postih např. kyberšikany, byl by PSIS v takových případech, ovšem pouze trestněprávně, odpovědný. Zákon měl primárně za cíl především boj s šířením pornografie po Internetu a, stejně jako většina podobných legislativních aktů, čelil kritice jako neústavní, konkrétně pro tvrzený rozpor s Prvním dodatkem Ústavy.

právních teoretiků. Ve světle těchto poznatků dochází k návrhu právní konstrukce, kdy by právně odpovědnými za příspěvky na svých stránkách byly ty stránky, které podporují nebo dokonce vyzývají k vkládání difamačního obsahu.⁸⁰

Závěrem autorka práce v této souvislosti navrhuje zamyslet se nad názorem kalifornského odvolacího soudu ve věci *Moreno v. Hartford Sentinel*, který uvádí v odůvodnění rozhodnutí, že: „Žádná rozumná osoba by nemohla 'očekávat soukromí' svých příspěvků na sociálních sítích.“ Klade si soud otázku, zda není marný boj o práva na ochranu osobnosti před difamací, pronásledováním, vpády do soukromí a zneužitím osobních údajů bezobsažnou konstrukcí a pokusem dovolat se práv, kterých se sami dobrovolně vzdáváme každou informací, kterou v internetovém prostředí sdílíme? Toto je jeden ze zásadních sporů při diskuzích o osobnostních právech v kyberprostoru. Cesta prevence a samoregulace je oproti právní regulaci nezdědka nahlížena jako snadnější, do budoucna flexibilnější varianta právě s ohledem na předpoklad odklonu společnosti od priorit jako je důstojnost jednotlivce či od aktuálních společenských norem. S tímto názorem se autorka této práce neztotožňuje a domnívá se, že zajištění vymahatelnosti práva na ochranu osobnosti v kyberprostoru je pro rozvoj moderní společnosti naopak nutné.

1.3. Problematika sociálních sítí

Služba Facebook má přes 845 miliónů aktivních uživatelů. Mimoto má Facebook vlastní ekonomiku a vlastní měnu, způsob řešení sporů a systém vztahů s ostatními, reálnými, státy a jejich institucemi⁸¹ Tyto vlastnosti Facebooku však stále stojí poněkud v pozadí, systémy nefungují bezproblémově a legalitu některých z nich lze vidět jako spornou. Mezi sociálními sítěmi⁸² existují z právního hlediska významné rozdíly. Například sociální sítě, jako je YouTube (pro sdílení, sledování a komentování video-příspěvků nebo Twitter (pro okamžité sdílení a komentování zasílaných aktuálních krátkých zpráv ze života uživatele, jak slovem, tak obrazem) mají charakter sítě „veřejné“, kde uživatel předpokládá, že komunikuje se širokou veřejností i jemu neznámých osob. Na rozdíl od těchto, Facebook nebo VKontakte jsou sociální sítě,

⁸⁰ Srov. publikace „I know who you are and I saw what you did: Social network and the death of privacy“ (více použitá literatura) a dále Social Network Constitution. Dostupný z WWW: <<http://www.socialnetworkconstitution.com/the-social-network-constitution.html>>

⁸¹ ANDREWS, Lori B.; *I know who you are and I saw what you did: social network and the death of privacy*, Free Press, 2012. s. 2. ISBN 978-1-4516-5051-8

⁸² Dále také jako OSN (Online Social Network).

kteřé od počátku své služby uživatelům prezentovali, jako komunikaci a sdílení dat s přáteli a rodinou.

Informace, které by byly ve světě off-line považovány za intimní mohou být na internetu ať již cíleně či z nepozornosti sdíleny daleko otevřeněji než právě off-line. Jen v roce 2010 užívalo Facebook více než 20 mil. nezletilých dětí⁸³. 7,5 mil. z nich bylo mladších než 13 let. 5 mil. z těchto uživatelů bylo 10 let nebo méně a nad většinou z jejich profilů nijak nedohlíželi rodiče. Podle oficiálních údajů se v roce 2010 stal 1 milion dětí na internetu obětí obtěžování, zastrasování nebo jiné formy kyberšikany. Je potřeba vzít v úvahu, že se jedná pouze o hlášené případy.⁸⁴ Podle průzkumu EUKids Online 52% českých dětí ve věku mezi 9-12 lety používá nějakou sociální síť. Evropský průměr v této skupině je přitom 38 %. Ve skupině 13–16letých už je to 77 %. V České republice jsme dokonce na 90 %.⁸⁵

1.3.1. Právní závaznost a vymahatelnost Podmínek užívání

Souhlas s průlomem do osobnostních práv v kyberprostoru poskytuje uživatel nejčastěji provozovatelům vyhledávačů, e-mailových účtů, internetových obchodů, ale zejména sociálních sítí. Uživatel PSISs má jen minimální právní záruky soukromí a dalších osobnostních práv, a i ty jsou často narušovány. Uživatel nemůže obsah závazku nijak ovlivnit či regulovat a tyto jsou mimoto jednostranně měněny PSIS. Chris J. Hoofnagle z právnické fakulty Kalifornské univerzity Berkeley se v dokumentu Facebook Obsession⁸⁶ vyjádřil, že regulace soukromí na Facebooku zaručená zněním Podmínek užívání a zásadami ochrany soukromí je poskytována na bázi „ber nebo nech ležet“ a neposkytuje uživatelům žádnou třetí možnost nebo pozici pro vyjednávání. Podle R. Polčáka je problémem dominance některých těchto služeb. Podle Polčáka pro dítě nebo pro teenagera, kteří vidí, že všichni ostatní síť používají, je těžké na ni nebyť. Vlastně by došlo k jejich sociálnímu vyloučení. Podle Polčáka tak můžeme uvažovat i o

⁸³ Skutečná čísla jsou však pravděpodobně mnohem vyšší.

⁸⁴ *Consumer Reports Magazine*, That Facebook Friend might be 10 Years Old, červen 2011, Dostupný také z WWW: <<http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm>>

⁸⁵ Na internetu přibývá dětí i starých [online]. *ManagerWebIHNed.cz* 19. červen 2012 [cit. 2013-02-12], Dostupný z WWW: <<http://managerweb.ihned.cz/c1-56207930-na-internetu-pribyva-deti-i-starych>>

⁸⁶ „Facebook Obsession“ [televizní dokument]. *CNBC*, 2011 [cit. 2012-08-02]. Dostupný z: Netflix (USA)

tom, zda poskytovatelé služeb nezneužívají svého dominantního postavení.⁸⁷ V této situaci přistupuje k ochraně svých obyvatel velice progresivně zejména Spolková republika Německo, která je velice aktivní v regulaci služeb informační společnosti potenciálně zasahujících do osobnostních práv obyvatel. Jeden z mála možných kroků pro celosvětové uživatele rozličných sociálních sítí a dalších SIS, užívajících jejich osobní údajů a obsahu (dat) učinila Electronic Frontier Foundation (EFF)⁸⁸, která monitoruje **Podmínky užívání (Terms of Use/Terms of Services)** významných PSISs, a poskytuje uživatelům možnost okamžitého upozornění ohledně jejich častých změn. Uživatel takové služby však v současné době nemá jinou možnost, než se na změnu připravit a počítat s ní, nebo službu, často virtuální prostor, ve většině případů bez nashromážděných virtuálních hodnot, opustit.⁸⁹ Dalším problémem sociálních sítí je šedá zóna nakládání s uživatelskými informacemi. PSIS je také správcem uživatelského účtu a zejména některé sociální sítě tak archivují bez udání důvodu veškerá data, která uživatel smazal, či jejichž výmaz vyžádal. Mimoto jsou data o uživatelích využívána pro poskytování dalších komerčních služeb třetím osobám, především pro reklamní účely a výzkum trhu.

Součástí Podmínek užívání však může být např. také poskytnutí souhlasu uživatele s budoucími, v době uzavření jemu neznámými změnami v Podmínkách užívání, které PSIS provede. Na rozdíl od např. společnosti Yahoo, která tyto změny provádí bez upozornění uživatele, např. Instagram poskytne uživatelům „včasné varování“, které je informuje o změnách Podmínek užívání, a poskytne jim možnost v případě nesouhlasu, přestat službu užívat. Jiný je přístup společnosti Facebook, která poskytuje uživatelům omezený čas pro hlasování o chystaných změnách. „Voleb“ se však musí účastnit alespoň 30% uživatelů. Pokud se hlasování nezúčastní dostatečný počet uživatelů, jsou podmínky zavedeny bez dalšího. Vzhledem k vysokému počtu uživatelů služby a nastavení hlasování na hlasování o odmítnutí navrhované změny, je

⁸⁷ JANUŠ, J.; Rozhovor s R. Polčákem: Hodně z toho, s čím lidé souhlasí na sítích, je nemravné nebo neplatné. *Právní rádce*, (2012) 10/2012. s.12-15

⁸⁸ Terms Of (Ab)Use [online]. *Electronic Frontier Foundation* [cit. 2013-02-02], Dostupný z WWW: <<https://www.eff.org/issues/terms-of-abuse>>

⁸⁹ JANÁK, M., Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu [online]. *IT Právo*, 2009 [cit. 2012-11-19]. Dostupný z WWW: <http://www.itpravo.cz/index.shtm?l?AA_SL_Session=8bab7c81254d3179ff720eb355e677c0&sh_itm=556af04eed0e>

nepravděpodobné, že by se v krátkém čase vyjádřilo k navrhované změně dostatečné množství uživatelů.

Právní povaze vztahu mezi uživatelem a PSIS se věnuje P. Otevřel ve svém článku „Sociální sítě z pohledu firmy: Co můžete a co ne?“. Připomíná především, že právní vztah, který vzniká v souvislosti s registrací a užíváním služeb nabízených provozovateli sociálních sítí je natolik atypický, že není možné použít žádný zákonem stanovený smluvní typ. V případě absence výslovného ustanovení ve smlouvě tak bude pro obě smluvní strany obtížné dovozovat svá práva a nároky ze zákona odkazem na přiměřené použití toho či onoho ustanovení. Platí tak zásada, že obě smluvní strany budou mít právě taková práva a povinnosti, jak si je ve smlouvě sjednají.⁹⁰ Autor dále v článku připomíná praxi, kdy mnoho zahraničních PSIS provozujících sociální sítě uplatňuje v těchto smlouvách – Podmínkách užívání své domovské právo a do této jurisdikce, zpravidla z mnoha ohledů výhodné pro PSIS, jako např. právo státu Kalifornie u služby Facebook, se také snaží přenést všechny případné právní spory s uživateli. Jak bude dále osvětleno v této práci, lze však uvažovat také o uplatňování zákona o mezinárodním právu soukromém nebo judikatury, jako např. rozhodnutí ve spojených věcech *eDate Advertising GmbH proti X a Olivier Martinez a Robert Martinez proti MGN Ltd.* Nezletilý by také mohl žalovat PSIS v souvislosti se sběrem osobních údajů bez závazného souhlasu uživatele. Také by pak neplatila doložka o žalování jen u kalifornského soudu, a právní vztah by se mohl řídit přísnějším národním právem uživatele, a zde by také mohl být příslušný soud.

Proto je zcela zásadní věnovat se blíže české právní úpravě platnosti tohoto právního úkonu ve vztahu k nezletilému. Co se spornosti závaznosti smlouvy s PSIS týče, můžeme se např. obrátit k § 49 OZ, který poskytuje možnost odstoupit od smlouvy účastníku, který ji uzavřel v tísní za nápadně nevýhodných podmínek. Takové odstoupení smlouvu od počátku zneplatňuje. Vzhledem k výše uvedené úvaze R. Polčáka je teoreticky tato aplikace představitelná. Bylo by totiž možné se, za jistých okolností odvolávat, vzhledem ke znění Podmínek užívání, na tíseň vzhledem k jazyku ujednání. Ačkoli Podmínky jsou např. u sociální sítě Facebook dostupné již po určitou dobu také v českém jazyce, připomeňme, že jak uvádí stránky E-bezpečí, Podmínky užívání služby Facebook byly do češtiny přeloženy teprve v roce 2012, a veškeré

⁹⁰OTEVŘEL, P.; Sociální sítě z pohledu firmy: Co můžete a co ne?, *Právní rádce*. (2012) 10/2012. s. 8-11

informace o aktivitách společnosti vůči uživatelským datům, se nachází v několika různých dokumentech.⁹¹ Podmínky mimoto především obsahují doložku, která jako závaznou ustanovuje anglickou verzi smlouvy. Pokud nezletilý jazyk neovládá natolik, aby anglickou verzi našel a porozuměl ji, lze analogicky užít stejnou argumentaci, jako u cizince zavazujícího se smluvně bez znalosti českého jazyka⁹².

Co tedy z domnělé relativní neplatnosti podmínek vyplývá? Sociální síť nebo podobná SIS tak teoreticky nemůže užívat široké licence k fotografiím, resp. k celému autorskoprávnímu obsahu, jehož je nezletilý autorem. Dalším následkem může být, že pro uživatele nemusí být závazné, že nesmí svůj profil založit, pokud je mladší 13 let nebo že nemá zakládat falešné profily jiným či neexistujícím osobám. Nezletilý není povinen dodržovat také další omezení definovaná Podmínkami, mající za cíl minimálně nastolení jakéhosi základního pořádku v užívání, především na základě zásad netikety⁹³. Zároveň však není teoreticky PSIS povinen chránit nezletilého uživatele svých služeb nabízenými prostředky ochrany, ačkoli v tomto případě by, minimálně v případech zásahů kvalifikovatelných jako trestné činy, PSIS tuto povinnost měl, zejména ve většině zemí EU, na základě upozornění. Vzhledem k právní odpovědnosti má tato neplatnost vliv zejména v tom smyslu, že by nezletilý, který tím pádem ani nedal souhlas ke shromažďování svých osobních údajů, nakládání s těmito a jejich dalšímu postupování třetím osobám, mohl teoreticky zřejmě podat podnět Úřadu pro ochranu osobních údajů (ÚOOÚ), který by následně mohl udělit PSIS správní pokutu. Došlo-li by k zásahu do osobnostních práv nezletilého, v některých případech by zřejmě tento mohl také podat občanskoprávní žalobu na PSIS.

Zajímavou se jeví z tohoto pohledu úvaha v publikaci „Ochrana osobnosti podle občanského práva“, o tom, zda je v rozporu se zákonem či s dobrými mravy⁹⁴ bylo-li za

⁹¹ DOBEŠOVÁ, P.; SZOTKOWSKI, R.; Stručný přehled vybraných podmínek užívání Facebooku [online] *E-bezpečí*, 2. leden, 2013 [cit. 2013-13-01]. Dostupný z WWW: <<http://www.e-bezpeci.cz/index.php/temata/socialni-sit/587-struny-pehled-vybranych-podminek-uivani-facebooku>>

⁹² § 37 odst. 1 OZ, §49a OZ

⁹³ Etiketa pro internet – zásady slušného a bezpečného chování v kyberprostoru

⁹⁴ Dobré mravy vymezuje nález Ústavního soudu č. II.ÚS 249/97: „Dobré mravy' jsou souhrnem etických, obecně zachovávaných a uznávaných zásad, jejichž dodržování je mnohdy zajišťováno i právními normami tak, aby každé jednání bylo v souladu s obecnými morálními zásadami demokratické společnosti. Tento obecný horizont, který vývojem společnosti rozvíjí i svůj morální obsah v prostoru a čase, musí být posuzován z hlediska konkrétního případu také právě v daném čase, na daném místě a ve vzájemném jednání účastníků právního vztahu. Takovéto hodnocení přísluší výhradně obecným soudům, není ani v možnostech ústavního soudu vnikat do oněch subtilních vztahů jednotlivců, pokud jejich jednání nesignalizuje porušení základních práv a svobod.“

udělení svolení k nakládání s určitou osobnostní hodnotou smluveno peněžité či jiné plnění. Autoři publikace dochází k závěru, že bude záležet především na tom, o jakou hodnotu se jedná. Dále konkrétně příkladmo uvádějí, že je-li za plnění dán souhlas k nakládání např. s lidskou svobodou nebo důstojností, bude dohoda o plnění za poskytnuté svolení v rozporu se zákonem respektive s dobými mravy⁹⁵. Vzhledem k tématu práce si tak lze připomenout experimenty společnosti Google s placením uživatelům za jejich sledování a užívání veškerých jejich osobních údajů a navrhované modely licencování osobnostních hodnot. Podstatné však je, že svolení fyzické osoby lze, obecně řečeno, vztáhnout pouze na takové užití hodnoty její osobnosti, jehož způsob, rozsah a účel jí byl znám, resp. jí musel být znám v době udělování tohoto svolení. Toto tvrzení opět stojí proti povaze Podmínek užívání v kontextu jejich změn a vývoji povahy poskytovaných služeb.

Jak již bylo řečeno, pro bezpečnostní politiku provozovatelů sociálních sítí je typický dynamický vývoj. V současné době již neplatí bez výhrad, že uživatel má možnost téměř veškeré informace, které o něm lze např. na Facebooku najít nastavit do detailního soukromého či částečně soukromého módu pouze za cenu projití 50 různých nastavení, výběru ze 170 možností a případně studia Prohlášení o ochraně soukromí na Facebooku, které má víc než 45.000 slov⁹⁶. Ačkoli ke změnám na tomto poli dochází, ty nepředstavují vždy zlepšení. Jsou totiž doprovázeny nezřídka matoucími změnami uživatelského prostředí a automatickým zpřístupněním některých dat, která v původní podobě uživatel nastavil jako soukromá, a to bez náležitého upozornění uživatele či poskytnutí možností změny před aplikací zpřístupnění. Pravdou zůstává, že uživatelé internetových služeb nejsou dostatečně poučeni. Souhlas, který s Podmínkami užíváním služeb rychlým odkliknutím poskytují, není informovaným souhlasem. Jedním z důkazů této skutečnosti mohl být pokus, při kterém společnost Gamestation do Podmínek užívání začlenila pasáž, kterou se v typických ustálených formulacích odborného právního textu uživatel zavazovat upsat společnosti svou duši. 88% uživatelů souhlas

⁹⁵ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 108. ISBN 80-7201-484-6

⁹⁶ ANDREWS, Lori B.; *I know who you are and I saw what you did: social network and the death of privacy*, Free Press, 2012. s. 129 ISBN 978-1-4516-5051-8

poskytlo⁹⁷. Pokud může většinu SIS podle Podmínek užívání užívat osoba starší 13ti let, je možné předpokládat u takto staré nezletilé osoby jednak schopnost pochopit význam podobného textu, a zároveň právní způsobilost uzavírat takto smlouvu? Autorka této práce se domnívá, že pro svou povahu a složitost právního vztahu mezi uživatelem a PSIS je platnost takovéto smlouvy z právního hlediska sporná? Bude tomu tak zejména s ohledem na české, potažmo evropské právo, ačkoli americké soudy Podmínky užívání jako závazné smlouvy uznávají.

2. Nezletilý na Internetu

2.1. Úvod

Tato práce se zabývá velice specifickou skupinou subjektů nezletilými uživateli. O to těžší je regulovat jejich aktivity na internetu, kterými mohou nezletilí být ohrožováni nebo naopak sami ohrožovat druhé. Jak mezinárodní úmluvy⁹⁸, tak např. Listina přikládají zásadní význam právu dítěte, resp. osobnosti na svůj všestranný rozvoj. Moderní technologie jistě slouží k rozvoji osobnosti. O všestrannosti tohoto rozvoje však lze polemizovat. Obsahu internetu a jeho vlivu na osobnost nezletilého je potřeba věnovat pozornost také z toho důvodu, že se jedná o významné prostředí rozvoje dnešních nezletilých, mající mimořádný vliv na tvorbu žebříčku hodnot, potřeb a vzorců chování dětí a mládeže.

Jednou z otázek, které si musíme klást při úvahách o ideální podobě právní regulace ochrany osobnosti nezletilých v kyberprostoru, je jejich přístup k chráněným osobnostním právům, především k soukromí. V roce 2008 byl proveden rozsáhlý výzkum John D. and Catherine McArthur Foundation o užívání internetu nezletilými. Z jeho výsledků vyplývá, že nezletilí užívají internet k tomu, aby se seznamovali a rozšiřovali počet přátel, ale také, aby se věnovali svým zájmům. Expertka na sociální

⁹⁷ 7,500 Online Shoppers Unknowingly Sold Their Souls [online]. *Fox News* 15 duben, 2010 [cit-2012-07-21]. Dostupný z WWW: <<http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/>>

⁹⁸ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Úmluva Rady Evropy č. 185 o kybernetické kriminalitě, Doporučení Rady ministrů Rec(2001)8E ze dne 5. září 2011 o samoregulaci vzhledem ke kybernetickému obsahu (samoregulace a ochrana uživatele před protiprávním a škodlivým obsahem v nových informačních a komunikačních službách), Úmluva o ochraně lidských práv a základních svobod Rady Evropy, Úmluvě o ochraně lidských práv a základních svobod, Úmluva o ochraně dat z roku 1980, Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 108), Mezinárodní pakt o občanských a politických právech OSN

sítě a pohyb nezletilých v kyberprostoru danah boyd⁹⁹, která se ve svém výzkumu soustředí na komunikaci nezletilých, tvrdí, že mladí lidé jsou ochotni sdílet mnohem více osobních informací na internetu. Vysvětluje, že není pravdou, že by se mládež nezajímala o své soukromí, pouze jej vnímá jinak, než dospělí. Na rozdíl od dospělých, domov není pro nezletilé místo, kde nachází soukromí. Domov je, z pohledu mládeže, podle výzkumu danah boyd, ovládán rodiči, kteří tak mají přehled o životě, přátelích, návštěvách a aktivitách svých dětí. Výsledkem je, že na internetu se mladý člověk cítí více v soukromí, protože v tomto prostředí má větší kontrolu nad děním¹⁰⁰. Ačkoli je obecným předpokladem, že nezletilí se nechovají odpovědně ohledně sdílení informací o svém soukromí, poslední studie ukazují, že neblahé zkušenosti s osobnostními ohroženími a zásahy na internetu změnily jejich náhled na ochranu soukromí na internetu. Například ze studie Pew 2010 vyplynulo, že nezletilí a mladí uživatelé internetu jsou starostlivější, co se ochrany svého soukromí týče, než starší dospělí uživatelé¹⁰¹. John Palfrey a Urs Gasser z Harvardského Bergman Centra naopak docházejí k závěru, že mladší generace, která vyrůstala s technologiemi (tzv. digital natives¹⁰²) dělají méně rozdílů mezi tím, co budou sdílet a co ne, a obecně pojmají více důvěry ke sdílení dat na internetu. Podle autorů se jedná o celosvětový trend¹⁰³. Je tedy evidentní, že v této podstatné otázce nevládne jednota.

2.2. Přechod k virtuálním hodnotám

R. Polčák ve svých přednáškách zmiňuje problematiku virtualizace, kterou se v minulosti zabýval především Pierre Lévy¹⁰⁴, a která zasahuje do občanského práva v několika ohledech. Základní otázkou tohoto přístupu je: Může právo regulovat virtuální objekty? Virtualizace přináší nové způsoby porušování práva, představuje oblast, pro kterou doposud neexistuje uspokojivá právní regulace těchto ohrožení a

⁹⁹ Zápis bez kapitálek je ustálená forma zápisu jména danah boyd.

¹⁰⁰ JOHNSON, B.; Privacy No Longer a Social Norm, says Facebook Founder [online] *The Guardian*. 11. leden 2010 [cit-2012-17-08]. Dostupný z WWW:

<<http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>>

¹⁰¹ PEW Internet 2010: Generations 2010. *Pew Research Center*. Dostupný z WWW:

<<http://pewinternet.org/Reports/2010/Generations-2010.aspx>>

¹⁰² Digital natives (ang.) doslovný překlad: Původní obyvatelstvo oblasti digitálních technologií. Jedná se o mladou generaci, která jako první vyrostla s počítači a ovládá je lépe, než dospělí.

¹⁰³ PALFREY, J.; GASSER, U.; *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books, 2008. s. 66-69. ISBN 978-0-465-00515-4

¹⁰⁴ Autor knihy *Cyberculture*, University of Minnesota Press (2001) ale také studie *Qu'est-ce que le virtuel? La Découverte*, Paris (1998) /*Becoming Virtual. Reality in the Digital Age*, Plenum Trade, NY (1998) ISBN-10: 0306457881

zásahů a může také představovat prostor pro aplikaci sankcí, pokud nedojde k rozvoji práva pro kyberprostor. Z rozlišovaných kategorií virtuální podnik, virtuální peníze a virtuální přátelství se bude tato práce zabývat pouze posledními dvěma kategoriemi.

2.2.1. Virtuální peníze

Příklady negativních následků nesprávně právně regulovaného užívání peněz nezletilými v kyberprostoru ilustruje hromadná žaloba na Apple App Store¹⁰⁵, týkající se dětských počítačových her Fish Tank a Smurf Village. Tyto počítačové hry jsou cílené na děti. Hry lze stáhnout z platformy Apple App Store zdarma. Pro jejich správné fungování ale hra vyžaduje, aby si dítě za reálné peníze dokupovalo doplňky (např. pro chov rybiček ve hře Fish Tank je potřeba koupit krmení, další ryby atp.). Dítě není podle žaloby schopné rozeznat cenu peněz a především virtuálního zboží a je zneužíváno PSIS. Podobně v The Sims Store, internetovém obchodu pro počítačovou hru představující simulaci života, uživatel nakupuje předměty každodenní potřeby pro své postavy ve hře za virtuální měnu, kterou je však potřeba zakoupit za reálné peníze. Také Second Life nabízí možnost obchodu, namátkou, s módou nebo dokonce s nemovitostmi, kde pouze virtuální statky jsou pořizovány za skutečné peníze. Problémem z pohledu osobnostních práv může být ztráta odstupů a schopnosti odlišovat hodnoty virtuální od reálných, který ilustruje případ Legend of Mir¹⁰⁶, kdy v Singapuru zavraždil hráč svého spoluhráče za odcizení a prodej virtuální zbraně z počítačové internetové hry za reálné peníze na internetové nákupní platformě. K podobnému případu došlo také v České republice, kdy brněnská policie zadržela čtrnáctiletého chlapce, který se pokoušel prodat virtuální postavu z oblíbené internetové počítačové hry World of Warcraft, kterou neoprávněně získal hackerským útokem. Chlapec se dopustil trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací. (...) Předmětná virtuální postava bojovníka měla pro zasvěcené hráče vysokou hodnotu, patřila totiž k jedněm z nejsilnějších. „Majitel toho dosáhl nejen herními schopnostmi, ale také tím, že do jeho vybavenosti investoval značnou sumu

¹⁰⁵ LEE, A.; Apple Hit with Class Action Lawsuit Over Minors' Purchase Of In-App Goods. *Huffington Post* [online] 16. leden 2011 [cit. 2012-08-21]. Dostupný také z WWW: <http://www.huffingtonpost.com/2011/04/15/apple-hit-with-class-acti_n_849936.htm>

¹⁰⁶ MICHELL, A., P.; Gamer Killed Over Virtual Legend of Mir 3 Sword. *The Internet Patrol*, 14. říjen 2010 [cit. 2012-05-14]. Dostupný z WWW: <<http://www.theinternetpatrol.com/gamer-killed-over-virtual-legend-of-mir-3-sword/>>

peněz.“¹⁰⁷ Problematika právní regulace virtuálních obchodních transakcí je samostatnou složitou otázkou, není však předmětem této práce. Tato realita, kde nezletilý uživatel je nezdědkou manipulován k akumulaci větších zisků PSIS či třetí stranou, přispívá nejen k zásahu do soukromí nezletilého uživatele sběrem jeho osobních údajů (např. hra sice nepovoluje užívání osobami mladšími 13ti let, ale svým obsahem a architekturou je primárně orientovaná právě na tuto skupinu), ale zároveň může také představovat zásah do práva dítěte na osobní rozvoj, rodinný život a další.

2.2.2. Virtuální přátelství

Podle průzkumu EU Kids Online¹⁰⁸ „Česko vychází jako stát, kde se mladiství výrazně častěji dostávají do rizikových situací, například v seznamování s cizími lidmi. Evropský průměr překračují v tomto směru téměř dvakrát.¹⁰⁹ (...) 46 % českých dětí ve věku od 9ti do 16ti let používajících internet někdy na síti mělo kontakt s člověkem, kterého znaly právě jen virtuálně. A celých 15 % dětí se pak s někým takovým setkala i osobně.“¹¹⁰ Vytváření virtuálních přátelství může v některých případech představovat otevřenou bránu pro manipulaci, difamaci, šikanu a ohrožení nezletilých vytvářením virtuálních přátelství s potenciálními predátory¹¹¹.

Zajímavým příkladem budování virtuálních přátelství je prostředí zmíněné simulace Second Life. Původně společnost Linden Lab provozovala dvě platformy - jednu pro uživatele starší 17ti let a druhou, nazvanou Teen Second Life, pro uživatele od 13ti do 17ti let. Později ale pro nedostatek dohledu společnosti „dětský“ Second Life začal sloužit jako zázemí pro radikální skupiny propagující především rasovou nenávist. Reakcí provozovatele bylo snížení věkové přístupnosti „dospělého“ Second Life na 16 let a dále byl „dětský“ Second Life 22. ledna 2011 oficiálně uzavřen. Uživatelé, kteří dosáhli 16ti let mohou užívat „dospělý“ Second Life s všeobecnou přístupností, a jeho

¹⁰⁷ Chlapec ukradl v on-line hře postavu bojovníka, zadržela ho policie [online], *novinky.cz*, 16. leden 2011 [cit. 2012-08-21] Dostupný z WWW: <<http://www.novinky.cz/krimi/290172-chlapec-ukradl-v-on-line-hre-postavu-bojovnika-zadrzela-ho-policie.htm>>

¹⁰⁸ EU Kids Online, Dostupný z WWW: <<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx>>

¹⁰⁹ POVOLNÝ, D., mluvčí brněnské Masarykovy univerzity, která výzkum v Česku na jaře 2012 prováděla.

¹¹⁰ KEMÉRYOVÁ, Z.; České děti přitahuje internet: Podceňují riziko anonymního seznamování [online] *Ihned*, 21. červenec 2012 [cit. 2012-11-05]. Dostupný z WWW: <<http://zpravy.ihned.cz/cesko/c1-56609270-ceske-deti-pritahuje-internet-podcenuji-riziko-anonymniho-seznamovani>>

¹¹¹ Just How Many Facebook Friends Do You Need? [online], *Newsweek Magazine*, 15. říjen, 2012 [cit. 2012-20-10]. Dostupný z WWW: <<http://www.thedailybeast.com/newsweek/2012/10/14/just-how-many-facebook-friends-do-you-need.html>>

části s věkově nevhodným obsahem po dovršení 18ti let. Osoby mezi 13ti - 16ti roky se mohou v prostoru Second Life pohybovat, ovšem pouze na vyhrazených místech a určeným způsobem, a to pouze tehdy, pokud jsou součástí instituce, která nad tímto prostorem dohlíží. V praxi se bude např. jednat o virtuální třídy škol a organizované volnočasové aktivity. Do doby zrušení „dětského“ Second Life působila regulace růstu uživatele značné uživatelské i právní diskuze. Po dovršení Second Life „dospělosti“, tedy 17ti let (posléze 16ti let), byl totiž uživatel automaticky, i s veškerým svým virtuálním majetkem, přenesen do prostředí „dospělého“ Second Life, a do „dětského“ se již nesměl vrátit. Pokud tak docházelo k navazování virtuálních přátelství mezi nezletilými, třeba i z různých kontinentů, tato byla, alespoň v podobě virtuální socializace, přetržena a mohlo tak docházet k osobnostní újmě nezletilého.

2.3. Sporná otázka závislosti

Podle studie společnosti Telefonica je průměrný věk prvního kontaktu s počítačem v České republice 3 roky. Hry mohou být spojeny s behaviorálním marketing a některé vyzývají děti k utrácení skutečných peněz za virtuální benefity ve hře¹¹². Ve většině světových zemí není závislost na počítačových hrách, technologiích, počítači či internetu uznanou diagnózou. Jinak tomu je v některých technologicky rozvinutých asijských zemích, jako je Jižní Korea nebo Japonsko. Psychiatr Ahn Dong-Hyun se z pověření korejské vlády věnoval tříleté studii závislostí dětí na internetu. Došel k závěru, že se nejedná o pouhý společenský trend, ale o skutečnou závislost. V Koreji se tak jedná o oficiální psychiatrickou diagnózu a jsou tak např. budována odvykací centra pro závislé děti. Závislost si nezletilý nemusí vybudovat jen na hrách v tradičním slova smyslu, popsány jsou také případy závislosti na virtuální komunikaci, on-line pornografii, budování svého virtuálního alter-ega nebo na informacích, tedy vyhledávání. Jedná se o problematiku, která se blíže dotýká také České republiky. Podle studie J. M. Parsona z Iowské univerzity¹¹³ splňuje až 15% hráčů také v České republice oblíbených MMORPG požadavky pro kvalifikaci internetové závislosti. Fakt, že ve Velké Británii je až 18% studentů považováno za patologické uživatele internetu,

¹¹² Srov. Fish Tank, Smurf Village a další

¹¹³ PARSON, J. M.; An examination of massively multiplayer online role-playing games as a facilitator of internet addiction [online] *Iowa Research Online*. 2005 [cit. 2012-08-11]. Dostupný také z WWW: <<http://ir.uiowa.edu/etd/98/>>

kterým užívání SIS způsobilo prokazatelné studijní nebo interpersonální problémy¹¹⁴, nebo že až 3,5% německých nezletilých dětí vykazuje znaky internetové závislosti¹¹⁵ je důkazem, v mnohém bezesporu pozitivní, globalizované povahy světa dnešních dětí. O to složitější je právní regulace jejich aktivit, a o to snadnější je celosvětové šíření negativních uživatelských aktivit. Je nutné připomenout, že internetová závislost je podle studií nezdědka spjata také s depresemi, sebepoškozováním a dalšími patologickými jevy.

2.4. Narušení sociálních vazeb

Ročně mluví s rodiči průměrné dítě jen 50 hodin, zato u počítače ročně stráví 1500 hodin¹¹⁶. Může tak docházet mimo jiné k potlačování zmíněného práva na všestranný rozvoj a práva na rodinný život. Nadměrné užívání technologií může vést k narušení sociálních vazeb. Směrodatným se v některých případech může pro nezletilého stávat názor neznámých osob z prostředí internetu, a tak, pokud se nezletilý dostane do krizové situace, může dojít k tomu, že i v případech, kdy je dostupná pomoc odborníků či rodiny, může se tato mítet účinkem. Upozornit je nutné především na problematiku internetových „sebevražedných paktů“ nezletilých, které se objevují stále častěji jak v USA, tak i v zemích EU¹¹⁷.

2.4.1. Případová studie: *Minnesota v. Melchert-Dinkel*

Následující případová studie ilustruje nebezpečí neregulovaného navazování kontaktů nezletilých v kyberprostoru a také, proč by měl být při vyhodnocování otázky osobnostní újmy přikládán v přiměřené míře význam také subjektivnímu vnímání zásahu obětí, jak bude blíže rozebráno v jiné části této práce. Kanadská studentka Nadia Kajouji trpěla depresemi a nespavostí. Dívka začala anonymně komunikovat s mladou

¹¹⁴ NIEMZ, K. et al., Prevalence of Pathological Internet Use among University Students and Correlations with Self-Esteem, the General Health Questionnaire (GHQ), and Disinhibition [online] *CyberPsychology & Behavior*. 6. prosince 2005 [cit-2012-09-18], Volume: 8 vydání 6, s. 562-570. Dostupný také z WWW: <<http://online.liebertpub.com/doi/abs/10.1089/cpb.2005.8.562>>

¹¹⁵ PEUKERT et al., Internet- and computer game addiction: phenomenology, comorbidity, etiology, diagnostics and therapeutic implications for the addictives and their relatives, *Psychiatr Prax.* [online] 2010, Epub 2010, červenec 37(5) [cit. 2012-07-14] s. 219-24. Dostupný z WWW: <<http://www.ncbi.nlm.nih.gov/pubmed/20597036>>

¹¹⁶ Safer internet.cz. Projekt Saferinternet.cz - představení [prezentace]. Zdroj: výzkumu, *Francouzská asociace rodičovských sdružení (UNAF)*.

¹¹⁷ Tři mladé Němky spáchaly sebevraždu. [online] *idnes.cz*. 17. srpen 2011 [cit. 2012-09-23]. Dostupný z WWW: <http://zpravy.idnes.cz/tri-mlade-nemky-spachaly-v-lese-spolecnou-sebevrazdu-p00-zahranicni.aspx?c=A110816_212723_zahranicni_brm>

americkou zdravotní sestrou, se kterou se seznámila na internetu. Zdravotní sestra jménem Cami se svěřila Nadie, že sama dlouhodobě trpí depresemi a je rozhodnuta spáchat sebevraždu. Cami navrhla studentce spáchat společně sebevraždu před webkamerou počítače. Přibližně ve stejnou dobu se bývalá učitelka z Velké Británie po smrti svých rodičů také obrátila k internetu. Narazila na několik chatových skupin pro sebevrahy. Poté, co si pročetla rozhovory ve skupině, upoutaly ji příspěvky zdravotní sestry Cami. Z jejich znění získala žena podezření, že se zdravotní sestra snaží přimět mladé lidi k sebevraždě. Cami byl ve skutečnosti 46ti-letý William Francis Melchert-Dinkel, americký deviant z Minnesoty, který se snažil získat možnost sledovat nezletilé při páchání sebevraždy¹¹⁸. Britce se nakonec podařilo identitu Melchert-Dinkela odhalit¹¹⁹. Ve chvíli, kdy policie začala Melchert-Dinkela prověřovat byla Nadia Kajouji již dva týdny mrtvá. Melchert-Dinkel se zapojil do více než deseti sebevražedných paktů, pět z jeho obětí sebevraždu, s největší pravděpodobností pod jeho vlivem a naléháním, spáchalo¹²⁰. Ohlasy na případ byly smíšené – někteří bojovníci za lidská práva jednání Melchert-Dinkela a jeho obětí hájili a připomínali svobodu jedince, právo na tělesnou integritu a sebevraždu. Americké soudy se potýkaly s přeshraničním prvkem věci (Nadia zemřela v Kanadě bez přítomnosti Melchert-Dinkela) a s nedostatkem opory v psaném právu. Zatímco napomáhání sebevraždě trestné je, jeho definice podle amerického práva zní: „poskytování fyzického/ých prostředku/ů, s jejichž pomocí zamýšlí druhý dokonat sebevraždu nebo účast na fyzickém aktu, kterým druhý zamýšlí dokonat sebevraždu.“ Kanada oproti tomu má právo, které upravuje trestnost nabádání k sebevraždě¹²¹. Kanadské úřady se však rozhodly nezažádat o vydání Melchert-Dinkela, neboť nepřikládaly jeho korespondenci s obětí dostačující podíl na její sebevraždě. Ačkoli také ve státě Minnesota je trestné nabádat k sebevraždě, právní zástupce Melchert-Dinkela argumentoval tím, že jeho aktivity byly chráněny Prvním dodatkem. Minnesotský soud nakonec shledal Melchert-Dinkela vinným z nabádání k sebevraždě a odmítl argumentaci, že by se na jeho

¹¹⁸ *Minnesota v. Melchert-Dinkel*, 2011 WL 893506 (Minn. Dist. Ct. 2011)

¹¹⁹ Village Sleuth Unmasks US Internet Predator Behind Suicide Pacts. [online] *Algeria.com* [cit-2012-09-12]. Dostupný z WWW: <<http://www.algeria.com/forums/computer-internet/27173-village-sleuth-unmasks-u-s-internet-predator-behind-suicide-pacts.html>>

¹²⁰ *Minnesota v. Melchert-Dinkel*, 2011 WL 893506, popis skutkového stavu, odst. 39, (Minn. Dist. Ct. 2011)

¹²¹ Kanada. Criminal Code of Canada, R.S. 1985, c-46, s. 241. Dostupný také z WWW: <<http://www.efc.ca/pages/law/cc/cc.html>>

zákeřné chování, které způsobilo přímou újmu druhým osobám, vztahovala ochrana svobody projevu podle Prvního dodatku.¹²² Na podobných případech, které jsou stále méně ojedinělé, lze ilustrovat nejen rizika anonymity a nedostatečné kontroly internetu, ale také tragické následky stále rozšířenější víry nezletilých, že jejich jediným soukromím je svět na internetu, a že nemoderované anonymní skupiny jsou jediným místem, kde se mohou svěřit a hledat řešení svých problémů.

2.5. Právní definice osobnosti a její specifika v kyberprostoru

Definice osobnosti v českém právu vychází z judikatury. Základní právní věta zní: **„Za osobnost lze považovat člověka jako jednotlivce, jako subjekt poznání, resp. poznávání, prožívání a jednání ve své společenské podstatě i individuálních zvláštnostech, jako nejmenší sociální jednotku i určitou psychofyzickou a sociálně psychologickou strukturu.“**¹²³. Úplný výklad této definice představuje také několik poměrně podstatných závěrů pro ochranu osobnosti nezletilých v kyberprostoru. Některé z nich zde krátce vyložíme.

Nejprve se věnujme části usnesení se zněním: **„Osobnost se projevuje jako dynamický systém, jehož rysy se mění podle věkových stupňů, přičemž dosahují relativně větší stálosti v dospělosti.“** Lze tedy předpokládat, že jinak bude vnímat stejný zásah osoba různého věku. Jedná se také o připomínku procesu vývoje v jeho individualitě.

Dále: „Psychologické vlastnosti osobnosti jsou zprostředkovány zvláštnostmi nervového systému, které však samy o sobě neurčují charakter, zájmy a sklony člověka. Ty se vytvářejí v **procesu individuálního vývoje** vlivem výchovy, výuky a společenského prostředí vůbec, přičemž aktivita subjektu ("sebetvoření člověka") v průběhu vývoje roste.“ Uvedení individuality vývoje spolu s celkovým vyzněním této části odůvodnění lze chápat jako podpůrné tvrzení pro uznání individuálního charakteru závažnosti zásahu do osobnosti jedince.

„Každá osobnost (...), zároveň však odráží specifické historické podmínky své doby, národa, společenského zařazení, povolání a má své svérázné, neopakovatelné rysy. **Je tak mimo jiné i produktem své doby a jejích podmínek,** zároveň v té či oné míře

¹²² Warrant of Commitment, *Minnesota v. Melchert-Dinkel*, Case No. 66-CR-10-1193 (Minn. Dist. Ct., May 4, 2011)

¹²³ Usnesení Nejvyššího soudu ze dne 16.8.2007, sp. zn. 30 Cdo 2082/2007 nebo Usnesení Nejvyššího soudu ze dne 31. 1. 2008, sp. zn. 30 Cdo 2072/2007

svým podílem na tom produkuje tuto dobu a její podmínky utvářením a přetvářením svého okolí.“ Tato část je podstatným signálem utváření společenských hodnot a změn v obecném hodnocení osobnostních hodnot společností. Výše uvedené má význam vzhledem k současnému vývoji společnosti a doposud nejasnému hodnocení vztahu společnosti k rozvoji některých moderních technologií potenciálně zasahujících do osobnostních práv člověka při jejich stále intenzivnějším užívání. „A protože **se jedná o nejvlastnější, nejniternější a nejintimnější sféru lidské osoby**, jejíž **dotčení zvenčí je zásahem dotčenou fyzickou osobou velmi často pocitováno se značně nepříznivou intenzitou**, (...).“ Tuto část lze opět uplatnit jako argument pro přiměřené zohlednění subjektivní složky při hodnocení újmy způsobené zásahem do osobnostních práv nezletilé osoby.

Jak vyplývá z definice osobnosti, která je odvozována z, v této souvislosti již rozebrané judikatury, citový a mentální vývoj jedince je velmi individuální. I pokud má věkový standard odrážet pouze technologickou zdatnost jedince v moderní společnosti, tedy věk, kdy je dítě již natolik obeznámeno s kyberprostorem, že mu nehrozí žádná rizika, je taková hranice nepřesná. Citovat lze výsledky studie „Living and Learning with New Media“ centra John D. and Catherine McArthur Foundation: „Vzhledem k rozmanitosti druhů digitálních médií je problematické vytvořit měřítka, proti kterým by bylo možné změřit technologickou vyspělost a znalost nezletilých.“¹²⁴

3. Formy ohrožení či zásahu do osobnostních práv nezletilého v kyberprostoru

3.1. Zneužívání nezletilé osoby

Docházet k němu může několika různými způsoby. Většina z nich bude řešena trestním právem, může však být současně řešena také užitím občanskoprávního institutu ochrany osobnosti. Nejzávažnější z aktivit zde bude oklamání nezletilé oběti pod falešnou identitou za účelem pohlavního zneužití, tzv. cyber/kybergrooming¹²⁵. Je namístě připomenout, že se jedná o typické závadné jednání v kyberprostoru a nikoli

¹²⁴ John D. and Catherine McArthur Foundation, Living and Learning with New Media: Summary of Findings from the Digital Youth Project [online] listopad 2008 [cit. 2012-07-14] s. 2. Dostupný z WWW: <www.digitalllearning.macfound.org/ethnography>

¹²⁵ Stručný úvod do problematiky kybergroomingu pro nezletilé uživatele lze nalézt na <<http://www.nebudobet.cz/?page=kybergrooming>>

samostatnou skutkovou podstatu. Rozsáhle se tomuto nebezpečnému jednání věnuje např. publikace „Bezpečnost dětí na internetu“¹²⁶ nebo studie Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci.

Sexting je aktivitou, kdy je přes internet, tedy nejen e-mailem, ale i přes téměř jakoukoli sociální platformu nebo mobilní telefon odeslána fotografie erotického nebo sexuálně explicitního charakteru druhé osobě¹²⁷. Obvykle tak u nezletilých bývá činěno s cílem získat náklonnost této osoby, nebo se přizpůsobit ve vztahu. Sextingové fotografie jsou hrozbou zejména proto, že pro svou digitální povahu mohou být dále šířeny bez vědomí osoby na nich zachycené. Vzhledem k vývoji moderních technologií může snadno dojít také k okamžitému přenesení fotografie doručené na mobilní telefon do sítě internet. Sexting se do širšího povědomí veřejnosti dostal zejména poté, co byl zadržen hacker Christopher Chaney, který se naboural do mobilních telefonů a e-mailových schránek známých amerických hereček a jejich sextingové fotografie rozšířil po internetu. V dubnu 2012 se hacker přiznal k devíti z více než dvaceti bodů obžaloby. Chaney, který se naboural do e-mailových schránek více než 50ti veřejně činných osob může být odsouzen až k 60 letům odnětí svobody a pokutě ve výši 2,25 mil. dolarů.^{128, 129} K podobnému případu došlo v mnohem širším měřítku také v České republice. Neznámý pachatel odcizil v roce 2008 přes tisíc intimních fotografií ze seznamovacího portálu pro mladé – Libimseti.cz. Galerie s intimními materiály byly sice chráněny heslem, avšak hacker využil zastaralé a nedokonalé ochrany. Fotky jsou nyní volně k dispozici na internetu, dokonce se objevily v upravené verzi jako

¹²⁶ ECKERTO VÁ, L.; DOČEKAL, D.; *Bezpečnost dětí na internetu*, Computer Press, Brno, 2013. ISBN: 978-80-251-3804-5

¹²⁷ Jako sexting je někdy označována také sexuálně laděná sebe prezentace uživatelů internetu, např. zasílání erotických fotografií na vlastní profil na sociální síti. S tímto slučováním se ale autorka práce neztotožňuje a považuje jej z právního hlediska za zavádějící. To je ostatně i z hlediska terminologického, neboť pojem se vyvinul z ang. výrazu „texting“ označujícího výhradně zasílání SMS zpráv, tedy zpráv od jedné fyzické osoby určených jiné, zcela individualizované a předem známé fyzické osobě.

¹²⁸ MYERS, A., Celeb hacker Christopher Chaney says getting into emails was easy [online] *Daily Caller*. 24. duben 2012 [cit. 2012-12-09]. Dostupný z WWW: <<http://dailycaller.com/2012/04/26/celeb-hacker-christopher-chaney-says-getting-into-emails-was-easy/#ixzz2FllwyJXI>>

¹²⁹ Tento případ ilustruje nebezpečí propojenosti uživatelů sítě. Po překonání zajištění jedné schránky měl hacker, aniž by byl odhalen, přístup ke kontaktům na další osoby. Mimo to také došlo k zásahu do osobnostních práv nejen osoby, jejíž schránka byla otevřena, ale také každé osoby, s níž či o níž vedla soukromou korespondenci. Tomuto případu byla přikládána velká pozornost také z ekonomického hlediska. Muži se totiž podařilo získat citlivé informace, jako jsou podrobnosti utajovaného rozvodového řízení nebo sexuální orientace veřejně známých osob. Zveřejnění těchto dat by mělo rozsáhlé finanční následky pro řadu dalších subjektů spolupracujících se subjekty informací.

dvacetiminutové video.¹³⁰ Oba předchozí příklady neuvádí typickou formu zneužití sextingu, ale poskytují jasnější představu, jak o povaze sextingové zprávy, tak o možném rozsahu následků jejího rozšíření. Typicky však bude sextingová zpráva zneužita jejím adresátem. Zpráva může být nejen šířena po internetu, ale také je nezřídka zneužita k odcizení identity, resp. např. založení falešného profilu odesilatele na sociální síti nebo seznamce, kde je fotografie obvykle doplněna i o adresátu známé osobní, v nejhorší variantě kontaktní, údaje a difamační či provokativní sdělení. Totožnost osoby profil zakládající se neověřuje. Osoba si tak nemusí být vědoma, že jí byl takovýto profil založen, a že jejím jménem případně je i komunikováno. Situace je o to složitější, že původní fotografii zaslal subjekt informace adresátovi dobrovolně sám, a to navíc v digitální podobě, a často dokonce s vědomím, že fotografii zasílá na smartphon.

Sexting nezletilých je závažnou problematikou se složitým právním řešením. O prosazení zvláštního sextingového federálního zákona se od roku 2009 snaží skupina právníků z organizace WiredSafety. Sexting je v USA upraven pouze státními zákony, které se různí. Např. ve státě Pennsylvania může být nezletilý za zaslání sextingové fotografie obviněn z šíření dětské pornografie. V České republice je většina případů řešena buď samoregulací PSIS, kde byla fotografie zveřejněna, případně trestním právem. Problém spočívá mimo jiné v nejednotné definici nezletilé osoby v souvislosti s pornografií. Protiprávního jednání se sice nezletilé dítě starší 15ti let nedopouští sexuální aktivitou, ale jakýmkoli záznam takové aktivity je považován za dětskou pornografii, protože za nezletilé dítě zákon označuje osobu mladší 18ti let. Za tu jsou považovány také specifické záznamy obnažené nezletilé osoby. Jakékoli zaslání sextingové zprávy osobou mladší 18ti let, tak také v České republice může být klasifikováno jako šíření dětské pornografie.¹³¹ Je však potřeba upozornit, že vzhledem k jazykovému výkladu ustanovení § 192 TZ se lze domnívat, že zákonodárce si kladl za cíl postihnout další osoby a dítě samotné by tak jako pořizovatel sextingové fotografie postiženo být nemělo. Co se partnera týče, ten by se sice přechováváním nebo dokonce dalším šířením takové fotografie jednání kvalifikovatelného podle § 192 dopouštěl, ale

¹³⁰ Co je to sexting? [online] *Projekt Nebud' obět'* [cit. 2012-11-23]. Dostupný z WWW: <<http://www.nebudobet.cz/?page=sexting>>

¹³¹ Více Sexting a právo [online] *Projekt Nebud' obět'* [cit. 2012-11-23]. Dostupný z WWW: <<http://www.sexting.cz/>>

především co se první varianty týče, by byla těžko prokazatelná nebezpečnost činu pro společnost.

Z výzkumu Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci (dále také jen jako Centrum), který provedlo Centrum v roce 2010, vyplynulo, že více než 10% dětí odeslalo alespoň jednu další osobě svou vlastní sexuálně laděnou fotografii nebo videozáznam. Více než 9% nezletilých takovou fotografii sdílí na internetu.¹³² Ačkoli si podle dat ze stejného výzkumu většina nezletilých uvědomuje rizika této činnosti, sexting je stále rozšiřujícím se trendem, který může mít tragické následky. Sexting může být také spojen s vydíráním¹³³. Z českých případů lze připomenout sextingové vydírání nezletilé dívky, na kterou po rozchodu činil nátlak bývalý přítel právě výhružkami zveřejněním jejích sextingových fotografií. Dívka oznámila vydírání na kontaktní lince PSIS Seznam.cz se žádostí o vydání hesla k mladíkově e-mailové schránce. To jí vydáno být nemohlo. Dívka spáchala sebevraždu.¹³⁴ Případy sebevražd jako následku sextingu a následného vydírání nebo šikany jsou známy jak z evropských zemí, tak z USA, kde bylo nejmladší známé oběti 13 let.

Sexting je velice rozšířen nejen jako společenský trend při budování vztahů mezi nezletilými, ale také jako prostředek výdělečné činnosti nezletilých. V České republice stále více nezletilých dětí využívá v kyberprostoru seznamek a chatových fór k šíření těchto vlastních materiálů a k prostituci. Děti dokonce samy iniciují kontakt s potenciálním zákazníkem. Za úplatu zasílají své obnažené fotografie, kterými je následně ale může kontaktovaná osoba vydírat a přimět je k setkání s jasným vyústěním. Jeden z mužů, který takové fotografie získal přímo od dívek nebo od dalších uživatelů internetové skupiny, kde se setkávají pedofilové, pro projekt „Seznam se bezpečně“¹³⁵ vypověděl, že nejmladší dívce, od které takto fotografií získal, bylo 9 let. Platby probíhají dobíjením kreditu telefonu nezletilého zákazníkem na dálku. Stejným

¹³² Sexting v České republice [online]. *Projekt Nebud' oběť* [cit. 2012-11-23]. Dostupný z WWW: <<http://www.sexting.cz/>>

¹³³ Jak tomu bylo v případě Amandy Todd nebo v popisovaném případě z České republiky

¹³⁴ KOŽÍŠEK, M., Seznam se bezpečně [dokument]. *Seznam.cz* [cit. 2012-10-18]. 12:20 -15:00m. Dostupný také z WWW: <<http://www.youtube.com/watch?v=9bDFe5as5HA>>

¹³⁵ Seznam se bezpečně [dokument]. *Seznam.cz* [cit. 2012-10-18]. Dostupný také z WWW: <<http://www.seznamsebezpecne.cz/>>

způsobem probíhá také stále častější nezávislá dětská prostituce, kde se děti nabízejí na chatových fórech¹³⁶.

3.2. Kyberšikana

Kyberšikana může postihnout každé dítě. Mnoho studií dokazuje, že oběťmi šikany se zdaleka nestávají jen děti slabé či nějakým způsobem společensky znevýhodněné. Za šikanou může stát závist, pomsta nebo nedorozumění. Kyberšikaně se věnuje např. příručka „Rizika virtuální komunikace“¹³⁷. Od kyberšikany je potřeba oddělit aktivitu známou jako trolling¹³⁸, která je velice oblíbená, jak mezi dospělým, tak ale zejména mezi nezletilými. Na tomto místě je potřeba ji zmínit, protože, ačkoli nemusí působit jako přímý mezistupeň k šikaně, posouvá nejen pozitivním způsobem vztah nezletilých ke svobodě slova, sebevyjádření, veřejné diskuzi a budování vlastního názoru, ale také může způsobit jejich znečitlivění vůči sociálním normám chování, komunikace, nadsázky a úcty k člověku. V závislosti na svém obsahu může trolling také být označen za šíření difamační informací. Otázkou je, jak by k individuálním případům přistupoval soud, resp. jak by vyhodnotil argument, že se jedná o nadsázku, jejíž nevážnost je digital natives, na rozdíl od běžné fyzické osoby dobře známá a zřejmá po prvním přečtení.

3.2.1. Případová studie *U. S. v. Drew*

Jedním z celosvětově nejznámějších případů kyberšikany, který vedl ke změně v přístupu k této problematice v USA, byl spor *U. S. v. Drew*¹³⁹. Žákyně sedmé třídy Megan Meier přestoupila na novou školu a přerušila kontakty s někdejší nejlepší kamarádkou ze sousedství. Matka této kamarádky, Lori Drew, se údajně obávala, že Megan Meier by mohla o její dceři rozšiřovat nelichotivé informace¹⁴⁰. Dospělá žena proto založila na sociální síti MySpace falešný profil, prostřednictvím kterého

¹³⁶ Seznam se bezpečně [dokument]. *Seznam.cz* [cit. 2012-10-18]. Dostupný také z WWW: <<http://www.seznamsebezpecne.cz/>>

¹³⁷ KOPECKÝ, K.; KREJČÍ, V.: *Rizika virtuální komunikace*, (2010), NET University, ISBN: 978-80-254-7866-0

¹³⁸ Trolling je zasílání provokativních, hanlivých nebo irelevantních příspěvků k citlivým tématům účastníkem online diskusních fór, chatů či blogů. Hlavním smyslem této činnosti je vyprovokovat ostatní uživatele k vytožené emotivní odezvě. Zdroj: *PCMAG.com* a *Wikipedie: Otevřená encyklopedie*, Dostupný z WWW: <http://www.pcmag.com/encyclopedia_term/0,2542,t=trolling&i=53181,00.asp#>

¹³⁹ *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)

¹⁴⁰ *United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009)

vystupovala a komunikovala jako šestnáctiletý chlapec. MySpace sice ve svých Podmínkách užívání zakazuje tvorbu falešných profilů, kontrolní systém však chybí, a tak tento zákaz, tak jako v mnoha jiných případech regulace uživatelství sociálních sítí, slouží především jako liberační pojistka pro PSIS. Lori Drew vyhledala Megan Meier pod falešnou identitou jako Josh, spřátelila se s ní, začala jí lichotit a ucházet se o ni. Nezletilá dívka se do chlapce zamilovala. V tu chvíli se tón zpráv změnil a Lori Drew začala na dívku útočit a bezdůvodně ji šikanovat. Jako Josh získala Lori Drew také mnoho dalších dětí a spolužáků Megan jako MySpace přátele a přiměla je, aby se k útočné kampani proti dívce připojili. Nakonec napsala Megan jménem neexistujícího chlapce, že svět by na tom byl bez ní lépe. Zamilovaná dívka se po poslední útočné zprávě oběsila v šatně dětského pokoje¹⁴¹.

Už samotné okolnosti případu jsou alarmující a poukazují na nedostatky právní regulace ochrany osobnostních práv nezletilých na internetu v USA. Když vyšla najevo pravá identita Joshe - Lori Drew, nemohl státní zástupce na ženu podat obžalobu. Ve státě Missouri neporušila žádný zákon – obtěžování je trestné pouze písemnou nebo telefonní komunikací, a federální úprava kyberšikany v USA neexistuje. Ani judikatura zde nepomohla. Nakonec se podařilo najít alternativu, prostřednictvím které bylo možné podčlenit jednání Drew pod konkrétní skutkovou podstatu. Tím, že založila profil pod falešným jménem, porušila podmínky užívání služby poskytované MySpace. Protože MySpace má hlavní sídlo ve státě Kalifornie, bylo možné tvrdit, že čin byl spáchán v Kalifornii, ačkoliv byla jak Drew, tak i oběť ze státu Missouri¹⁴². Drew byla obžalována z porušení Zákona o počítačovém podvodu a zneužití dat, který zakazuje přístup k počítači za překročení autorizace k užití za účelem spáchání zločinu, přečinu nebo jiného porušení zákona. Vzhledem k tomu, že však nejzásadnější zprávu, která vedla k dívčině sebevraždě, zaslala Drew prostřednictvím jiné internetové služby, musela porota vzít v úvahu pouze její přečin vůči porušení Podmínek užívání služby. Drew nemohla být odsouzena za kyberšikanu ani napomáhání k sebevraždě. Mimoto Electronic Frontier Foundation (EFF), nezisková organizace zabývající se právy uživatelů internetu vypracovala odborný právní posudek na podporu Drew: Pokud by

¹⁴¹ MAAG, CH. A Hoax Turned Fatal Draws Anger but No Charge [online] *The New York Times*. 28. listopad, 2007 [cit.-2012-07-28]. Dostupný z WWW:

<http://www.nytimes.com/2007/11/28/us/28hoax.html?pagewanted=print&_r=0>

¹⁴² ANDREWS, Lori B.; *I know who you are and I saw what you did: social network and the death of privacy*, Free Press, 2012. s. 99. ISBN 978-1-4516-5051-8

byla odsouzena za pouhé porušení Podmínek užívání, dopouštěli by se přečinu např. všichni, kdo své názory na internetu projevují anonymně, což by mohlo mít zásadní dopad na základní fungování demokratické společnosti, a ve svém důsledku také na odhalování trestné činnosti. Argumentace EFF byla zjednodušeně prezentována jejími odpůrci v tom smyslu, že nemůže být trestné neuvádět o sobě pravdivé informace na internetu, protože je o sobě na internetu neuvádí mnoho uživatelů. Pro srovnání je na místě uvést, že, jak vyplynulo z mezinárodního průzkumu UltraYou, nepravdivé informace o sobě na sociálních sítích jen v České republice udává 59% mužů a 56% žen¹⁴³. Cílem EFF bylo však nejen vyhnout se nechtěné kriminalizaci toho, kdo na internetové seznamce udá nižší věk. Pokud by totiž bylo trestné porušit smluvní ujednání (Podmínky užívání) s PSIS, jehož detaily nejsou uživatelům často známy, a ke kterému se zavazují zivatele pouhou registrací, byly by limity trestnosti pouze v diskreci PSISs.

Soud se přiklonil k názoru EFF a Drew zprostil obžaloby. Na základě rozhodnutí soudu ve věci *U.S. v. Drew* přijalo několik států USA zákony na ochranu před kyberšikanou. Žádný z nich však neposkytuje nezletilým plnohodnotnou právní ochranu před kyberšikanou a zásahy do soukromí a dalších osobnostních práv.

3.2.2. Případová studie: *New Jersey v. Ravi*

Případ Tylera Clementiho se stal mezi lety 2010 – 2012 ve Spojených státech amerických mimořádně důležitým soudním sporem, který rozpoutal vlnu aktivizmu v otázkách kyberšikany. Talentovaný student Rudgersovy univerzity spáchal sebevraždu, jež byla dávána do souvislosti s incidentem, který ji předcházel. Tyler Clementi požádal svého spolubydlicího na koleji Dharuma Raviho, aby mohl v soukromí použít jejich společný pokoj pro osobní návštěvu. Ravi nainstaloval v pokoji bez vědomí Clementiho na svůj počítač internetový přenos webkamerou se vzdáleným přístupem (technologicky zcela dostupný, běžný, dětmi často užívaný a v některých případech těžko pozorovatelný proces, který je umožňován v současnosti v podstatě každým počítačem). Ravi se poté ke svému počítači připojil na videochatu z pokoje spolužačky, a přes veřejně dostupné elektronické zprávy na svém profilu na síti Twitter

¹⁴³ SVOBPODA, P.; Průzkum Intel: Na sociálních sítích vytváříme své „lepší já“ [online], *UltraYou, Intel* [cit. 2012-11-05]. Dostupný také z WWW: <<http://www.playzone.cz/clanky/pruzkum-intel-na-socialnich-sitich-vytvarime-sve-lepsi-ja>>

informoval spolužáky a veřejnost, že právě viděl svého spolubydlícího intimně se stýkat s mužem. Tyler Clementi se později o umístění skryté kamery dozvěděl a přečetl také reakce spolužáků na veřejné sociální síti Twitter. Internetové komentáře se vyznačovaly netolerancí a homofobii. Clementi se také na sociální síti Facebook svěřil se svým rozhořčením a zoufalstvím nad incidentem. Ravi se pokusil sledovat homosexuálního spolubydlícího ještě při jedné příležitosti, kdy opět veřejně informoval o přesné hodině, kdy má schůzka proběhnout, a vyzval studenty školy, aby oba muže tajně sledovali s ním. Tyler Clementi nyní sledování zabránil, podal na Raviho stížnost na kolejní správu, a požádal o výměnu pokoje. Dříve, než na tuto bylo reflektováno, mladík 22. září 2010 spáchal sebevraždu. Jedná se o jeden z nemála případů, kdy byl mladý člověk šikanován pro svou sexuální orientaci. Vzhledem k tématu této práce je na místě dále připomenout případ z roku 2010, kdy spáchal sebevraždu teprve 13ti-letý Seth Walsh z Kalifornie, který byl obětí šikany a kyberšikany ze stejného důvodu. Tyto jsou pouze jedněmi z mnoha případů tzv. bullycide, tedy sebevraždy způsobené šikanou.

Na základě množících se podobných případů se rozvinula veřejná diskuze o tom, jak by mělo právo posuzovat jednání osoby, která šikanou dožene jiného člověka k sebevraždě. Složitost současné právní situace nejen v USA ilustruje právě případ Tylera Clementiho. Když se soud začal případem zabývat, jasně si jako cíl vytyčil striktně oddělit jednání Dharuma Raviho od následné sebevraždy Tylera Clementiho, a v tomto smyslu soud také instruoval porotu. Dharum Ravi, kterému kvůli indickému občanství hrozilo mimo jiné také vyhoštění ze země, byl obžalován ze zásahu do soukromí, z manipulace s důkazy, ze spáchání trestného činu s motivem předpojatosti vůči skupině, resp. zde s motivem předpojatosti proti homosexualitě. Ekvivalentem by v českém právu byl nejbližší § 356 odst. 3 písm. a) TZ¹⁴⁴. V tomto směru byl také obžalován z tzv. *hate speech*, tedy projevu, který je negativně zaměřen proti rasové nebo jiné skupině obyvatel a tak není chráněn právem na svobodu projevu.

Státní zastupitelství se pokoušelo prokázat, že Raviho čin byl motivován Clementiho homosexualitou. Postup státního zastupitelství ve věci byl však kritizován pro údajnou snahu přizpůsobit právo mimořádností okolností případu. Právnická veřejnost vedla debatu o tom, zda právě zmíněná nutnost oddělit smrt mladík od

¹⁴⁴ Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem

jednání, která k ní mohla vést, vedla zastupitelství k silnému zájmu na prokázání co nejzávažnějších dalších protiprávních jednání, která by tak měla „suplovat“ pro Raviho trest za Clementiho smrt. Jednalo se zároveň o mimořádně násilnou formu zasahování do intimní sféry osobnosti prostřednictvím technologií, se kterým se právo mezi mládeží globálně neúspěšně potýká již mnoho let, a tak byl případ vnímán veřejností velice intenzivně.

Ravi byl nakonec porotou shledán vinným ve všech 15 bodech obžaloby, včetně několika týkajících se činu motivovaného předpojatostí vůči určité skupině. Byl odsouzen pouze k 30 dnům v nápravném zařízení a podmíněčnému trestu odněti svobody, obecně prospěšným pracím a výchovným konzultacím na téma kybernetické šikany.

Jeden z ústředních problémů kybernetických zásahů ilustruje také SMS zpráva, kterou Dharum Ravi zaslal Tyleru Clementi poté, co Clementi na sociální síti informoval veřejnost, že se chystá skočit z mostu: „(...) Nechci, aby tvůj první rok na univerzitě byl zničený na základě drobného nedorozumění (...).“¹⁴⁵ Základním problémem je právě chlad zasahujícího a jeho ignorance k závažnosti zásahu do soukromí Tylera Clementiho. „Někteří odborníci míní, že mediální prostředí zahrnující mimo jiné i různé reality show využívající princip skrytých kamer otupuje schopnost mladých lidí poznat škodlivý dopad svých činů. Nedávná studie Michiganské univerzity například zjistila, že schopnost empatie u vysokoškoláků klesla v letech 1979 až 2009 o zhruba 40%, přičemž největší propad nastal po roce 2000.“¹⁴⁶

Rodina Tylera Clementi se rozhodla nepodat občanskoprávní žalobu. Od podzimního semestru 2012 vešel v platnost v New Jersey nový Zákon Tylera Clementiho pro vysokoškolské instituce proti obtěžování¹⁴⁷, který mimo jiné, ukládá školám zřídit zvláštní funkci dohlížející na případné pokusy o obtěžování a ustavující obtěžování, nebo šikanu a podobné negativní aktivity, a to i v kyberprostoru, jako důvod pro okamžité pozastavení studia nebo vyloučení.

¹⁴⁵ MUSKAL, M.; Rutgers suicide: Tyler Clementi's parents won't sue in webcam case [online] *Los Angeles Times*. 5. říjen 2012 [cit. 2012-10-09]. Dostupný z WWW:

<<http://articles.latimes.com/2012/oct/05/nation/la-na-nn-clementi-parents-wont-sue-rutgers-20121005>>

¹⁴⁶ Dostupný z WWW: <http://zpravy.idnes.cz/usa-resi-sebevrazdu-studenta-jehoz-sex-spoluzaci-natocili-a-dali-na-internet-1wf-/zahranicni.aspx?c=A101003_113248_zahranicni_ipl>

¹⁴⁷ USA. Tyler Clementi Higher Education Anti-Harassment Act

Problémem je opět jak sektorální povaha amerického práva, tak fakt, že byl zákon přijat teprve na základě tragédie, ke které došlo. Na stejném pozadí byl ve Spojených státech již přijat také Zákon o registraci osob odsouzených za sexuálně motivované zločiny, tzv. Megan's Law, který byl přijat nejprve v New Jersey jako reakce na případ znásilnění a vraždy sedmileté Megan Kanka¹⁴⁸ nebo tzv. Alicia Law, zákon, který upravuje financování a zajištění nutné infrastruktury pro provoz dvou národních center pro boj s internetovou kriminalitou cílenou na děti - Internet Crimes Against Children (ICAC). Tento zákon byl přijat v roce 2008 ve státě Virginia a iniciátorkou jeho prosazení byla Alicia Kozakiewicz, která se stala obětí cybergroomingu, když byla vězněna a sexuálně zneužívána pedofilem, který se na internetu původně vydával za čtrnáctiletou dívku.¹⁴⁹

3.3. Zasahování do soukromí

Na rozhraní kyberšikany a difamace stojí zasahování do soukromí, které může být součástí kyberšikany a být vyplněno difamačním obsahem. Nejčastějšími příklady zasahování do soukromí rozšířenými mezi nezletilými dětmi je sexting a kopírování a další distribuce těchto fotografií či fotografií z alb na sociálních sítích bez vědomí osoby na fotografii, v některých případech za účelem dosažení zisku z prodeje reklamního prostoru, jak je tomu např. na internetových stránkách Lamebook, shromažďujících ponižující záznamy z Facebooku nebo studentská báze CollegeHumor, kde se pak mohou objevit difamační fotografie osob bez jejich vědomí a přesáhnout tak zásadně původně zamýšlený nebo předpokladatelný okruh osob, které mohou fotografie vidět. Pokud je např. fotografie pořízena na rodinném večírku, nebude její subjekt předpokládat, že bude, navíc ve zcela jiném kontextu dosažitelná celosvětově.

¹⁴⁸ Tento právní předpis uzákoňuje registr odsouzených za sexuálními zločiny v Kalifornii. Jedná se o veřejně přístupný registr, na jehož základě mohou rodiče ověřit, zda v okolí jejich bydliště nežije nebo nepracuje odsouzený sexuální zločinec. Společně s detailním výpisem z jeho rejstříku trestů, zejména dat o povaze trestného činu, kterého se měl dopustit, se na veřejných webových stránkách zobrazí také fotografie a popis propuštěného, PSČ jeho bydliště a zaměstnání, a mapka jeho takto odvozeného možného pohybu a případně jiné identifikátory. Podobný registr existuje také ve Velké Británii, kde vzbudil při svém zavedení debaty odborníků zabývajících se právem na soukromí.

¹⁴⁹ Zde se vracíme k právně složité problematice velice aktuální v posledních letech v České republice. Alicia Kozakiewicz totiž později v průběhu kybernetického přátelství zjistila, pravou identitu muže. Nezletilá s tímto dobrovolně dále udržovala virtuální kontakt, a když s ní začal predátor komunikovat intimní témata, reagovala také na tuto konverzaci. Fakt, že případy zneužití jsou často komplikované a vztahují se pochopitelně i na situace, kdy manipulované dítě ke svému ohrožení přispělo ve velké míře samo, je diskutován jen omezeně.

3.3.1. Případová studie: *Catsouras v. DCHP*¹⁵⁰

Případem, který ilustruje zásadní zásah do soukromí v kyberprostoru je případ Nikky Catsouras, dívky, která zemřela při autonehodě poté, co ve vysoké rychlosti narazila do sloupu mýtné brány. Fotografie pořízené dálniční policií byly zaslány do počítače na policejní centrálu. Dispečer Aaron Reich se rozhodl několik snímků zničeného automobilu a zohavených ostatků dívky zaslat své rodině a přátelům. Později tvrdil, že tak činil ve snaze varovat před následky nezodpovědného chování za volantem. Fotografie byly pro svou mimořádnou drastičnost přeposílány dalším uživatelům a během krátké doby byly uloženy a dosažitelné na nejméně 2 500 různých internetových stránkách. Také kontext, do kterého byly fotografie zasazeny, měl potenciál mimořádně hlubokého osobnostního zásahu do osobnostních práv zesnulé i pozůstalých, neboť mnoho ze stránek, které fotografie převzaly, se zabývalo výhradně zobrazováními pornografie a fotografií zachycujících smrt či utrpení. Na sociální síti MySpace byl otevřen falešný profil dívky s difamačními komentáři a vyobrazeními detailů fotografií jejího zohaveného těla. Tato sociální síť je veřejná a profily, jak již víme, zde bylo možné založit bez zpětné kontroly. Pouhých několik dní po smrti dívky obdržel její otec pracovní e-mail, který obsahoval policejní fotografii dcery, kterou do té doby neviděl spolu s komentářem vyznívajícím jako pozdrav dcery, která se raduje, že stále žije.¹⁵¹ Teprve tak otec oběti zjistil, že internet je zahlcen fotografiemi, jako je tato. Otec dívky byl nucen změnit zaměstnání za méně placené místo, kde ale nemusel užívat internet. Sestrám dcery rodiče zakázali používat internet. Spolužáci mladší z dcer ji však vyhrožovali, že fotografie vytisknou a nalepí na její školní skříňku. Proto byla rodina nucena odepsat dceru ze školy a vyučovat ji doma.¹⁵² Rodiče se postupně spojili s většinou stránek, které fotografie převzaly, a požadovali stažení fotografií. Ve valné většině případů však provozovatelé stránek odmítli fotografie stáhnout, odvolává se na právo Prvního dodatku.

Teprve advokátní kanceláři se prostřednictvím řady předžalobních výzev podařilo docílit stažení fotografií z větších a známějších serverů. Rodiče Nikky Catsouras se rozhodli zažalovat jak oddělení dálniční policie California Highway Patrol

¹⁵⁰ *Department of California Highway Patrol (dále také jen jako CHP)*

¹⁵¹ BENNETT, J; A Tragedy That Won't Fade Away [online] *NEWSWEEK*, April 25, 2009 [cit. 2012-08-12]. Dostupný z WWW: <<http://www.newsweek.com/2009/04/24/a-tragedy-that-won-t-fade-away.html>>

¹⁵² AVILA, J. et al. A Family Nightmare [online] *abc News* 16. Listopad 2007 [cit. 2012-08-12]. Dostupný z WWW: <<http://abcnews.go.com/TheLaw/story?id=3872556&page=1>>

(CHP) tak dva policejní dispečery, kteří fotografie dcery sdíleli. V žalobě právní zástupce rodiny uvádí, že se dopustili vpádu do soukromí oběti a její rodiny, a že rodině záměrně způsobili psychickou újmu. Prvoinstanční soud žalobu jako nepodloženou zamítl. Odvolací soud ale dal zapravdu žalobcům. V odůvodnění rozhodnutí zejména uvedl, že právo na to být informován se na tento případ nevztahuje a že osoby fotografie sdílející měly předpokládat, že se stanou předmětem morbidního zájmu senzacechtivé společnosti¹⁵³. Rodina s žalobou však nakonec uspěla pouze z důvodu, že v Kalifornii je nezákonně „vynášet“ fotografie z pitvy a analogicky se tak za porušení pracovních povinností podobného rázu dalo považovat i jednání policejních dispečerů. V lednu 2012 došlo mezi pozůstalou rodinou a CHP k mimosoudnímu vyrovnání. Fotografie jsou na internetu stále dostupné, a to jak na mnoha serverech, tak prostřednictvím vyhledávače Google.

3.4. Difamace

V kyberprostoru jsou velmi často tato jednání součástí kyberšikany. V této práci se věnujeme mnoha takovým případům. Také osamocené difamační zásahy jsou na internetu velice časté. Právě pro jejich snadnost, četnost a především jejich anonymitu, je jejich právní postih neskutčný. Proti ojedinělým zásahům v podobě difamačních komentářů ve vláknu diskuze apod. se lze v současné době v zásadě bránit pouze kontaktováním příslušného PSIS se žádostí o jejich stažení¹⁵⁴. Zajímavé srovnání nabízí článek Stevena Jamese, který poskytuje analýzu připravovaného nového britského (Anti)difamačního zákona ve světle aktuální evropské judikatury zásahu do práva na občanskou čest a lidskou důstojnost. Návrh zákona má za cíl zajistit vyšší úroveň ochrany PSISs, a zajistit jednotnost v budoucí rozhodovací praxi soudů. Z pohledu amerického práva je šíření difamačních informací jednáním, které zahrnuje šíření nepravdivé informace osobám jiným, než je ta, které se týkají. Informace musí být dále způsobilá přivodit subjektu informace újmu.

¹⁵³ *Catsouras v. Department of California Highway Patrol*, 181 Cal. App. 4th 875 (Cal. Ct. App 2010)

¹⁵⁴ Srov. rozsudek Vrchního soudu v Praze ze dne 2. 3. 2011, č. j. 3 Cmo 197/2010-8. Více: ZAHRADNÍČEK, J.; 88471. Odpovědnost poskytovatelů služeb informační společnosti - několik postřehů k závěrům Vrchního soudu v Praze v kauze „PROLUX“ [online] *EPrávo*, 14.2. 2013 [cit. 2013-03-02]. Dostupný z WWW: <<http://www.epravo.cz/top/clanky/odpovednost-poskytovatele-sluzeb-informacni-spolecnosti-nekolik-postrehu-k-zaverum-vrchniho-soudu-v-praze-v-kauze-prolux-88471.html>>

Z pohledu českého práva je zajímavý přístup amerických soudů k finanční satisfakci žalobce. Náhrada škody nebyla poškozenému pouze výjimečně přiznána, pokud také nevyžadoval stažení difamačního obsahu z internetu¹⁵⁵. Ačkoli právní odpovědnost PSIS je podle amerického práva, ač z jiného důvodu než z jakého je tomu v zemích EU, vyloučena, i zde se nemusí jednat o ochranu bezvýhradní. I přes výjimku ustanovenou § 230 Zákona o mravnosti (elektronických) komunikací (Communication Decency Act)¹⁵⁶ i zde již soud¹⁵⁷ rozhodoval ve prospěch žalobce o právní odpovědnosti správce komunikace¹⁵⁸ za difamační obsah. Žalobu je obvykle možné podat v rámci promlčecí doby nastavené jednotlivými státy. Tato je např. v Kalifornii pouze jeden rok.

3.4.1. Zásah do pozitivní složky práva na informační sebeurčení nezletilé osoby - případová studie *Alexa Dell*

Zásahu do soukromí nebo difamace, kde jedno zpravidla vede v kyberprostoru ke druhému, se mohou dopustit také rodiče, a to i v situacích, kdy se na dítě snaží výchovně působit. Důkazem je nedávný případ Alexy Dell, dcery Michaela Della, generálního ředitele společnosti Dell, a její soukromé fotografie, kterou pořídila na svůj smartphone pomocí aplikace Instagram¹⁵⁹. Takové fotografie sice mohou být sdíleny jen s omezenou skupinou osob, ale mohou být také veřejné a také je lze dále sdílet např. se sociální sítí Facebook nebo Twitter. S tou Alexa Dell své fotografie a informace o životě svém a své rodiny bez vědomí otce sdílela.

Dvojice podnikatelů založila internetovou stránku „Bohaté děti na Instagramu“ („Rich Kids of Instagram“), s podtitulem „Mají daleko víc peněz, než ty, a tohle s nimi dělají“¹⁶⁰, kde uveřejňuje překopírované fotografie uživatelů aplikace Instagram nebo Twitter, často bez vědomí jejich pořizovatele nebo/a subjektu/ů na nich zobrazených. Klíčem pro výběr fotografií je, zda jsou na nich zobrazeni převážně nezletilí uživatelé

¹⁵⁵ Např. *Cannon v. Mathis*, S02G0361 (Ga. Sup. Ct., Nov. 25, 2002)

¹⁵⁶ Section 230 of Title 47 of the United States Code (47 USC § 230)

¹⁵⁷ Ačkoli toto rozhodnutí bylo posléze zrušeno Nejvyšším soudem státu Kalifornie

¹⁵⁸ *Stephen J. Barrett, et al. v. Ilena Rosenthal*, S122953, 40 Cal.4th 33 (Cal. Sup. Ct., November 20, 2006)

¹⁵⁹ Instagram je velmi rozšířená fotografická aplikace. Původně se jednalo o aplikaci, po jejíž instalaci mohl majitel smartphonu pořizovat umělecké fotografie prostřednictvím zajímavých filtrů a funkcí. Vzhledem k rozšířenosti aplikace Instagram rozhodla koupit společnost Facebook. Po změně vlastníka bylo možné aplikaci užívat pouze, pokud si uživatel smartphonu založil profil na internetové stránce Instagram, ekvivalentu sociální sítě s prvky uložiště-sociální sítě pro sdílení fotografií jako je např. Flickr.

¹⁶⁰ Rich kids of Instagram. Dostupný z WWW: <<http://richkidsof Instagram.tumblr.com/page/4>>

z velmi bohatých rodin, dávající provokativně na odív luxus, kterému se oddávají. Tyto fotografie kdokoli může anonymně prohlížet, kopírovat a dále s nimi nakládat.

Nedávný rozsudek trestního soudu v New Yorku společnosti Twitter uložil předat vyšetřovacím orgánům starší vzkazy zaslané uživatelem, který byl zapojen do protestních akcí Occupy Wall Street, které na Twitteru již nebyly dosažitelné.¹⁶¹ V odůvodnění svého rozhodnutí soud uvedl, že vzkazy na Twitteru jsou svou povahou veřejné, a proto se na ně nevztahují ustanovení Čtvrtého dodatku. Dalším rizikem služby Twitter je její povaha servisu okamžitého sdílení zpráv, to znamená, že uživatelé update, tedy aktuální informace, v podobě zprávy nebo komentované fotografie zasílají převážně přes mobilní telefon, několikrát denně, a to přímo z místa, kde se nacházejí, často i s geolokačními údaji. To bylo také základem problému s fotografiemi Alexz Dell - dcery Michaela Della, jehož majetek se odhaduje na 18 miliard dolarů. Dcera na Twitteru uváděla ve veřejném statutu nejen fotografie ilustrující nesmírné bohatství rodiny, ale také informace jako například, kde bude její maturitní večírek nebo, že je rodina na dovolené.¹⁶² Alexa Dell uveřejnila zejména fotografii, na níž označila svého nezletilého mladšího bratra. Fotografie jej zobrazovala při opulentní snídani na palubě soukromého tryskáče. V popisu fotografie autorka informovala, že je rodina právě na cestě na Fiji. Jedinou fotografií tak komukoli na internetu nejen ukázala podobu svého bratra, ale také zadala přesné informace o tom, kde se rodina bude kdy nacházet, a především, kde se nacházet nebude. Právě tato fotografie se objevila také na stránce „Rich Kids of Instagram“. Poté, co se Michael Dell dozvěděl o její existenci a následně o dceřiných aktivitách na sociální síti Twitter, kontaktoval společnost Twitter a zažádal o okamžité stažení dceřina profilu, a to z bezpečnostních důvodů. Twitter tak neprodleně učinil, a to přirozeně bez souhlasu Dellovy dcery, která profil založila. Pomineme-li autorskoprávní otázku, musíme se jistě zamyslet nad tímto jednáním z pohledu práva na ochranu osobnosti. Lze si teoreticky představit, že by nyní Alexa Dell zažalovala jak otce, tak především společnost Twitter za likvidaci svého profilu.

¹⁶¹ *People v. Hartus*, 2012 NY Slip Op 22175 [36 Misc 3d 868], Dostupný z WWW: <http://www.nycourts.gov/reporter/3dseries/2012/2012_22175.htm>

¹⁶² Na stránkách „Rich kids of Instagram“ lze pod každou fotografií nalézt také původní komentář k fotografii od uživatele, který ji uveřejnil na svém profilu např. na Twitteru, a jeho přezdívku ve formě hypertextu, který je možné rozkliknout, čímž se návštěvník stránky „Rich kids of Instagram“ dostane na Instagramový nebo Twitterový profil toho či onoho „bohatého dítěte“. Přezdívkami jsou často skutečná jména uživatelů.

Jak bylo řečeno na začátku, tato situace je typickou ukázkou řešení bezpečnostních rizik a problematiky osobnostních práv na internetu na bázi *ad hoc* rozhodnutí společností. Více se této problematice v globálním měřítku věnuje Jeffrey Rosen ve svém článku „Google's Gatekeepers“¹⁶³. Případ Alexy Dell je však z pohledu práva na ochranu osobnosti, dle názoru autorky této práce, mimořádně zajímavým předělem v tomto tradičním postupu PSISs. Je jistě pochopitelné, že uživatelka ohrožovala bezpečnost jak svou, tak celé rodiny. Jaká by však byla situace, kdyby společnost Twitter kontaktovala svobodná matka v invalidním důchodu a požádala o smazání profilu své stejně staré pohledné dcery, která uvádí, stejně jako Alexa Dell, kde bude její maturitní večírek, zasílá fotografie své 11ti-leté sestry v bikinách na zahradě domu a informuje, že po příští dva týdny bude celá rodina na dovolené? Zrušil by Twitter tak promptně i její profil? Zcela přímo řečeno: Proč je důležitější ochránit bohatou dědičku před únosem než chudou a třeba nechtěně provokativní dívku před sexuálním predátorem? Proč je možné omezit autorská práva a právo na svobodu projevu a budování sociálních vazeb jedné uživatelky ve snaze ochránit majetek její rodiny, a třeba nepřistoupit ke stejnému postupu v případě druhé? Lze nějak měřitelně vyhodnotit rizika únosu jedné dívky oproti zneužití druhé? Změnila by se situace, kdyby dívka z modelové situace bydlela v oblasti s vysokou kriminalitou a velkým počtem nahlášených sexuálních útoků? A zabýval by se vůbec těmito údaji Twitter? Autorka této práce se domnívá, že v případě Alexy Dell sledujeme moment zcela zásadní důležitosti pro vymahatelnost práva na ochranu osobnosti nezletilých v kyberprostoru. Tímto momentem je patová situace, do které se společnost Twitter dostala svým rozhodnutím zrušit profil uživateli z bezpečnostních důvodů za uvádění informací naprosto identických s těmi, které o sobě a svých rodinách uvádí milióny i mladších uživatelů služby Twitter. V souvislosti s odůvodněním v podobě potenciální hrozby nebezpečí připomeňme znovu případ *Catsouras v. Department of California Highway Patrol*. Sourozenci Nikky Catsouras byli obsahem stránek také vážně ohroženi (obsah stránek byl zřejmě dokonce závažnější než obsah profilu Alexy Dell) a přesto se Twitter rozhodl Dellovi okamžitě vyhovět, a to přesto, že se jedná o server primárně určený pro komunikaci veřejnou a uzavřením profilu byla zcela nesporně porušena mimo jiné ústavní práva z Prvního dodatku zakladatelky profilu, Alexy Dell.

¹⁶³ ROSEN, J.; Google's Gatekeepers, *The New York Times*, 30. listopad, 2008

Na příkladech bylo ilustrováno, že se tak Twitter ocitl v situaci, kdy bude teoreticky muset zrušit profil každého nezletilého uživatele potenciálně ohrožujícího svou bezpečnost či bezpečnost svých blízkých, jehož rodič o to požádá. Tím by mohl do složité situace dostat také ostatní sociální sítě operující na stejné bázi. Pokud tak Twitter neučiní, jak se také lze domnívat, bude muset přiznat, že ochránit nezletilé uživatele sociálních sítí před sebou samými, resp. před bezpečnostními riziky, jejichž existenci zrušením profilu jednoznačně přiznal, jde, ale fakticky je klíčem pro rozhodnutí o neměřitelné intenzitě hrozícího rizika vliv a postavení zainteresovaných stran. Toto přiznání by mohlo Twitter vystavit nejen tlaku médií a FTC, ale také hrozbě skupinové žaloby ze strany rodičů, jejichž děti před lupiči, sexuálními predátory a podvodníky ochráněny nebyly. Situace je o to složitější, že Alexe Dell bylo 18 let. Zajímavé je zde srovnání s přístupem společnosti Facebook, která v informaci pro rodiče uvádí, s odvoláním na platné právo, že v podobné situaci profil uživatele neodstraní.¹⁶⁴

3.4.2. Zásah do negativní složky práva na informační sebeurčení nezletilé osoby při užívání výchovných prostředků v kyberprostoru

K zásahu do osobnostních práv dítěte rodiči v souvislosti s novými technologiemi může dojít několika způsoby. Nejčastěji to bude při snaze dítě chránit preventivně. Například společnost Software4Parents a další poskytuje mnoho standardních aplikací na bázi kybernetických chův¹⁶⁵. Užití těchto může svou povahou zasahovat do osobnostních práv nezletilé osoby. Mimo extrémních případů kontroly písemností osobní povahy však v podobných případech není dobře představitelná žaloba

¹⁶⁴ „(...) Zákony na ochranu soukromí obecně nám zakazují poskytnout neoprávněný přístup osobě, která není vlastníkem účtu. Uvědomte si, že všichni uživatelé, kteří dosáhli třinácti let věku nebo jsou starší, jsou považováni za oprávněné vlastníky účtu a jsou zahrnuti do rozsahu těchto zásad.“, zdroj: Facebook pomoc pro rodiče, Dostupný z WWW: <<http://www.facebook.com/help/parents>>

¹⁶⁵ Tzv. kybernetická chůva (z ang. cyber nanny) je v tomto smyslu jakýkoli druh softwaru, který umožňuje kontrolu a/či omezování nakládání nezletilých členů domácnosti, žáků škol nebo např. uživatelů veřejných knihoven, s internetem a případně sledování jejich pohybu v kyberprostoru. Tento komplexnější princip rodičovského zámku užívají rodiče ke kontrole aktivit svých dětí na internetu. Kybernetické chůvy však mohou také představovat prostředek problematický z právního hlediska, právě s ohledem na ochranu osobnosti. Některé programy např. umožňují číst e-maily nezletilého dítěte. Zejména ve věku mezi 15-18ti lety je ovšem používání těchto zařízení právně problematické, neboť v tomto věku může být dítě schopné samo rozhodovat o zpracování svých osobních údajů, tedy i o zabezpečení internetu. Nezletilý má také ústavou zaručené právo na svobodu projevu a právo na informace a obecněji pak právo na informační sebeurčení. Tato práva mohou být užíváním kybernetických chův omezována.

na ochranu osobnosti nezletilého na rodiče. Bude tomu tak zejména s ohledem na ustanovení § 31 odst. 1 a 2 zákona č. 94/1963 Sb., zákon o rodině, upravující rodičovskou zodpovědnost a jeho práva a povinnosti spočívající v péči také o citový, rozumový a mravní vývoj dítěte, spolu s právem rodiče užít přiměřených výchovných prostředků, jakými může být v podobně výjimečných případech také přístup k internetové korespondenci dítěte.

Případy zásahu do osobnostních práv nezletilých dětí rodiči mohou mít však daleko problematičtější podobu. Jsou jimi právě výchovné prostředky v kyberprostoru. Ty spočívají v jednání, kdy rodič donutí dítě např. vystavit svou ponižující fotografii s varovným nápisem na sociální síti jako reakci na přestupek dítěte proti zásadám bezpečného zacházení s internetem¹⁶⁶ či pro jiný přestupek v chování¹⁶⁷, nebo kdy sám rodič na stránkách dítěte sděluje druhým informace o dítěti přihlášením na profil dítěte¹⁶⁸ bez jeho souhlasu či vědomí. Trestání dětí rodiči přes sociální sítě se stává oblíbeným výchovným prostředkem díky významu, jaký tyto hrají ve společenském životě dnešních dětí a mládeže. Toto jednání však vyvolává nemálo právních otázek. Rodič může jednat právě v rozporu s ustanovením § 31 odst. 2 zákona č. 94/1963 Sb., zákon o rodině, když přistoupí k výchovnému opatření, které vede k dotčení důstojnosti dítěte a může ohrozit jeho citový, v extrémních případech i mravní, vývoj. Rodič samozřejmě může jednat také v rozporu s právní úpravou ochrany osobnosti podle občanského zákoníku a dále se může dopouštět jednání v rozporu s ustanovením § 230 odst. 1 zákona č. 40/2009 Sb., trestní zákoník, pokud získá neoprávněný přístup k počítačovému systému, mimo jiné v některých případech právě využitím elektronické chůvy. Připomeňme si permanentnost informací na internet vyložených. Pokud může být v budoucnu dospělé dítě nespokojeno s přítomností svých dětských fotografií potenciálně difamačního charakteru na internetu, lze hovořit i o otázce změny poměrů, které se tato práce také věnuje.

¹⁶⁶ GOMSYN, A.; Daughter 'Begged' for Spanking Instead of Mom's Embarrassing Web Photo [online]. *abc news* 21. květen 2012 [cit. 2012-12-02]. Dostupný z WWW: <<http://abcnews.go.com/blogs/lifestyle/2012/05/daughter-begged-for-spanking-but-author-posted-embarrassing-web-photo-instead/>, Mom Disciplines Daughter With Humiliating Facebook Timeline Cover Image>

¹⁶⁷ COHEN, D.; Mom disciplines daughter with humiliating Facebook Timeline cover image [online]. *Allfacebook*, 26. duben 2012 [cit. 2012-07-21]. Dostupný z WWW: <http://allfacebook.com/cover-image-discipline_b87219>

¹⁶⁸ ROMOLINI, J.; Best Facebook update of all time, posted by a dad [online] *Shine*, 4. srpen 2011 [cit. 2012-07-20]. Dostupný z WWW: <<http://shine.yahoo.com/work-money/best-facebook-update-of-all-time-posted-by-a-dad-2520529.htm>>

Zmíněné zveřejňování fotografií dětí na internetu, a především na sociálních sítích, je samo o sobě z pohledu práva nezletilého dítěte na ochranu osobnosti sporné. Je třeba připomenout, že i děti mohou mít způsobilost vyjádřit souhlas či nesouhlas se zveřejněním své fotografie, a to dle stupně své rozumové vyspělosti. K vykládání nevhodných fotografií dětí rodiči na sociální síť dochází velmi často a děje se tak nezřídka také s uvedením dalších nevhodných či přímo nebezpečných informací. Rodič tak nemusí ohrožovat jen osobnostní práva dítěte, ale i jeho bezpečnost. Pokud by však teoreticky dítě přistoupilo k žalobě na zákonného zástupce, bude soud vyvažovat práva dítěte vůči právům rodiče za hodnocení jeho jednání v kontextu rodičovských povinností.

3.5. Dokazování v rodinném právu a Internet

Dalším příkladem problematického užívání internetu ve vztahu k nezletilým je užívání veřejného, ale i soukromého obsahu internetu při rozvodových řízeních a řízeních o svěřeni do péče. Podle průzkumu platformy Divorce Online¹⁶⁹, obsahovala více než třetina návrhů rozvod manželství ve Velké Británii slovo „Facebook“ a 81% amerických rozvodových právníků potvrdilo, že sleduje nárůst zainteresovanosti internetu a sociálních sítí ve své agendě nebo že přímo využilo důkazních prostředků získaných na internetu¹⁷⁰. Vzhledem k možnosti snadné manipulace takových důkazů a relativní problematičnosti jejich hodnocení soudem, tak lze uvažovat o zásahu do práva na rodinný život nezletilého dítěte v případě navržení a provedení takového důkazu, který by byl zmanipulován..

V České republice není doposud praxe předkládání podobného důkazního materiálu zcela běžná, ale pokud se jedná o veřejně přístupná data, nebrání nic tomu, aby navržený takové důkazní prostředky byly. Jedna ze stran může např. navrhnout důkaz fotografií, která byla umístěna do virtuálního alba na sociální síti. Může se jednat o fotografii prokazující jakoukoli okolnost stěžující postavení strany od vyššího než uváděného příjmu (př. fotografie s drahým automobilem, na exotické dovolené atp.)

¹⁶⁹ Alarming increase in Facebook related divorces in 2011 [online] *Divorce. Online Blog.*, 28. prosinec, 2011 [cit. 2012-11-02]. Dostupný z WWW: <<http://blog.divorce-online.co.uk/?p=2338>>

¹⁷⁰ Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers [online] *American Academy of Matrimonial Lawyers*, 10. únor, 2010 [cit. 2012-11-02]. Dostupný z WWW: <<http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social-networking-evidence-says-survey->>>

přes životní styl neslučující se s péčí o nezletilého nebo zanedbání rodičovských povinností, až po tvrzený alkoholismus.

Z praktického hlediska však provádění elektronických důkazů a zejména jejich hodnocení může pro soudy představovat nesnadný úkol. S důkazem mohlo být manipulováno po jeho získání. Proto je nutná spolupráce odborných znalců, což ale proces prodlouží a zdraží. Důkaz také mohl být vytvořen nezákonně, protože mohl být na internetu uveřejněn třetí osobou, která zneužila např. profil na sociální síti patřící objektu na fotografii. To představuje jeden z nejzávažnějších problémů elektronického důkazu – určit aktéra elektronického jednání totiž prozatím ve většině případů není možné s jistotou. Podle Vladimíra Smejkal je toto podstatnou slabinou elektronického důkazu: „ (...) obtížně je přiřazujeme ke konkrétní osobě, protože prokázat, kdo „měl ruce na klávesnici“ je možné pouze s využitím elektronického podpisu nebo jiných autentizačních metod (použití hesla, SMS, čipové karty atd.)“¹⁷¹ Problematické budou dále situace, kdy půjde opět o fotografii, která byla získána v rozporu se zákonem z důvodu, že byla pořízena a šířena bez souhlasu osoby, o jejíž podobiznu se jedná, respektive, která je na fotografii seznatelná.

Jak ale přistupovat k ještě jinému způsobu projevení nesouhlasu s veřejnou publikací fotografie, než je přímý výslovný projev nesouhlasu osobně nebo on-line? Lze jako takový nesouhlas kvalifikovat také to, že osoba fotografií, na které je zachycena, na sociální síti zařadila na svém internetovém profilu do alba, které ale není veřejně přístupné a není například přístupné ani všem jejím kontaktům, ale pouze afirmativně vybraným osobám? Tento krok představuje informovaný, zcela rozhodný pokus o vytvoření soukromé sféry na sociální síti a je projevem práva souvisejícího s právem na informační sebeurčení v podobě, v jaké bylo naznačeno v úvodu této práce, tedy i sdílená informace může být informací soukromou.

Aplikujme tento příklad na výše uvedené procesní kroky při dokazování. Jedné straně se podařilo přesvědčit některou z osob, které byla svěřena dostatečná důvěra protistrany k tomu, aby měla k těmto fotografiím přístup, a tato bez jejího vědomí fotografii ze soukromého alba zkopírovala a poskytla ji protistraně, která tuto předložila jako důkaz. V takovém případě mohou nastat dvě situace: fotografovaná osoba bude schopna prokázat irelevantnost fotografie ve smyslu, jaký byl již uveden výše (nevlastní,

¹⁷¹ Rozhovor s Vladimírem Smejkalem. Elektronické důkazy – současnost či budoucnost českého soudnictví? *Bulletin Advokacie* 2012 9/2012, s. 11

nehýří), nebo se irelevantnost resp. jiný kontext fotografie zobrazené osobě prokázat nepodaří (a ne nutně pouze proto, že opravdu vlastní, hýří atd.). Jestliže nedal subjekt souhlas, resp. projevil nesouhlas s veřejným šířením fotografie, na které je zobrazen, ideálně, kterou sám pořídil, dostáváme se do situace, kterou v době před rozvojem moderních technologií soudy často řešily šalamounsky v tom smyslu, že důkaz sice provedly, ale nepřihlížely k němu. Také pro naši modelovou konstrukci by ve většině případů sloužil §132 občanského soudního řádu (dále také jen jako OSŘ) jako pojistka.

Lze předpokládat, že soudy budou přistupovat k podobným důkazům spíše konzervativně a ve svém hodnocení důkazu se budou přiklánět k jedné z rozšířených teorií podložených průzkumem zmíněným na jiném místě této práce, tedy, že naše virtuální identita je budována s cílem působit lépe i za cenu udávání nepravdivých informací. Virtuální alter ego uživatele, především na sociální síti, není často přesnou ilustrací života subjektu, ale modelovanou preferenční osobností, personou, za jakou chce být uživatel považován. Je však potřeba připomenout, že soudy by neměly v tomto smyslu automaticky zlehčovat každý důkaz, který je jim ze sociální sítě předložen, protože v situaci, kdy tyto jsou často snadným komunikačním prostředkem, ne každý je užívá za účelem přetvářky – lidé, např. jednoduše komunikují s rozvětvenou rodinou a přáteli, a uvádějí informace přesné a pravdivé, či se, jako především nezletilí, jednoduše chlubí, jak dokazuje zmiňovaný případ Alexy Dell. Přesto je otázkou, zda může soud takový důkaz vůbec připustit. Zájem na blahu dítěte bude jistě hrát podstatnou roli. Je ještě potřeba dodat, že na rozdíl od otázky výše výživného, kdy budou podobné důkazy jistě velmi často navrhovány, bude otázka svěření do péče o poznání složitější a do velké míry směřodátným bude názor příslušného orgánu péče o dítě.

Lze shrnout, že je tedy pouze otázkou času, kdy se s problematikou těchto důkazních prostředků budou pravidelně potýkat také české soudy a bude vždy na uvážení soudce, jakým způsobem k podobným důkazům přistoupí.

4. Právní úprava ochrany nezletilých v kyberprostoru

4.1. Úvod: Sporné otázky právní regulace

Obecně platí, že k regulaci právních vztahů souvisejícím s kyberprostorem lze přistupovat buď formou aplikace platného práva (pokud jeho normy jsou dostatečně obecné a v plném rozsahu nadále použitelné i na právní vztahy vznikající v

kyberprostoru) nebo prostřednictvím zapojení pokročilých interpretačních metod k řešení online případů (přičemž normy pozitivního práva tímto získávají novou dimenzi). Konkrétní situace může také vyžadovat přijetí nových právních norem, jelikož aplikační problémy není možné překonat s využitím interpretačního instrumentária a přijetí nového legislativního opatření se jeví jako vhodnější.¹⁷² Vzhledem k rychlosti rozvoje inovací v kyberprostoru se tak právo informačních technologií do velké míry rozvíjí prakticky, nikoli zákonodárně. Z článku Radima Polčáka¹⁷³ dovozuje autorka, že aktuální samoregulační právní systémy přibližující se *lex mercantoria* plní sice požadavek na právo spočívající v praktické užitečnosti, zároveň ale nemohou zaručit další dvě funkce práva a to zajištění spravedlnosti a jistoty.

4.1.1. Otázka kvalifikované ochrany osobnostních práv nezletilých osob

V návaznosti na definici osobnosti danou v českém právu judikaturou je potřeba si připomenout, že současní mladí jsou první generací, která vyrostla obklopena technologiemi, první generací, která se zcela přirozeně pohybuje v kyberprostoru a užívá internetu, ve formě Webu 2.0.

Jedná se o zcela jedinečnou situaci, kdy nezletilí jsou nositeli znalostní dominance nad generačními autoritami v podobě rodičů či pedagogů. Do společenských věd se tak zapsal termín korektně označující osobu s hendikepou spočívajícím v malých uživatelských schopnostech inovací, tedy „technologically challenged“, významově v podstatě „technologicky postižený“. Oproti tomu moderní mladá generace je souhrnně označována jako „digital natives“, tedy ti, kteří jsou „původními obyvateli kyberprostoru“, ti, jejichž přirozeností je ovládat digitální technologie. Lze si tak snadno představit, že ačkoli budou zvláštní standardy ochrany nastaveny pro osoby mladší 13ti nebo 18ti let, za situace, kdy je v moderním světě již nevyhnutelné pohybovat se v kyberprostoru, budou, pro svou nezkušenost či nízké znalosti ohroženy naopak starší generace. Listina základních práv EU, která věnuje Článek 25 právům starších osob, říká, že: „Unie uznává a respektuje právo starších osob na důstojný a

¹⁷² MAREŠ, D., 81280 K limitaci odpovědnosti providera v prostředí internetu – 1. část. *Epravo* [online]. 16.3 2012 [cit. 2012-12-11]. Dostupný z WWW: <<http://www.epravo.cz/top/clanky/k-limitaci-odpovednosti-providera-v-prostredi-internetu-1-cast-81280.html>>

¹⁷³ POLČÁK, Radim. *Lex Informatica - užitečnost práva a budoucnost informační sítě*. In Vladimír Zoufalý. *XX. Karlovarské právnícké dny*. 1. vyd. Praha: Leges, 2012. s. 236-249, 14 s. ISBN 978-80-87576-16-8. Také *Právní rozhledy* 2012, 17/2012aké

nezávislý život a na jejich aktivní účast na společenském a kulturním životě.“ Pokud ale nebudou také starší osoby efektivně chráněny, podobně jako nezletilí, před aktivitami nejen ohrožujícími jejich osobnostní práva v kyberprostoru, ale před jakoukoli nezákonnou činností v kyberprostoru, bude přinejmenším značně ztížena vymahatelnost jejich práva jak na nezávislý život, tak na účast na společenském a kulturním životě. Zvláště pak bude ohroženo jejich právo na důstojný život.

Lze tedy shrnout, že skupinou uživatelů ohroženou obdobným způsobem jako nezletilí, jsou také senioři, kteří se například teprve učí internet ovládat. Tito se mohou stát oběťmi identity theft¹⁷⁴, phishingu¹⁷⁵ nebo dalších podvodných jednání snáze, než technologicky schopný mladý uživatel. Měla by se tedy zvláštní povaha této skupiny ve vztahu k inovacím také zohlednit kvalifikovanou ochranou? Lze toto tvrzení, jak ohledně jedné, tak druhé věkové skupiny paušalizovat?

Za ideálního stavu musí být poskytována dostatečná právní ochrana všem uživatelům, bez ohledu na věk. Autorka této práce se domnívá, že s ohledem na zvláštnosti každé skupiny a individuální úroveň ohrožení každého jejího člena, nelze poskytovat speciální ochranu žádné z těchto skupin. Jako prevence hrozeb, které jsou na internetu přece jen do jisté míry specifické pouze pro mladistvé uživatele, jako je cybergrooming, šikana, proAna¹⁷⁶ atp. by pak mohlo být řešením např. vytvoření klouzavé uživatelské věkové hranice pro přípravu k získání tzv. uživatelského/technologického průkazu (více viz úvahy *de lege ferenda*) s odchylkou až 3 roky v diskreci příslušného úřadu ochrany práv dítěte nebo soudu s ohledem na odborný znalecký posudek znalce z odvětví psychiatrie, specializace vývojová

¹⁷⁴ Identity theft (ang.), zneužití osobních údajů, zneužití identity fyzické osoby v kyberprostoru.

¹⁷⁵ Phishing (ang.) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo od IT administrátorů. Zdroj: *Wikipedie: Otevřená encyklopedie*. Dostupný z WWW: <<http://cs.wikipedia.org/wiki/Phishing>>

¹⁷⁶ Pro-ana je postoj podporující mentální anorexii a další poruchy příjmu potravy jako životní styl. Mnoho členek tohoto hnutí, které se organizuje kolem webových stránek a skupin na sociálních sítích jsou nezletilé dívky. Na internetu se takto dívky motivují v hladovění i vzájemnou psychologickou manipulací a sem také zasílají rady, jak poruchu utajit před rodiči, či jak dlouhodobě hladovět. Setkat se lze na mnoha stránkách i s prvky náboženského uctívání, jak v podobě uctívané „bohyně“ Any, tedy anorexie a motivačních sloganů a „modliteb“ popisujících anorexii, jako znak disciplíny, úspěchu, nadřazenosti a varujících před utrpením života těch, kdo opustí tento životní styl v porovnání s vizí šťastného mimořádného života vyvolených - anorektiček. Zdroj např.: <<http://proana-blog.blog.cz/>>, <<http://rooftops.blog.cz/>>

psychologie. Volné plné užívání internetu dítětem bez dozoru by bylo podmíněno právě získáním technologického oprávnění (průkazu).

4.1.2. Subjektivní stránka újmy na osobnostních právech nezletilé osoby

Zásah do práva na ochranu osobnosti má dvě složky, a to společenskou – objektivní, a vnitřní - subjektivní, a i přes naprosto nezbytné nastavení jasné hranice, která neumožní nárokování bezvýznamných osobnostních zásahů, by měly být zohledněny v možné míře obě tyto složky. V současné době však právo zastává názor, že je nutné přidržovat se spíše objektivního posuzování újmy, neboť opak by způsobil jednak nerovnost původců, vzhledem k míře, do jaké jeden či druhý dotčený vnímá zásah subjektivně, jako újmu, a dále by jiný, než objektivní přístup, způsobil beztrestnost zásahu do práva na ochranu osobnosti v případech, kdy se dotčený o tomto zásahu nedozví¹⁷⁷.

Není samozřejmě možné založit rozhodnutí soudu jen na subjektivním vylíčení emoční újmy dotčeným. Tak také říká výklad práva, který vylučuje, aby se pro hodnocení způsobilosti vyvolat nemajetkovou újmu staly rozhodujícími pouze subjektivní pocity dotčené fyzické osoby neboli její negativní individuální psychické reakce.¹⁷⁸ Autorka této práce se domnívá, že pro případy porušení osobnostních práv nezletilých by měl existovat režim, především využívající svědeckých výpovědí, znaleckých posudků a přípustných důkazů z kyberprostoru, k prokázání skutečné emoční újmy způsobené konkrétnímu dotčenému, ke které by se mělo, alespoň do určité míry přihlížet. Ačkoli s ohledem na zásahy do osobnostních práv nezletilých nelze snižovat zásadní význam rovného postavení před zákonem a rovných záruk ohledně práv subjektu, bylo by do jisté míry, která lze vyhodnotit např. právě znaleckým posudkem z odvětví psychiatrie, specializace vývojová psychologie, podle autorky práce, vhodné posoudit následky zásahu na osobnost konkrétní osoby a případně tyto přiměřeně zohlednit při vyhodnocování újmy. Je však potřeba zdůraznit, že posudek nemá řešit otázku, zda došlo k újmě, toto posouzení přirozeně náleží jen soudu.

¹⁷⁷ Srov. KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 151. ISBN 80-7201-484-6

¹⁷⁸ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 151. ISBN 80-7201-484-6

V americkém právu bude toto mimo jiné řešeno nepřímo žalobou nejen na vpád do soukromí (privacy invasion) ale také způsobení psychické újmy (infliction of emotional distress). České právo se touto problematikou zabývá výkladem, který vyhodnocení přítomnosti újmy specifikuje v návaznosti na to, zda by každá jiná osoba ve stejném postavení cítila újmu. Pouze věk a obecné posouzení nemohou být, vzhledem k subjektivním zkušenostem, emočnímu vývoji a dalším okolnostem ontogeneze jedince, zcela směrodatnými. Například specifický zásah do osobnosti nezletilé, která byla v minulosti obětí znásilnění, bude mít na tuto silný emoční vliv, ačkoli stejně stará dívka bez tohoto traumatu by podobný zásah nevnímala jako způsobující újmu. Soud by k podobným okolnostem, zejména za předpokladu, že o traumatu zasahující věděl, měl přihlídnout. Taková okolnost jednání má svůj hodnotící význam také podle platného práva. Není rozhodující pro posouzení, zda k zásahu došlo, zato se ale k této skutečnosti přihlíží při rozhodování o výši nemajetkové újmy. Platné právo pro zásahy do osobnostních práv užívá objektivní odpovědnost, čímž již zasahujícího znevýhodňuje a je také z tohoto evidentní zohlednění veřejného zájmu na prevenci zásahů do osobnosti jedince. Pokud by mělo dojít k zohlednění subjektivní stránky újmy, muselo by však pravděpodobně dojít k přechodu na subjektivní odpovědnost, kde by bylo tedy nutné prokázat alespoň vědomou nedbalost. Toto by v praxi bylo značně problematické. Pokud by byl však udržen model objektivní odpovědnosti, bylo by možné zajistit lepší podmínky aplikační praxí, která by kladla větší důraz na subjektivní specialitu/zvláštní okolnosti osobnosti jedince.

Ve chvíli, kdy se zasahující rozhodne zásahu dopustit, činí tak především s cílem poškodit subjekt osobnostně. Osobnost je tak úzce spjata se subjektivitou jedince, že není zcela adekvátní hodnotit ji pouze v návaznosti na průměrného zástupce společenského zařazení subjektu, a na efekt zásahu na její okolí, či na mínění okolí. Ačkoliv lze bezesporu souhlasit, že hranice musí být dána maximálně jednotně a jistá měřitelnost existovat musí, alespoň částečně by tedy soud měl přihlížet k subjektivnímu následku zásahu na osobnost jedince. Lze se domnívat, že soud tak činí, ve velmi omezené míře, v rámci hodnocení důkazů, ale některé další, jako zmíněné znalecké posudky, v praxi nejčastěji nebudou vůbec provedeny.

Prudký rozvoj komunikačních technologií měl ve vztahu k ochraně osobnosti uživatelů, a to především uživatelů nezletilých, dva důsledky. Prvním z nich je

zjednodušení a zpřístupnění možností a prostředků umožňujících dalekosáhlý veřejný zásah do osobnosti uživatele. Druhým z těchto důsledků je potom rapidní nárůst technologické komunikace, kde, především mezi nezletilými, lze zaznamenat zásadní posun ve vnímání soukromí a intimní sféry. Postupně tak může dojít k situaci, že i v případech, kdy bude skutečně možné takový zásah prokázat, nebude možné jej považovat za nezákonný. Jak totiž říká nález Ústavního soudu sp. zn. I. ÚS 156/99 „(...) takový zásah (do osobnostních práv, *pozn. autorky*) je dán pouze tehdy, (1.) jestliže existuje mezi zásahem a porušením osobnostní sféry příčinná souvislost a (2.) jestliže tento zásah v konkrétním případě **přesáhl určitou přípustnou intenzitu takovou mírou, kterou již v demokratické společnosti tolerovat nelze.**“ Pokud dojde pod vlivem technologií a médií k celkovému posunu společenského vnímání soukromí a pravdy, může se stát v demokratické společnosti postupně tolerovatelným daleko hlubší osobnostní zásah, především do dobré pověsti nebo do soukromí. Jedná se o evoluci člověka nebo by bylo na místě tomuto stavu zabránit?

Význam by, podle autorky práce mělo přihlídnutí k subjektivní stránce mít v určité míře i při posuzování způsobilosti nezletilého k právním úkonům v kyberprostoru. Je ovšem již na tomto místě nutné připomenout, že principy, na kterých je založena platná právní úprava, která není v České republice s touto ideou snadno slučitelná, mají v systému práva svůj pochopitelný smysl a význam.

4.1.3. Změna poměrů a otázka promlčení

Nezletilý subjekt je nejtypičtějším příkladem možného opožděného následku osobnostní újmy. V době zásahu či zjištění zásahu do jeho osobnostního práva si tento nemusí pro svůj věk plně uvědomovat vážnost újmy. Bude se jednat např. o zásah, takového charakteru, že bude způsobilý újmy teprve s odstupem několika let v jeho dospělosti. Pokud bude např. někdo o nezletilém učni pravidelně na internetu psát, že pohrdá profesí, ke které se připravuje, je možné, že k vyučujícím se tato informace nedostane a učeň mezi spolužáky poškozen nebude, ba přímo naopak. Pokud si ale jeho jméno před pohovorem o několik let později vyhledá případný zaměstnavatel, již dospělému uchazeči tento zásah uškodí od momentu opětovného vyvolání tvrzení. Jiným příkladem může být šikana. Zde je možné, že v některých specifických případech se proti šikaně nezletilý dočasně „obrní“ a teprve po letech pocítí závažné následky

emoční újmy, která mu byla způsobena. Věra Neradová dochází ve svém článku na toto téma k závěru, že, ve světle právní úpravy ochrany osobnosti v novém občanském zákoníku „(by) předmětem úvah soudů mělo být zodpovězení otázky, zda v konkrétním případě konkrétní neoprávněný zásah může být v době rozhodování soudu (podání žaloby) zmírněn některou z forem morální satisfakce. Důvody takto uplatňovaných nároků jsou natolik osobní, že otázka, zda je možno požadovanou morální satisfakcí dosáhnout jejího účelu, tj. zmírnění následků neoprávněného zásahu, může být zodpovězena až po zjištění a zhodnocení všech okolností případu a nikoliv pouze zkonstatováním této nemožnosti s odkazem na prekluzi práva.“¹⁷⁹ Z autorčina článku lze dovodit, že se v této souvislosti přiklání k zohlednění subjektivní složky vnímání újmy při posuzování nároku soudem, které jsme se již věnovali. Výše uvedené hypotetické příklady mají totiž svůj reálný protějšek v judikatuře, a to již z konce 80. let 20. století, kdy nebyla problematika nových technologií ani zdaleka tak závažná jako nyní. Jedná se o příklad z německé soudní praxe zajímavý tím, že osobnostní zásah byl shledán právě s ohledem na plynutí času, resp. časový odstup, a zároveň se dotýká také svolení. Mladá žena byla v roce 1974 vyfotografována s odhalenými ňadry během dovolené s jejím tehdejší přítelem. Sama byla studentka, ale její přítel byl známý zpěvák. Tehdy k pořízení fotografie dala dívka souhlas. Po uplynutí pěti let byla ovšem fotografie v jiné souvislosti otištěna a neboť se jednalo o sumarizaci žen, se kterými zpěvák udržuje vztah, byla na ni žena označena za jednu z jeho milenek. V mezidobí pěti let však došlo k závažné změně okolností: Žena mezitím získala společenské postavení a se zpěvákem již vztah neudržovala. Soud došel k závěru, že otištění **fotografie za podstatně změněných okolností představuje závažný neoprávněný zásah do její osobnosti.**¹⁸⁰

Právo na ochranu osobnosti se obecně neprekluduje ani nepromlčuje, tedy lze jej vymáhat v průběhu celého života žalobce. Ačkoli se právo na ochranu osobnosti nepromlčuje, vznesené nároky v žalobě bude soud v současné době běžně posuzovat různým způsobem také s ohledem právě na plynutí času. Pokud z pohledu soudu po

¹⁷⁹ NERADOVÁ, V.; Ochrana osobnosti, Zamyšlení nad otázkou zohlednění „plynutí času“ při uplatnění nároků z titulu ochrany osobnosti. *Právní rozhledy*. 2011, PR 102/2011. s. 362, 363

¹⁸⁰ Rozh. OLG Frankfurt/M. z 11. 9. 1986 – 6 U 171/85; KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITY, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 298 – 299 ISBN 80-7201-484-6; ŠIMÍČEK, V. (ed.), *Právo na soukromí*, RYŠKA, M.; *Ochrana soukromí vnitřního kruhu i jeho okolí v praxi práva na ochranu osobnosti*, s. 84 – 85, *Masarykova univerzita, Mezinárodní politologický ústav*, Brno 2011

uplynutí doby od zásahu již odstranění závadného stavu, s ohledem na toto časové období, po které již např. difamační obsah na internetu uveřejněn zůstal, nebude mít restituční efekt nebo již odpadla hrozba opakování jednání, proti kterému má mít rozhodnutí soudu preventivní účinek, žaloba bude zamítnuta. Je namístě, aby soud s ohledem na význam běhu času posuzoval i satisfakční způsobilost poskytnutí požadované omluvy. V době dokončení této práce se podle judikatury promlčoval nárok na náhradu nemajetkové újmy v penězích, a to v obecné promlčecí době tři let¹⁸¹. Spornost promlčitelnosti nároku na náhradu nemajetkové újmy v penězích je velice důležité právě pro nezletilé subjekty zejména s ohledem na právní otázku významu změny poměrů. Oproti tištěným médiím, s ohledem na která byl zákon koncipován, která jsou jeden den vydána a po roce jsou zapomenuta díky množství dalších výtisků a nových zpráv, internet takto nefunguje – během sekundy i několik let starý článek lze nalézt nebo znovu vyvolat, ať již se kdokoli hledající snaží najít konkrétní článek, nebo jakoukoli informaci o konkrétní osobě. Může nastat i situace, kdy nastalé okolnosti iniciují potlačení přirozeného procesu zapomnění, např. pokud se osoba stane v průběhu svého života veřejně činnou, ať již ze své vůle, či jako sekundární efekt svého soukromého života (její manžel se rozhodne kandidovat na prezidenta, zasnoubí se se známým sportovcem, zjistí, že jejím biologickým otcem je známý moderátor atp.). V takové situaci jde význam porušení práva na ochranu osobnosti na internetu „proti proudu času“ a velice snadno a rychle může být připomenut difamující obsah, který je v novém kontextu způsobilý přivodit ještě závažnější újmu, než dříve. Ne nepodobně tomu bude také v případech, které připomněl R. Polčák na přednášce Masarykova institutu v Praze, tedy v případech, kdy existuje veřejný zájem na návratu odsouzených do společnosti po vykonání trestu. Jistě existuje také veřejný zájem na ochraně obyvatel, nicméně média, o to závažněji v době internetu, berou vyvažování těchto dvou hodnot často do vlastních rukou. Internet poskytuje daleko širší prostor pro veškeré podobné zprávy, které se dají snadno přenášet a kopírovat a mají neomezené publikum (např. publikum večerních zpráv bylo většinou omezeno na ty, kteří se dívali v době jejich vysílání), články lze vyvolat kdykoli a publikum je může v reálném čase komentovat a doplňovat o další nepodložené informace. Na tomto místě lze k osvětlení stanoviska

¹⁸¹ Rozsudek Nejvyššího soudu ze dne 12. 11. 2008, sp. zn. 31 Cdo 3161/2008

autorky k této problematice připomenout případ pronásledování muže, který údajně vydíral Amandu Todd na základě udání skupiny Annonymous¹⁸².

Nakonec lze připomenout, že připravovaný balíček evropské regulace informační společnosti, konkrétně Návrh Komise upravující ochranu osobních dat uživatelů internetu¹⁸³, se zabývá mimo jiné tzv. právem na zapomnění¹⁸⁴. V tom nelze vidět nic jiného, než pokus zohlednit, spolu s přirozeným právem člověka na osobní vývoj v čase, přetáť v současnosti možnostmi technologií, obdobné situace uvedené výše. K základním charakteristikám předmětného práva ještě shrňme, že toto právo je nepřevoditelné, subjekt se jej nemůže zříci, je neoddělitelně spjato s jeho osobou a je nepostizitelné výkonem rozhodnutí. Dynamika pohybu informací v kyberprostoru a jejich relativní okamžitá obnovitelnost za každých okolností představuje hrozbu případů, jako byl „Red Kimono“¹⁸⁵ coby do budoucna častější problematiky.

4.2. Právní úprava ochrany osobnosti nezletilých v České republice

Ústava České republiky¹⁸⁶ v Článku 1 uvádí, že se jedná o demokratický právní stát založený na úctě k právům a svobodě člověka a občana. Listina základních práv a svobod, která je součástí ústavního pořádku České republiky osobnostní práva relevantní pro tuto práci v konkrétní podobě zaručuje¹⁸⁷. Tak lze tedy říci, že v České republice je právo na ochranu soukromí a dalších osobnostních hodnot součástí ústavního práva. Prostředky ochrany osobnosti nacházíme jak v právu veřejném tak soukromém. Nejvýznamnější je však, zejména pro svůj dosah, úprava v právu občanském. Do budoucna lze hodnotit český právní systém relativně pozitivně. Jednak se české právo vyvíjí dynamicky souběžně s právem evropským a mimoto je české právo uzpůsobeno pozitivnímu rozvoji práva informační společnosti v některých důležitých ustanoveních právního řádu, jako je například univerzální právní úprava

¹⁸² QUAN, D., Amanda Todd: Mother of girl's accused tormentor lashes out at online 'lynch mob' [online] 17. říjen 2010 [cit. 2012-12-21], *canada.com*, Dostupný z WWW: <<http://www.canada.com/news/Amanda+Todd+Mother+girl+accused+tormentor+lashes+online+lynch/7400570/story.htm>>

¹⁸³ EU. Proposal for a Regulation of the European Parliament and of the Council COM(2012) 11 final, of 25.1. 2012, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Dostupný také z WWW: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

¹⁸⁴ srov. dále v této práci

¹⁸⁵ *Melvin v. Reid*, 112 Cal.App. 285, 297 P. 91 (1931)

¹⁸⁶ Ústavní zákon č. 1/1993 Sb., Ústava České republiky

¹⁸⁷ Relevantní práva zaručená Listinou základních práv a svobod, ústavním zákonem č. 2/1993 Sb., nacházíme v článku 1, 7 (1), 10 (1), (2), 12 (1), 13, 17 (1), (2), (3), (4).

nakládání s osobními údaji jak orgány veřejné správy a samosprávou, tak soukromými fyzickými a právníckými osobami ze zákona o ochraně osobních údajů, nebo právní úprava dokazování, která díky znění ustanovení § 128 OSŘ a ustanovení § 51 správního řádu umožňuje přípustnost elektronického důkazu.

Zákon č. 40/1964 Sb., občanský zákoník

Zákon č. 40/1964 Sb., občanský zákoník (dále také jen jako OZ) poskytuje obecnou osobnostní ochranu v generální klauzuli v § 11¹⁸⁸. Tato má značný význam zejména pro aplikaci práva ve vývoji společnosti, tedy na nové oblasti regulace, protože svým typem poskytuje dostatečný prostor pro dotváření práva v návaznosti na nové potřeby společnosti. Generální klauzule obsahuje také demonstrativní výčet osobnostních hodnot, které jsou chráněny. Demonstrativnost naznačuje neuzavřenost této družiny, na druhou stranu typová určení zase poskytují záchytné body pro výklad, s jehož pomocí lze argumentovat ohledně konkrétních hodnot, jednání a situací jak do této družiny typově spadajících tak nikoli.

V § 12, poskytujícím zvláštní právní úpravu ochrany osobnosti, jsou taxativně vyjmenovány osobnostní hodnoty, které občanské právo chrání. Zajímavou otázkou ve vztahu k vývoji technologií, je definice „hodnoty“ ve vztahu k tomuto ustanovení a jeho následný výklad. Jedná se vlastně o dvojí předmět práva: obsah projevu a jeho záznam. Obsahem úpravy je však právo nikoli majetkové k záznamu, ale osobnostní k hodnotám zachyceným a formě jakou jsou předneseny. Ačkoli lze pochopit zvláštní právní úpravu vázanou na hmotný substrát, neboť jsou zde vymezeny zásahy, kde tento je nezbytným prostředkem, který je nezávislým na osobě, jejíž osobnostní hodnotu nese, a po svém vyhotovení, jak říká Knap, „žije vlastním právním životem“, je možné nahlížet na tuto úpravu také jinak. V publikaci „Ochrana osobnosti podle občanského práva“ kolektiv autorů¹⁸⁹ uvádí, že „§ 12 OZ zakotvil navíc zvláštní právní úpravu pro taxativně vypočtené osobnostní hodnoty, konkrétně pro písemnosti osobní povahy, podobizny, obrazové snímky a obrazové i zvukové záznamy, které se týkají fyzické osoby nebo

¹⁸⁸ Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.

¹⁸⁹ KNAP, K.; ŠVESTKA, J.; JEHLÍČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 16. ISBN 80-7201-484-6

jejích projevů osobní povahy“¹⁹⁰. Autorka této práce se domnívá, že k takovéto interpretaci ustanovení § 12 může v podmínkách současné informační společnosti být nabídnuta alternativa umožňující jeho snadnější aplikaci na nové technologie. Interpretace kolektivu autorů výše uvedené publikace předpokládá, že osobnostními hodnotami, které jsou tímto chráněny, jsou písemnosti osobní povahy, podobizny, obrazové snímky a obrazové i zvukové záznamy. To by předpokládalo, že ochrana osobnosti je ochranou práva majetkové povahy, a to k hmotnému předmětu, zde nosiči projevu osobnosti, který osoba v mnoha případech nikdy nevlastnila, vlastnit neměla a k jehož vytvoření ani nedala souhlas. Dochází tedy k posunu předmětu právní ochrany. Také jiné osobnostní právo, a to zvláště osobnostní právo - právo autorské, nezakládá automaticky osobnostní ani majetkově právní nároky autora, které navíc upravuje pod jiným režimem než ty osobnostní, směrodatné pro tuto analogii, k nosiči jako takovému, ale chrání práva autora k předmětu ochrany, kterým je dílo literární, umělecké a vědecké, které je jedinečným výsledkem tvůrčí činnosti autora, a které je trvale nebo dočasně vyjádřené v jakékoliv objektivně vnímatelné podobě¹⁹¹. To znamená, že stejně jako právo autorské odděluje dílo od jeho hmotného substrátu, a jako hodné autorskoprávní ochrany logicky určuje dílo, jako výsledek tvůrčí činnosti autora, lze se domnívat, že § 12 nechrání taxativně vyčtené formy záznamu, resp. metod zachycení, jako je podobizna, nebo i např. dopis či jiná písemnost, protože tyto jsou pouhým hmotným substrátem, a nikoli osobnostní hodnotou. Co je osobnostní hodnotou lze odvodit ze znění § 11, tedy konkrétně, že „Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.“ a dále z definice osobnosti z judikatury.

Je potřeba připomenout, že § 12 představuje zvláštní úpravu, která nevylučuje využití úpravy obecné z § 11. § 12 dále vyjmenovává výjimky, za kterých se lze jinak ohrožujícího či porušujícího jednání dopustit, tedy za kterých lze tuto vládu subjektu nad svou osobnostní porušit. Obecně lze říci, že těmito výjimkami zajišťuje § 12 například legalitu pořízení obrazového záznamu subjektu, buď s jeho svolením, nebo průlom do práva ve veřejném zájmu. Co se souhlasu týče, zde lze vycházet opět z odborné publikace „Ochrana osobnosti podle občanského práva“, která přichází

¹⁹⁰ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 71. ISBN 80-7201-484-6

¹⁹¹ § 2(1), z.č. 121/2000 Sb., Autorský zákon

s výkladem v tom smyslu, že § 12 představuje zvláštní úpravu pro ty osobnostní hodnoty, které lze zachytit na hmotný substrát, a dále toto ustanovení také představuje právní základ pro domněnku, že nejen k nakládání se záznamem osobnostní hodnoty, ale také k jeho pořízení je potřeba svolení subjektu osobnostní hodnoty, tedy, že je potřeba požádat o souhlas k pořízení záznamu¹⁹². Mimo svolení fyzické osoby a zákonných licencí lze omezit právo na ochranu osobnosti v případě nutnosti plynoucí pro zajištění hodnot, na jejichž zajištění existuje zájem převažující zájem na zaručení ochrany osobnosti jedince. Je však nutné se vyhnout možným excesům, a proto ústavní právo omezuje tuto výjimku ze zaručenosti práva na ochranu osobnosti na nutné minimum¹⁹³. Jak říká publikace „Ochrana osobnosti podle občanského práva“¹⁹⁴ je nutné „aby omezující zásahy byly ve smyslu judikatury Evropského soudu pro lidská práva odůvodněny naléhavou sociální potřebou a zároveň byly přiměřené sledovanému legitimnímu cíli.“ Je potřeba, aby právní řád poskytoval jasně vyložené meze, kdy je možné takto do osobnostních práv zasáhnout. Nápomocná bude nutně i judikatura. Jedním ze základních limitů takového průlomu je, že elementární důstojnost fyzické osoby spolu se základem osobnosti každé fyzické osoby musí být zachovány¹⁹⁵.

Výše bylo jako příklad uvedeno vkládání fotografií fyzické osoby na internet bez jejího souhlasu. V mnoha případech vyložení fotografií na sociální síť je jako legitimní argument legality uváděn konkludentní souhlas subjektu, který, nechává-li se fotografovat, dává souhlas s pořízením obrazového záznamu, a v době smartphonů a sociálních sítí také teoreticky s jeho šířením po internetu. Tento výklad je sporný i u osoby vědomě fotografované. Na fotografiích mohou ale být dále také zachyceny i osoby, které si nemusí být pořizování fotografie vědomy, a přesto je lze na snímku označit, čímž se fotografie dostane bez jejich souhlasu na jejich profilovou stránku. Označování, a jím způsobená dosažitelnost fotografií jsou vnímány sociální sítí Facebook jako samostatná závažná problematika, a vzhledem k přísnější ochraně osobnosti a osobních údajů v Evropě než v USA dochází při stahování a znovuzavádění této funkce k zajímavému vývoji. Zkráceně lze říci, že po zákazu funkce v Německu a

¹⁹² KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 138, 139. ISBN 80-7201-484-6

¹⁹³ Čl. 4 (4) Listiny a Čl. 8 (2) Úmluvy

¹⁹⁴ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 104. ISBN 80-7201-484-6

¹⁹⁵ Interpretován KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 106. ISBN 80-7201-484-6

jejím dočasném omezení v USA byla nyní znovu zavedena v USA a plánuje se její úplné vyloučení pro uživatele v Evropě, ačkoli prozatím pouze pro ty nově registrované¹⁹⁶. Platforma pro sdílení a komentování videí YouTube zase, v reakci na význam sociálních sítí během Arabského jara, zavedla v červenci 2012 funkci pro rozostřování tváří.

Fakt, že svolení lze udělit konkludentně má zásadní význam také pro právní regulaci sextingu v České republice. Pokud by se např. přeposílání soukromé fotografie, která byla určena výhradně pro adresáta, mělo řešit občanskoprávní žalobou na ochranu osobnosti, mohl by žalobce mimo jiné tvrdit, že, vzhledem ke kontextu a okolnostem (např. se jednalo o partnerský pár, kde partnerka neměla důvod předpokládat, že by partner její fotografii sdílel se širším okruhem osob) poskytl konkludentní souhlas s užitím fotografického záznamu své osoby adresátem, tedy zde partnerem, to však jen za účelem užití pro vlastní potřebu. Změnou oprávněnosti předpokladu, že tuto fotografii nebude muž dále šířit (např. rozchodem), by nebylo možné argumentovat, neboť rozhodný bude podle platného práva stav v době udělování souhlasu. Tuto konstrukci by bylo možné užít, jak bylo naznačeno, jak pro případy, kdy fotografii pořídí subjekt sám a zašle ji svému partnerovi na mobilní telefon nebo e-mail, tedy lokaci jasně určenou jedinečnému adresátovi, tak pro případ, kdy fotografii na svůj telefon za konkludentního souhlasu subjektu pořídí partner fotografované. Judikatura se přiklání k restriktivnímu výkladu svolení.

Co se svolení týče, je dále důležité, že jednou dané svolení může osoba kdykoli bez udání důvodu odvolat. Časově je však pojem „kdykoli“ výrazně omezen a tím je také možnost odvolání svolení laickou veřejností často dezinterpretována. Jedná se totiž o možnost bezdůvodně svůj souhlas odvolat kdykoli v mezidobí od původního poskytnutí souhlasu a provedení nebo ukončení faktického příslušného zásahu do osobnosti, tedy nikoli posléze.

Ustanovení § 13 upravuje právní nároky z regulace ochrany osobnosti vyplývající a procesně-právní prostředky, které zákon subjektu za tímto účelem poskytuje. Dále § 13 upravuje náhradu nemajetkové újmy v penězích, ač tak činí

¹⁹⁶ Srov. ESSERS, L.; Regulators confirm Facebook deleted all EU facial recognition data [online] *PCW World*, 7. únor, 2013 [cit. 2013-02-12]. Dostupný z WWW: <<http://www.pcworld.com/article/2027598/regulators-confirm-facebook-deleted-all-eu-facial-recognition-data.html>>

s výhradou v podobě stanovení nutné míry snížení důstojnosti fyzické osoby jednáním žalovaného jako „značné“. Tím je soudu poskytnuta možnost uvážení okolností konkrétního případu a dopadu konkrétního porušení zákona na osobnostní práva žalobce. Vzhledem k, v této chvíli již známým, negativním dopadům porušení osobnostních práv na internetu, a s přihlédnutím k nezletilosti jejich oběti, lze tvrdit, že předpoklad „značné míry snížení důstojnosti“ bude splňovat velké množství takových zásahů.

Ustanovení § 15 upravuje posmrtnou ochranu osobnosti, jejíž uplatňování přísluší, zjednodušeně řečeno, nejbližším žijícím rodinným příslušníkům v určeném pořadí. Porovnáme-li nastalý stav ve věci *Catsouras v. Department of California Highway Patrol* s obdobnou hypotetickou situací hodnocenou podle českého práva, a omezíme-li se na žalobu na ochranu osobnosti, dojdeme ke dvěma způsobům, kterými se lze tohoto práva domáhat. Připomeňme však, že vzhledem ke znění obecné úpravy způsobilosti k právům a povinnostem z § 7 OZ vyplývá, že smrtí tato způsobilost zaniká. Pozůstali tak nevymáhají právo zemřelého na ochranu jeho osobnosti „v zastoupení“, ale vymáhají právo na ochranu osobnosti zemřelého, protože, s ohledem na památku zemřelého, pietu, a mimo jiné i vzhledem k případným osobám blízkým, přetrvává zájem na vymahatelnosti tohoto práva i po smrti osoby. Jedná se o originální osobnostní právo. Podobný zásah však také může mít povahu zásahu do soukromí a rodinného života pozůstalých. Pro tyto případy v současné době platí, že je možné se takovou žalobou domáhat pouze emoční satisfakce, nikoli finančního zadostiučinění. Z jiného rozhodnutí vyplývá, že také osobnostní práva samotného pozůstalého mohou být v některých případech narušena způsobenou smrtí osoby blízké¹⁹⁷. Obecně lze tedy podat na domnělého viníka smrti osoby blízké dvě žaloby, z nichž u druhé bude možné domáhat se také náhrady nemajetkové újmy v penězích. V konkrétním ilustračním případě (srov. výše) však žalovaná strana nezpůsobila smrt dívky, ale dopustila se porušení práva na ochranu osobnosti pozůstalých narušením jejich soukromí, vpádem do intimní sféry piety, a dále, mimo jiné, narušila jejich právo na budování rodinných vazeb a také se dopustila zásahu do ochrany osobnosti zesnulé.

Podrobněji jsme se již věnovali pojmu osobnostní hodnoty. Nyní rozebereme pro tuto práci nejdůležitější z těchto hodnot. Těmi jsou občanská čest a lidská důstojnost,

¹⁹⁷ Rozsudek Nejvyššího soudu České republiky ze dne 31.1.2008, sp. zn. 30 Cdo 336/2007

a soukromí. Občanská čest a lidská důstojnost - tyto dvě hodnoty mají rozdílný charakter, přestože mohou být do určité míry zasaženy stejným jednáním. Lidská důstojnost je zakotvena již v Článku 10 Listiny a jedná se o důstojnost, která je předurčena každé lidské bytosti jako základní společenská norma pro jednání s ní. Stejně jako u soukromí se jedná o hodnotu, kterou je potřeba nahlížet jako do jisté míry subjektivní. Na rozdíl od občanské cti, která je podmíněna vnějším hodnotícím soudem, definice soukromí a lidské důstojnosti vzniká na základě hluboké introspekce každého jednotlivého subjektu. Jinými slovy, teoreticky, ačkoli se morální hodnoty společnosti jako celku, okolí subjektu v jeho obecnosti, posunou k mírnějšímu vnímání některých zásahů, tyto mohou být stále způsobilé přivodit osobnostní újmu konkrétnímu subjektu, který má právo vnímat morálku, intimitu, váhu tajemství a další související moduly těchto osobnostních hodnot zcela individuálně, podmíněně svému životnímu vývoji, zázemí, názorům a osobnímu morálnímu kodexu. Lidskou důstojnost je tak potřeba oddělit od pojmu občanské cti.

Občanská čest se mění jednak s ohledem na věk, ale zejména vlastním přičiněním osoby. Bude tak v průběhu jeho života vyšší nebo nižší s ohledem na jeho jednání, aspirace a funkci ve společnosti, státu, ale i ve své komunitě. Toto je nutné zdůraznit, protože k této povaze občanské důstojnosti konkrétního jedince lze přihlížet, pokud je v roli žalobce, při vyhodnocování oprávněnosti nároku a otázky, zda byl zásah do jeho osobnostních práv způsobilý přivodit této osobě nemajetkovou újmu nebo značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu.

Další významnou osobnostní hodnotou, která je velmi důležitá pro tuto práci, je soukromí fyzické osoby. Jedná se o osobnostní hodnotu fyzické osoby, která je v kyberprostoru porušována nejčastěji a již samotná existence Webu 2.0 představuje jedinečný prostor pro takové zásahy. V mnoha odborných pramenech se lze setkat se základním tvrzením, že bez soukromí by nebylo ani svobody¹⁹⁸. Do práva na soukromí subjektu spadá i právo na interakci, tedy že soukromím není myšleno jen utajování informací, ale i život ve společenství bez rizika sledování takového života třetími

¹⁹⁸ Soudce Federálního ústavního soudu Louise D. Brandeis, NY Civil Liberties Union; publikace *Ochrana osobnosti podle občanského práva*; WAGNEROVÁ, E. v článku *Právo na soukromí: Kde má být svoboda, tam musí být soukromí*, Právo na soukromí., MUNI Press, Mezinárodní politologický ústav Masarykovy univerzity, 2011. 49 s.; Usnesení Nejvyššího soudu ze dne 16.8.2007, sp. zn. 30 Cdo 2082/2007

osobami¹⁹⁹. Pro téma této práce tak bude mít tato konstrukce význam zejména z pohledu zásahu do osobnostních práv nezletilých při užívání elektronických důkazních prostředků z internetu, při excesech typu *Catsouras* nebo při zásahu do osobnostních práv nezletilého rodičem²⁰⁰. Je důležité ještě zmínit, že ani nedovolený sběr důvěrných informací, tedy informací spadajících do soukromé sféry subjektu, bez toho, aby tyto informace byly dále šířeny nebo jiným způsobem zneužity tak, že by poškodily subjekt, nepožívá právní ochrany.

Okrajově se můžeme zmínit také o osobnostních hodnotách, kterými jsou podoba a ochrana projevů osobní povahy. Ačkoli lze předpokládat, že většina osobnostních zásahů v kyberprostoru bude porušovat právo na soukromí nebo občanskou čest a lidskou důstojnost, ačkoli tak bude nezřídka činit za pomoci zneužití podoby a projevů osobní povahy, je na místě připomenout, že i tyto mají také samostatný nárok na ochranu. Co se podoby fyzické osoby týče, jedná se i o podobiznu, nikoli pouze fotografický záznam osoby. Jako projevy osobní povahy osoby lze nejčastěji označit osobní písemnosti, a to i elektronické pošty, ale také např. zvukový záznam jejího projevu.

Subjekty práva na ochranu osobnosti.

Oprávněným subjektem osobnostních práv je pouze fyzická osoba. Vzhledem k tématu této práce je nutné připomenout ustanovení § 7 – 9 OZ a způsob, jakým upravují právní postavení nezletilého a vymahatelnost ochrany jeho osobnosti.²⁰¹ Zabýváme-li se právem na ochranu osobnosti nezletilých, je důležité připomenout, že pokud je jediným předpokladem pro nabytí práv a povinností narození fyzické osoby, požívají práva i pokud pro svůj věk nebo psychický stav (stav duševního zdraví) nejsou s to chápat újmu, která jim vzniká neoprávněným zásahem jiného na jejich osobnosti, resp. na jednotlivých hodnotách osobnosti²⁰².

¹⁹⁹ Srov. 3.4.2.1. a 3.4.2.2. – pozitivní (aktivní, tedy komunikace, svoboda projevu, budování sociálních vazeb) a negativní (pasivní, právo nebýt subjektem sdílení osobnostních hodnot, právo *to be let alone*) složka práva na informační sebeurčení nezletilé osoby

²⁰⁰ srov. výše

²⁰¹ ŠVAŇHAL, R.; Poznámky k ochraně osobnosti nezletilých osob, *Právní Praxe* 10/2000, 2000. s. 635-643; JEHLIČKA, O.; ŠVESTKA, J. a kol: *Občanský zákoník. Komentář*. 3. vydání, Praha, C.H. Beck, 1996. s. 37. ISBN 80-7179-063-X

²⁰² KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 79 ISBN 80-7201-484-6

Co se ale týče právních úkonů, kterými se osoba ochrany svých osobnostních práv domáhá, tyto nemůže provádět nezletilý. Ten bude proto zastoupen při těchto nejčastěji rodičem nebo jiným zákonným zástupcem. Určit, zda je jako účastník řízení o ochranu osobnosti konkrétní nezletilý procesně způsobilý k příslušným úkonům s tímto spojeným, je však v diskreci soudu. Bude tomu tak v případech, kdy zájmy nezletilého jsou v kolizi se zájmy zákonného zástupce, tedy především v případech žalob na ochranu osobnosti, kdy zasahujícím subjektem do práva nezletilého byl právě zákonný zástupce. V konkrétním řízení bude kolizním opatrovníkem až na výjimky orgán sociálně-právní ochrany dětí. Podstatný význam má proto zákon o sociálně-právní ochraně dětí²⁰³. Podle toho má dítě právo požádat orgány sociálně-právní ochrany a zařízení sociálně-právní ochrany, státní orgány, kterým přísluší ochrana práv a oprávněných zájmů dítěte, pověřené osoby a dále školy, školská zařízení a zdravotnická zařízení o pomoc při ochraně svého života a dalších svých práv. Tyto orgány, právnické a fyzické osoby a pověřené osoby jsou povinny poskytnout dítěti odpovídající pomoc. Dítě má právo požádat o pomoc i bez vědomí rodičů nebo jiných osob odpovědných za výchovu dítěte.²⁰⁴ Z ustanovení § 9 OZ přímo vyplývá, že nezletilé fyzické osoby mohou v závislosti na svém vývoji fyzickém i psychologickém činit takové právní úkony, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku. Jak vyplývá z komentáře k občanskému zákoníku autorů J. Švestky, O. Jehličky a kol.²⁰⁵, toto kritérium je však potřeba chápat objektivně, tedy zcela bez ohledu na individuální psychickou vyspělost konkrétního dítěte. I pokud tak není možné, aby dítě samo provádělo právní úkony, má možnost domoci se právní ochrany, zde resp. zastoupení ve věci, resp. vyjednání odborné pomoci. Zároveň jsou jeho subjektivní práva v tomto procesu zohledněna v tom smyslu, že pokud je schopno formulovat své vlastní názory, má právo pro účely sociálně-právní ochrany tyto názory svobodně vyjadřovat při projednávání všech záležitostí, které se ho dotýkají, a to i bez přítomnosti rodičů nebo jiných osob odpovědných za výchovu dítěte. Vyjádření dítěte se při projednávání všech záležitostí týkajících se jeho osoby věnuje náležitá pozornost odpovídající jeho věku a rozumové vyspělosti.²⁰⁶ Toto ustanovení má primárně za cíl

²⁰³ Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů

²⁰⁴ Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, § 8 (1)

²⁰⁵ JEHLIČKA, O., ŠVESTKA, J. a kol.; *Občanský zákoník. Komentář*. 3. vydání. Praha, 1996, C.H. Beck s. 37

²⁰⁶ Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, § 8 (2)

zohlednit veřejný zájem o blaho dítěte²⁰⁷. Je z něj však také možno dovozovat, že představuje prostředek, jak zohlednit mentální a citovou vyspělost nezletilého, a jak mu poskytnout náležitou kontrolu nad způsobem aplikace práva na ochranu jeho osobnostních práv. Ačkoli nezletilý tedy osobnostní práva má, je potřeba posoudit, zda má také právní způsobilost k úkonům spojeným s jejich vymáháním. Jak ve svém článku na toto téma zdůrazňuje Roman Švaňhal: „může být aktuální (tato otázka, *pozn. autorky*) zejména v souvislosti s občanskoprávní ochranou osobnosti dítěte proti šikaně, souvislosti se zneužíváním rodičovských práv, reklamou využívající dítě a to jako nositele reklamy i jejího adresáta (...) atd.“²⁰⁸

Předmět a obsah jednotlivých prvků práva na ochranu osobnosti s ohledem na jednání nezletilých v kyberprostoru

Předmět a obsah práva na jméno

Ve valné většině případů, kterými se zabývá tato práce, bude ochraně podléhat jméno vlastní pouze spolu s příjmením. Jednalo-li by se však o nezletilého, který je osobou veřejně činnou a používá pouze jméno vlastní, které je s ním neoddělitelně spjato, bude ochraně podléhat i toto samostatně. Stejná situace nastane také v případě pseudonymů nebo přezdivek. Je však možné v některých případech tuto ochranu jiného jména, než je kombinace jména vlastního a příjmení, jak je zaneseno v rodném listu, předpokládat i tam, kde nezletilá osoba není osobou veřejně činnou. Vycházejme z výkladu v publikaci „Ochrana osobnosti podle občanského práva“: Vlastní jméno je předmětem tohoto práva buď tehdy, jestliže se pro určitou osobu stalo tak příznačným, že tvoří samo o sobě dostatečný individualizační znak, plníci vlastně obdobnou funkci jako např. pseudonym, anebo v těch případech, kdy je nutným doplňujícím znakem pro individualizaci určité osoby.²⁰⁹ První případ může v kyberprostoru nastat dvěma způsoby. Buď se přezdívka, pseudonym nebo vlastní jméno, ať původní nebo pseudonymní, přesune z reálného prostředí do kyberprostoru nebo jej subjekt naopak

²⁰⁷ Blaho dítěte je vůdčí zásada ovlivňující úpravu všech právních vztahů, které se týkají nezletilých dětí (zájem dítěte). Výslovně je zmíněna v Úmluvě o právech dítěte (vyhl. č. 104/1991 Sb.) a v zákonu o sociálně-právní ochraně dětí (zák. č. 359/1999 Sb.). Zdroj: HENDRYCH, D. a kol.; Právní slovník 3. vydání, 2009. *Beck-online*

²⁰⁸ ŠVAŇHAL, R.; Poznámky k ochraně osobnosti nezletilých osob, *Právní Praxe*, 2000, 10/2000. s. 635-643

²⁰⁹ KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. s. 283. ISBN 80-7201-484-6

začne užívat v kyberprostoru, a toto se s ním stane natolik spjatým, že identifikační funkci přebere i v reálném světě. Nemusí se jednat o známost široké veřejnosti, pokud tato osoba sama široké veřejnosti známa není. Bude tedy zřejmě postačovat, bude-li takové jméno s touto spjato v jejím okruhu sociálních vazeb, jako je škola, přátelé a rodina. První situace může být typicky reprezentována přezdívkou, pod kterou označují nezletilého všechny osoby v jeho okolí. Lépe průkazným, avšak méně častým příkladem může být situace, kdy např. při nástupu na střední školu deklaruje nová studentka svou individualitu tím, že se začne označovat pod jiným křestním jménem, bude vyžadovat, aby tak byla oslovoována i pedagogickým sborem, a pokud v tomto uspěje, bude její vlastní jméno, ač přejaté, požívat ochrany spolu s příjmením. Otázkou by však bylo, zda tato kombinace v právním nároku nepředčí právní nárok na ochranu původní kombinace vlastního jména a příjmení. Lze se však domnívat, že ne, a chráněny budou obě kombinace. Druhá situace nastává poměrně často. V současné době mnoho nezletilých využívá pro tvorbu svého kybernetického alter ega kombinace znaků, které jsou fragmenty jmen, přezdívek, akronymů a symbolických slov. Důvodem je často snaha o soukromí, resp. realizace práva na informační sebeurčení s cílem znemožnění rodičům, učitelům, příbuzným nebo nadřízeným na brigádě vyhledat jejich profil. Dalším motivem může být prostá snaha o vytvoření zajímavého stylového profilu. Pokud se bude jednat o přezdívkou, která se mezi kontakty v kyberprostoru uchytí a případně je převzata i v reálném světě, může tato, především pokud je jedinečná, také požívat ochrany jako jméno. Příkladem práva na jméno - přezdívkou jsou nezletilí tvůrci streetartu, jejichž pravé jméno nemusí být jejich okolí či širší základně příznivců často známo. Důvodem je nejen výše zmíněná snaha po stylizaci či sdělení, ale i snaha vyhnout se stíhání v případech užívání ploch v rozporu se zákonem²¹⁰.

Subjekt může také poskytnout souhlas s užitím jména. Takovéto svolení nemá předepsanou právní formu, ale musí se pohybovat v mezích zákona a v souladu s dobrými mravy a nezletilý musí být vzhledem ke svému věku a mentální úrovni konkrétní svolení schopen jej poskytnout, jinak by bylo neplatným. Konkrétně tak může

²¹⁰ Příkladem může být zletilý streetartový umělec z Velké Británie, který celosvětově proslul pod přezdívkou Banksy, kterou z bezpečnostních důvodů přejal. Tento velice důsledně střežil svou identitu i v době, kdy jeho díla byla prodávána ve známých aukčních domech. Teprve před nedávnem se novinářům podařilo zjistit jeho pravé jméno.

být právo nezletilého na jméno v kyberprostoru porušeno např. založením falešného profilu nezletilého či jiným zneužitím jména či „dostatečně silné“ přezdívky.

Předmět a obsah práva na podobu

Podle Občanského zákoníku se jedná o právo k podobizně a k obrazovému snímku. To znamená, že zejména v prostředí sociálních sítí je chráněno nejen vyobrazení mířené na subjekt s cílem vytvořit jeho portrét, ale také jeho náhodné zachycení, např. v pozadí při pořizování portrétu jiného subjektu, jak již bylo dříve v práci osvětleno. Protože se však jedná o právo na podobu, nikoli o právo na „zachycení“, je k vymahatelnosti nezbytné, aby osoba byla ze zobrazení identifikovatelná. Připomeňme, že se nemusí jednat o identifikovatelnost obličejovými rysy, ale jakýmkoli specifickým dostatečně jedinečným znakem podoby subjektu, či skupinou takových markant, ve své kombinaci nevzbuzujících pochyb o totožnosti osoby. V této práci byla již popsána pozitivní a negativní povaha obsahu tohoto práva, tedy oprávnění disponovat s touto osobnostní hodnotou, poskytnout svolení k jejímu zachycení, ale také bránit jejímu užití, tedy zachycení jakoukoli formou, ať již se jedná o libovolný druh podobizny nebo záznam, a další dispozici s tímto zachycením. Ačkoli svolení, jak již víme, nemusí být výslovné, má subjekt být seznámen s rozsahem a způsobem, jakým bude podobizna použita a rozšiřována. I zde ale platí, že souhlas může být i konkludentní. Důležité je také to, že soud v případném sporu bude vycházet podle okolností z domněnky, že dotčený způsob a rozsah užití subjekt znát musel. Ani toto však není pravidlem. Nejčastějšími porušeními práva nezletilých k podobě je tak nejen zveřejnění snímků, na kterých jsou identifikovatelní, ale také široké nakládání s podobiznou nad předpokládaný účel jejího pořízení. Připomenout lze, že v praxi s tímto subjekt zpravidla seznamován není, ani se o něj nezajímá, a lze se jen domnívat, že předpokládá, že pokud je fotografován vrstevníkem, v realitě, kdy oba jsou uživatelé sociální sítě, jeho fotografie je pořizována jako památka, a na sociální síti se objeví. Např. jen na sociální síť Facebook je denně nahráno uživateli přes 10 milionů fotografií. Tímto uživatelem však bude pořizovatel fotografií, a nikoli jejich subjekt. Je potřeba si uvědomit, že pořizovateli nebrání také nic v tom, aby digitální snímek graficky upravil do dehonestujícího výsledku a tento dále šířil nebo zneužil k odcizení identity subjektu, např. pro založení jejího falešného profilu na sociální síti, seznamce nebo stránkách zprostředkovávajících erotické služby, jak bylo potvrzeno praxí. Velice závažným

problémem je i fakt, že fotografie jednou na internet vložené jsou pro svou digitální podobu přístupné komukoliv, kdo je schopen je zobrazit, bez toho, aby jejich pořizovatel nebo subjekt měli možnost dozvědět se o tom, že někdo takovou fotografií zkopíroval a dále s ní jakkoli nakládal. Lze předpokládat, že s vývojem technologie rozeznávání biometrických údajů a vyhledávání na základě vizuálního porovnávání, nikoli klíčových slov, bude v budoucnu možné takto inkriminovaný snímek či osobu na veškerých v kyberprostoru dostupných fotografiích vyhledat. V současné době však tato možnost není uživateli běžně dostupná. Další formou zneužití podoby je vytvoření neexistující identity. Na sociálních sítích neexistuje, až na výjimky, žádný kontrolní systém, žádné ověření reálnosti uživatele nebo pravdivosti údajů, které uvádí. Existence velkého množství profilů neexistujících osob na sociální síti Facebook vyvolala negativní reakce u zadavatelů reklamy. Společnost tedy zahájila na podzim 2012 rozsáhlou „razií“, při které jsou postupně vymazávány všechny falešné profily z odhadovaného počtu 83 milionů. Jak bylo osvětleno dříve v této práci, takový postup ovšem může být z pohledu práva na ochranu osobnosti a dalších ústavou zaručených práv uživatele problematický.

Předmět a obsah práva na občanskou čest a lidskou důstojnost

K předmětu a obsahu práva na občanskou čest a lidskou důstojnost lze v kontextu nezletilých v kyberprostoru, mimo již uvedené, dodat, že k jeho porušení na internetu může dojít komentářem, blogovým příspěvkem, šířením difamující fotografie nebo šířením difamující fotografie mimo okruh jejích původních adresátů, odcizením identity nebo její manipulací za účelem difamace subjektu nebo neoprávněnou manipulací s účtem neboli profilem subjektu na sociální síti, nepravdivým označením osoby v difamujícím kontextu, nebo např. anonymním šířením nepravdivých tvrzení e-mailem. Podstatné je ještě věnovat se krátce pojmu kritiky. S tou se můžeme na internetu ve vztahu k nezletilým nejčastěji setkat v, často anonymních, reakcích na internetové příspěvky nebo v příspěvcích psaných pod vlastním jménem v rámci sociální sítě: Zásahem do práva na ochranu osobnosti nezletilého nebude oprávněná kritika, kterou je hodnotící úsudek založený na věcné reakci založené na subjektivním myšlenkovém vyhodnocení konkrétní věci vycházejícím z pravdivých údajů. Na pomezí kritiky a difamace bude tzv. trolling, kterému jsme se blíže věnovali dříve v této práci.

Pakliže by takovýto příspěvek či série příspěvků byli předmětem žaloby, bylo by jistě velice zajímavé sledovat posuzování tohoto projevu zvláštní povahy soudem.

Předmět a obsah práva na slovní projevy osobní povahy

V kyberprostoru se bude jednat o právo k písemnému projevu, tedy zejména k osobní korespondenci ve formě e-mailů, soukromých zpráv na službách jako je Facebook, anebo SMS zpráv či soukromých zpráv na chatových fórech či v rámci komunikace mezi hráči či zpráv na jiném rozhraní. Z pohledu zvukového záznamu v klasickém právu před rozvojem kyberprostoru byly nejčastěji uváděnými příklady nejrůznější formy odposlechů. V podstatě každý mobilní telefon, který má dnešní nezletilá osoba k dispozici umožňuje funkci nahrávání zvuku i videa. Nahrávat lze také na počítač. Nahrávány tak bez vědomí mluvčího mohou být např. soukromé hovory mezi nezletilými žáky, které lze velice snadno umístit na internet. Připomenout lze případ zástupce ředitele základní školy v newyorském Bronxu, který pozoroval studenty a jejich práci na počítači bez jejich vědomí díky vzdálenému přístupu k ovládání některých funkcí jejich školních laptopů. Mimo jiné tak sledoval v reálném čase obsah vyhledávání, otevřené soubory na ploše nebo, díky webkameře, i samotné děti²¹¹.

Předmět a obsah práva na osobní soukromí

V souvislosti s případem uvedeným v předchozí kapitole, lze uvést obdobný, ovšem závažnější zásah školy, zde především do práva dětí na soukromí, ve věci *Robbins v. Lower Merion School District*. Skupinová žaloba žáků prostřednictvím jejich zákonných zástupců byla podána poté, co se potvrdilo školou popírané podezření žáků, že jsou prostřednictvím laptopů školou sledováni²¹², a to mimo vyučování, ve svém soukromí a v prostředí domova, kde jsou tak sledováni také rodinní příslušníci dětí či osoby žijící ve společné domácnosti s těmito.²¹³

²¹¹ OTTERBEIN, N.; It's not just Lower Merion!: Bronx school watches unwitting students via Webcam [online] *City Pater*. 26. únor 2010 [cit. 2012-07-15]. Dostupný z WWW: <http://www.citypaper.net/blogs/nakedcity/its_not_just_lower_merion_bronx_school_watches_unwitting_students_via_webcam.htm>

²¹² MATYSZCZYK, Ch.; School shows off its laptop surveillance tactics [online] *CNET*, 26. únor 2010 [cit. 2012-12-19]. Dostupný z WWW: <http://news.cnet.com/8301-17852_3-10460729-71.htm>

²¹³ Wikipedia contributors; Robbins v. Lower Merion School Distrikt [online] *Wikipedia, The Free Encyclopedia*, 6. leden, 2013 [cit. 2013-01-23]. Dostupný z WWW:

Moderní technologie a internetové aplikace umožňují sledování pohybu subjektu, jako jsou jeho nákupní zvyklosti, jeho kulturní preference a mnoho dalších dat. Tato data jsou však buď zcela dostupná, nebo dostupná sice omezené, ale široké skupině osob. Lze tedy tvrdit, že se nejedná o zásah do zaručených práv uživatele, protože osoba poskytla konkludentní svolení se sběrem sdílením informací se širokou, často nepřesně definovatelnou skupinou subjektů v kyberprostoru. Problém však nastává, pokud se jedná o soukromé informace o osobě na internetu uveřejněné jinou osobou bez jejího vědomí a o jejichž existenci se osoba třeba nemá možnost dozvědět. Další variantou jsou případy, kdy osobní informace elektronicky sdílí osoba s velmi omezenou skupinou subjektů, některá z fyzických osob však, bez toho aby data kopírovala a šířila, tyto pouze prohlíží a ukazuje na obrazovce dalším fyzickým osobám, a to bez vědomí resp. souhlasu subjektu. Typicky se bude jednat o prohlížení zabezpečeného profilu s nastaveným soukromím na sociální síti nebo zpřístupňování sextingové fotografie na displeji mobilního telefonu. Zásahem do soukromého života bude získávání a šíření jakýchkoli informací spadajících do této chráněné sféry. Je nasnadě, že se bude jednat nejen o intimní informace smyšlené, ale také pravdivé. Zásahem bude také narušení práva na rodinný život a mnoho dalších jednání, která bude možné do této kategorie podčlenit. K vážnému zásahu do osobnostních práv nezletilé osoby takto bez pochyby došlo v nedávném případě z holandského města Driehuis, kde dospělý muž spáchal sebevraždu skokem pod vlak. Nezletilé osoby čekající na nedalekém nádraží okamžitě po události pořídily mnoho foto a videozáznamů z místa neštěstí, které okamžitě sdílely na internetu. Když poté policie oznámila pozůstalým smrt muže, zjistila, že jeho syn již viděl drastické fotografie z místa činu, pouze nepoznal, že se jednalo o jeho otce.²¹⁴ Pokud by byl případ posuzován podle platného českého práva, došlo k neoprávněnému zásahu do práva na soukromí a rodinný život také v případě z Velké Británie, kdy se Cheryl Jones, pouze ze vzkazů přátel na stránce své dcery na Facebooku dozvěděla, že tato zahynula, a to mnoho hodin předtím, než ji s tímto oznámením kontaktovala policie.²¹⁵ Matka podala stížnost na jednání příslušného policejního orgánu, který věc

<http://en.wikipedia.org/w/index.php?title=Robbins_v._Lower_Merion_School_District&oldid=5315519
81>

²¹⁴ Son learns of father's suicide through scarring Twitter photos [online] *The Dot Com*, červen 2012 [cit. 2012-11-18]. Dostupný z WWW: <<http://www.dailydot.com/news/son-father-suicide-twitter-photos/>>

²¹⁵ Facebook: Karla James' death revealed to mother [online] *BBC News*,

šetřil. V době odevzdání práce se touto zabýval příslušný odbor policie. V České republice by mohla pravděpodobně podat matka žalobu jak na policii, resp. stát, tak na mluvčího či mluvčí, tedy ty přátele, kteří informace o smrti na sociální síti zveřejnili. V této souvislosti lze ještě připomenout, že judikatura potvrdila rozšířenou definici zásahu nejen jako aktivního, ale i jako pasivního. Lze se jej tedy dopustit také opomenutím povinnosti či nečinností²¹⁶.

Sankce odpovídající porušení práva na ochranu osobnosti podle občanského práva

V ustanovení § 13 – 16²¹⁷ OZ nalezneme právní úpravu postihu za porušení, ale i pouhé ohrožení osobnostních práv. Tyto formy zadostiučinění mají mít restituční²¹⁸, reparační i preventivní charakter, a je možné je kombinovat s ohledem na konkrétní okolnosti věci. Odpovídají také tomu, že se jedná o nemajetkové, osobnostní právo. Náhrada nemajetkové újmy v penězích má funkci kompenzační, tedy je alternativní kompenzací závažných následků zásahu nemajetkové povahy. Obecně k nemajetkové újmě platí, že původce je povinován zákonem podle § 13 OZ zdržet se dalších neoprávněných zásahů, odstranit následky neoprávněných zásahů a/nebo poskytnout postiženému přiměřené zadostiučinění, ať již morální nebo peněžité. Tuto satisfakci vyjádřenou v penězích – nemajetkovou újmu nelze, a není proto třeba co do její výše prokázat, jak je tomu u škody, protože zde se nejedná o újmu materiální a tedy přesně vyčíslitelnou. Zcela zásadní význam má objektivní odpovědnost za zásah do práva na ochranu osobnosti podle OZ. Při zásahu do práva na ochranu osobnosti podle generální klauzule jde v některých případech použít důkaz pravdy, tedy původce se bude pokoušet dokázat, že difamační informace, která byla zásahem, se zakládají na pravdě. Toto se však nebude týkat případů, kdy došlo k zásahu do soukromí šířením intimních informací ze života dotčeného. Zde nejen, že nelze použít důkaz pravdy, ale o zásah se bude jednat i tehdy jedná-li se o informace, které nemají difamační povahu nebo jsou naopak vyloženě pozitivní. Původce má v těchto případech ale možnost vyvinut se pokud dokáže, buď, klasicky, že měl svolení dotčeného k šíření těchto informací, nebo pokud

20. září 2012 [cit. 2012-12-21] Dostupný z WWW: <<http://www.bbc.co.uk/news/uk-wales-south-east-wales-19662314>>

²¹⁶ Nález ÚS ze dne 14. října. 1995, sp. zn. I. ÚS 15/95

²¹⁷ Náhrada škody v souvislosti se zásahem do osobnostních práv není předmětem této práce.

²¹⁸ Vzhledem k již osvětlené povaze kyberprostoru a relevantních jednání, lze tvrdit, že v naprosté většině zásahů do osobnostních práv nezletilého v kyberprostoru nebude absolutní reparace možná.

by bylo možné spolehlivě dovodit, že osoba konkrétní předmětnou skutečnost ze své intimní sféry vyloučila. To bude prokazováno například tak, že bude prokazatelné, že tuto informaci sama rozšiřovala anebo k jejímu rozšiřování v jiné formě svolila, či za toto dokonce přijala plnění²¹⁹. Zde je však potřeba obezřetnosti, protože, jak bylo řečeno, ani informace sdělená více osobám, by se teoreticky neměla automaticky stát veřejnou, tedy dále přenosnou.

Subjekt občanskoprávních sankcí

Subjektem občanskoprávních sankcí za zásah do osobnostních práv fyzické osoby může být jak fyzická, tak také právnická osoba. V klasických případech žalob na ochranu osobnosti, zejména v případech, kdy k zásahu došlo v kyberprostoru, tedy v té nejjasnější podobě, tedy formou otištění difamačních tvrzení na stránkách internetového periodika, je nejčastější formou přiměřeného zadostiučinění omluva. Právě omluva v kyberprostoru, tedy nejčastěji na stránkách, kde k zásahu došlo se však ve valné většině případů, kterými se zabývá tato práce, jeví jako nedostatečná. Bude tomu tak zejména pro časový odstup, s jakým k uveřejnění může fakticky dojít a zároveň pro tzv. bannerovou slepotu²²⁰ uživatelů internetu a pro tzv. Streisand efekt²²¹, který má na internetu o mnoho horší následky než off-line, a to pro možnost okamžitého vyhledávání informace.

²¹⁹ Rozsudek Krajského soudu v Brně ze dne 31. 10. 2007, sp. zn. 24 C 48/2004, Rozsudek Vrchního soudu v Olomouci ze dne 28. 1. 2009, sp. zn. 1 Co 119/2008

²²⁰ Bannerová slepota (ang. banner blindness): Bannerovou slepotou je označována tendence uživatelů internetových stránek ignorovat reklamní plochy, a to i tehdy, obsahují-li informace, které návštěvník právě hledá. Za faktem, že uživatelé bannery přehlížejí, stojí zřejmě přesycenost webových stránek nekvalitně zpracovanými a informačně nehodnotnými reklamními formáty. Zdroj: *symbio* Dostupný z WWW: <<http://www.symbio.cz/slovník/bannerova-slepota-banner-blindness.htm>>

²²¹ Streisand efekt (ang. Streisand Effect): název používaný pro fenomén, kdy se subjekt snaží o odstranění určité informace dostupné k veřejnému oběhu, čímž k této ale přitáhne pozornost veřejnosti a docílí kontraproduktivního vyvolání zájmu o ni. Fenomén byl pojmenován podle případu, kdy právní zástupci zpěvačky a herečky Barbary Streisand podali žalobu na leteckého fotografa K. Adelmána, který pro vládní projekt California Coastal Records mapování eroze pobřeží okolo Malibu pořídil 12 000 fotografií útesů, které byly dostupné na stránce projektu. Na jedné z fotografií bylo zachyceno sídlo zpěvačky. Po zveřejnění žaloby se návštěvnost nezajímavé stránky neúměrně zvýšila a fotografie domu začala být sdílена. Zdroj: Wikipedia contributors; Streisand effect [online] *Wikipedia, The Free Encyclopedia* [cit. 2012-02-03] Dostupný z WWW: <http://en.wikipedia.org/w/index.php?title=Streisand_effect&oldid=543051477>

Související zvláštní zákony

Pro nastínění problematiky vymahatelnosti práv uživatelů na internetu, zejména vymahatelnosti osobnostních práv jako je ochrana soukromí a ochrana občanské cti a lidské důstojnosti, je zapotřebí věnovat se alespoň okrajově některým souvisejícím zvláštním zákonům. Těmito jsou především **Zákon č. 101/2000 Sb., o ochranně osobních údajů** a **zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)**. Oba jsou výsledky implementačního procesu evropského práva²²². Úkolem obou je regulovat pohyb dat, informací a osobních údajů stejně jako jejich zpracování a další nakládání s nimi, jak na území EU, tak ve třetích zemích. Lze téměř s jistotou tvrdit, že oba tyto zákony budou zasaženy změnou právní úpravy ochrany uživatelských dat v kyberprostoru plánovanou EU. Tyto zvláštní zákony mají pro téma této práce význam v tom, že upravují právní odpovědnost důležité skupiny subjektů, které mohou být způsobilé ohrožení či porušení osobnostních práv nezletilých uživatelů, tedy PSISs. Mimoto tyto zákony také poskytují ochranu preventivní, spočívající v regulaci činnosti těchto subjektů.

Právní regulace odpovědnosti PSIS vychází z ustanovení Kapitoly II Oddílu 4 Směrnice o elektronickém obchodu. PSIS poskytující službu, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací, za obsah přenášených informací odpovídá, jen pokud přenos sám iniciuje, zvolí uživatele přenášené informace anebo zvolí nebo změní obsah přenášené informace. Omezení odpovědnosti PSIS se vztahují na všechny oblasti práva včetně trestní odpovědnosti (např. v USA je toto omezení odpovědnosti upraveno zvláštními federálními zákony a trestní odpovědnosti se netýká). Na národní úrovni se ovšem úprava v jednotlivých členských zemích liší. Co se odpovědnosti za ukládaný obsah týče, bude však soud vždy zvažovat, jak uvádí Z. Císařová, vyváženost prostředků k ochraně práv dotčených subjektů ve srovnání se zachováním základních práv a svobod, zejména práva na svobodu slova a práva na svobodu podnikání.²²³ Zde se

²²² Zejména prostřednictvím Směrnice Evropského parlamentu a Rady 2001/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu, ÚL 2000 L 178/8 (dále také jen jako Směrnice o elektronickém obchodu)

²²³ CÍSAŘOVÁ, Z.; *Elektronická data a cloud computing z pohledu autorského práva a ochrany osobních údajů*. Univerzita Karlova v Praze, Právnická fakulta (2012), s. 36

nabízí srovnání s britskou judikaturou, podle které takovouto změnou může být i pouhá změna překlepů a gramatických chyb. V takovém případě se PSIS stává podle britského práva vydavatelem informace, a pokud ji promptně neodstraní, může nést právní následky za její šíření.²²⁴ Je však potřeba doplnit, že Velká Británie je zemí s nadprůměrnou nápadností a také úspěchem žalob na porušení práva na občanskou čest a lidskou důstojnost²²⁵. České právo nerozeznává klasickou solidární odpovědnost PSIS za cizí obsah. Co se odpovědnosti PSIS za vědomost výskytu nezákonného obsahu týče, je založena především na principu upozornění, tzv. Notice and Take Down (NTD) nebo Notice to Take Down and to Stay Down, kdy má být zajištěno také zabránění opětovnému výskytu závadného obsahu v síti. V České republice není zvlášť upravena a ani dosud nebyla vytvořena dostatečná legislativní praxe, na rozdíl od některých členských států Evropské unie, které notifikaci výslovně upravují nebo ustáleně judikují. Česká úprava je na rozdíl od komunitárního práva postavena na pozitivním výčtu případů, kdy je dána odpovědnost providera, což může působit jisté aplikační obtíže a je kritizováno.²²⁶ Systém NTD klade poměrně vysoké nároky na právní oddělení PSISs, nebo jiné osoby pověřené vyřizováním upozornění. Tyto musí přistoupit k rozvažování, zda, vzhledem k okolnostem, představují závažnější právní riziko pro společnost v konkrétním případě případné právní kroky ze strany dotčeného a případné uložení správní pokuty, anebo zda je, např. také s ohledem na politickou situaci v zemi, počet uživatelů a strategičnost trhu, vhodnější riskovat právní následky nevyhovění výzvě²²⁷.

Zákon č. 101/2000 Sb., o ochranně osobních údajů

Tento zákon je formou transpozice směrnice č. 95/46/EC a zohledňuje také požadavky vzešlé z ratifikace Úmluvy Rady Evropy č. 108/1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat v roce 2001. Jedná se o zvláštní

²²⁴ *Kaschke v. Gray and Hilton* [2010] EWHC 690

²²⁵ Zmiňme, že např. ve Velké Británii je připravován nový zvláštní zákon na ochranu občanské cti a lidské důstojnosti, Defamation Bill, Dostupný z vládních stránek WWW: <<http://services.parliament.uk/bills/2012-13/defamation.htm>>

²²⁶ POLČÁK, R.; *Internet a proměny práva*, Auditorium, Praha 2012, s. 149; CÍSAŘOVÁ, Z.; *Elektronická data a cloud computing z pohledu autorského práva a ochrany osobních údajů*. Univerzita Karlova v Praze, Právnická fakulta (2012), s. 37

²²⁷ Více ROSEN, J; Google Gatekeepers [online], *New York Times*, 28. listopad 2008 [cit. 2013-01-05], Dostupný z WWW: <<http://www.nytimes.com/2008/11/30/magazine/30google-t.htm?partner=rss&emc=rss&pagewanted=all>>

úpravu práva na ochranu osobních údajů, která je součástí práva na soukromí. Úprava z tohoto zákona je doplněna ještě zvláštními zákony a zákon má tedy povahu obecného právního předpisu. Tento zákon upravuje právní vztahy mezi subjektem, kteréhož data jsou zpracovávána, tedy v našem případě nezletilé fyzické osoby a mezi správcem, zpracovatelem a případně jiným subjektem. V praxi by se např. jednalo o vztah mezi uživatelem sociální sítě a provozovatelem sociální sítě a případnou třetí osobou, druhotným zpracovatelem dat spravovaných sociální sítí, konkrétně např. reklamní agenturou nebo přímo obchodní společností.

Omezení věcné působnosti tohoto zákona lze ilustrovat na působnosti jeho části zabývající se regulací předávání osobních údajů do zahraničí. „O předávání se nejedná v těch případech, kdy jednotlivec v členském státě vloží osobní údaje na internetovou stránku, která je umístěna u hostitelského správce (providera) sídlícího ve stejném státě nebo v jiném členském státě EU a tato stránka je pak přístupná každému, kdo se připojí k internetu, včetně osob ve třetích zemích. Pokud jsou osobní údaje umístěny na internetovou stránku, nedochází k přímému předání těchto údajů mezi dvěma konkrétními osobami. Jiný případ by nastal, pokud by šlo o akt úmyslného předání, např. mateřská společnost ve Spojených státech amerických by umístila na svých intranetových stránkách zaměstnanecké osobní údaje s cílem je zpřístupnit dalším dceřiným společnostem.“²²⁸ Toto vymezení je důležité především k objasnění právní odpovědnosti zahraničních PSISs, resp. tuzemských PSISs při mezinárodním šíření osobních údajů po internetu. Publikace „Předávání osobních údajů do zahraničí: Česká a evropská právní úprava, otázky a odpovědi“, pak dále uvádí příklad společnosti se sídlem v ČR, která provozuje mezinárodní seznamku, kde jsou profily uživatelů obsahující osobní údaje umístěné na stránkách společnosti a tyto budou využívány především občany EU a USA.²²⁹ Toto je zcela standardní situace většiny sociálních sítí²³⁰ a mnoha dalších internetových platforem.

Na základě rozsudku ve věci *Lindqvist v. Švédsko*²³¹ došlo k ustálení tohoto rozdělení na přenášení údajů nebo jejich dostupnost ze zahraničí. Pokud se budeme chtít

²²⁸ MORÁVEK, J., BURIAN, D.; *Předávání osobních údajů do zahraničí: Česká a Evropská právní úprava, otázky a odpovědi*, Linde Praha, a.s., 2012, s. 170

²²⁹ MORÁVEK, J., BURIAN, D.; *Předávání osobních údajů do zahraničí: Česká a Evropská právní úprava, otázky a odpovědi*, Linde Praha, a.s., 2012, s. 178

²³⁰ Těch, které, např. z daňových důvodů, jako Facebook, mají sídlo v některé z členských zemí EU.

²³¹ *Lindqvist v. Švédsko* C-101/1

poukázat na zcela flagrantní příklad porušení Zákona o ochraně osobních údajů ve vztahu k nezletilým, můžeme tak učinit následujícím příkladem. Ten je důležitý také z toho důvodu, že se jedná o situaci, kdy si lze představit úspěšné podání žaloby na ochranu osobnosti nezletilým, do jehož práva na soukromí bylo vážným způsobem zasazeno. Případ je navíc velmi vážný kvůli kombinaci zveřejnění citlivých a osobních údajů, a zejména z důvodu zpřístupnění údajů nezletilých osob, týkajících se jejich rasové příslušnosti, sociální příslušnosti a kontaktních údajů. Ministerstvo školství, mládeže a tělovýchovy zveřejnilo v listopadu 2011 osobní a citlivé údaje o 893 romských studentech středních či vyšších odborných škol, jejichž studium bylo finančně podporováno v rámci dotačního programu zprostředkovaného ministerstvem. Tabulka veřejně přístupná na stránkách ministerstva, obsahovala jména studentů, jejich adresy, data narození, a dále seznam škol, které dotace na tyto studenty čerpaly, tedy informaci o tom, kam tito docházejí do školy, a konkrétní částky, které škola čerpá. Těchto škol bylo na seznamu uvedeno 181. Aktuální rozhodnutí ÚOOÚ o uložení správní pokuty ve výši 450 000 Kč ministerstvu školství se stalo pravomocným teprve v říjnu 2012, tedy téměř po roce od události. Zdůraznit lze, že se jednalo o správní pokutu, a že tato částka tedy nebyla určena obětem.²³²

Zákon č. 94/1963 Sb., o rodině ve znění pozdějších předpisů

Tento zákon představuje, ve vztahu k tématu této práce regulaci obecného, široce zastoupeného předpokladu, že rodič má veškerá práva a povinnosti k dohledu a korekci kybernetických interakcí nezletilého dítěte, s cílem ochrany jeho bezpečnosti, tedy, že v rámci plnění rodičovských povinností je odpovědností především rodiče, aby ochránil dítě před škodlivými vlivy a právním ohrožením či zásahem v kyberprostoru. To může být, vzhledem k důvodům uvedeným v rozboru specifik osobnosti nezletilého uživatele SIS a jeho jednání v kyberprostoru, nezřídka pro rodiče poměrně nesnadné. Zásadní odpovědnost nesou, v rámci svých pravomocí, také školská zařízení, ta však především za vlastní aktivity potenciálně způsobilé ohrožení nebo zásahu do osobnostních práv nezletilého. Zajímavý pohled na otázku povinnosti chránit nezletilého přineslo rozhodnutí Evropského soudu pro lidská práva ve věci *KU v.*

²³² Ministerstvo školství dostalo pokutu 450 tisíc za únik dat o Romech [online] *Eurozpravy* [cit. 2012-08-12]. Dostupný z WWW: <<http://domaci.eurozpravy.cz/skolstvi/53026-ministerstvo-skolstvi-dostalo-pokutu-450-tisic-za-unik-dat-o-romech/>>

*Finland*²³³, kde soud zdůraznil odpovědnost také státu za ochranu osobnostních práv nezletilých dětí. Shledal Finsko právně odpovědným za nedostatečné poskytnutí prostředků nápravy v případě, kdy bylo porušeno právo na soukromí a na občanskou čest a lidskou důstojnost 12ti-letého chlapce neznámou fyzickou osobou. Protože národní právo neumožňovalo efektivně vymáhat stažení závadného obsahu na PSIS, došlo k zásahu do osobnostních práv nezletilého dítěte také státem.

Zákon č. 40/2009 Sb., trestní zákoník

Je-li cílem této kapitoly pokusit se o co nejkompaktnější přehled právní úpravy ochrany osobnostních práv v České republice, je nutné dotknout se alespoň okrajově také několika institutů trestního práva. Jednat se bude především o skutkové podstaty související s výrobou nebo šířením dětské pornografie, násilnou trestnou činností páchanou na dětech, ohrožování výchovy a dále o jednání naplňující skutkovou podstatu pomluvy nebo porušení tajemství listin a jiných dokumentů uchovávaných v soukromí²³⁴ a o jednání naplňující nové skutkové podstaty inkorporované do trestního zákoníku s cílem potlačování kybernetické kriminality, jako je např. již zmiňované ustanovení § 230 odst. 1 zákona č. 40/2009 Sb., trestního zákoníku (dále také jen jako TZ).

Právní prostředky nápravy dostupné nezletilému uživateli podle platného českého práva

Český uživatel má hned několik možností, jak na závadný obsah zasahující do jeho osobnosti upozornit. Postupovat bude ideálně dvěma cestami, jejichž kroky by měly být buď souběžné, nebo následovat alespoň bezprostředně po sobě. Uživatel může v mnoha případech, např. na sociální síti, využít ohlašovací funkci. Ta však nezřídka není, zejména nezletilým uživatelům, zcela srozumitelná a setkat se lze i se zdlouhavostí reakce na tuto formu upozornění²³⁵. Další možností je využití formuláře,

²³³ Rozhodnutí ESLP z 2. prosince 2008, *K.U. v. Finland* Application no. 2872/02

²³⁴ Především § 180 Neoprávněné nakládání s osobními údaji, § 181 Poškození cizích práv nebo § 182 Porušení tajemství dopravovaných zpráv, § 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (kde se lze domnívat, že za soukromí lze považovat také model soukromí v rámci kyberprostoru) a § 184 Pomluva.

²³⁵ „U každého profilu/stránky je tlačítko „Nahlaste stránku/tuto osobu“, tzv. „report button“ – po kliknutí dostanete možnost vybrat důvod nahlášení a tlačítkem „Odeslat“ se hlášení odešle do zákaznického centra Facebooku, kde případ budou řešit. Toto řešení má ovšem následující problém: vyšší prioritu při řešení

opět např. sociální sítě, sloužícího k upozornění na konkrétní zásah závadného obsahu²³⁶ do zaručených práv uživatele. Je pravdou, že, na první pohled jasné případy šikany, byly řešeny stažením závadného obsahu, pokud by se však také vkladatel dat rozhodl domáhat se svých práv k odstraněnému obsahu, situace by mohla být o poznání složitější. Další možností pro uživatele je využít tzv. Horké linky²³⁷, která podrobuje nahlášený závadný obsah obdobné analýze jako jednotliví PSISs a následně komunikuje zrychlenou cestou přímo s příslušným týmem v ústředí PSIS, a to i v zahraničí. Ani tato iniciativa však neposkytuje dotčenému plně efektivní právní ochranu. „Vyškolení pracovníci hlášení vyhodnotí v souladu s platnými předpisy a zpracované podněty předají příslušným orgánům k přijetí nezbytných opatření, která zamezí dalšímu šíření tohoto obsahu. V České republice platí, že pouze soud může rozhodnout o nelegálnosti nahlášeného obsahu, čili o jeho trestnosti (*sic*). Horká linka tedy nemůže, a ani k tomu není určena, odstranit či jinak znepřístupnit nahlášený obsah.“²³⁸ Z toho vyplývá, že Horká linka je tedy pouhým prostředníkem, který může díky spolupráci se sítí INHOPE, podporované Evropskou komisí, která sdružuje internetové horké linky zahraničních center, upozornit na závadný obsah i s uživateli běžně špatně komunikující zahraniční PSISs. Nově má pro hlášení závadného obsahu sloužit také jednoduchý on-line formulář pro hlášení závadového obsahu a aktivit v síti internet na stránkách Policie ČR. Ten ale nenahrazuje elektronickou podatelnu Policie České republiky, a tudíž se nejedná o podání dle ustanovení § 59 zákona číslo 141/1961 Sb., o trestním řízení soudním, ani dle ustanovení § 37 zákona č. 500/2004 Sb., správního řádu.²³⁹

Nejčastěji bude postupováno proti jinému uživateli, alternativně, proti uživateli a PSIS, který nesjednal nápravu²⁴⁰, jak bude ilustrováno níže v aktuálním případě z USA. I přes naprostý nedostatek judikatury pro tento postup lze jako příklad užít případ

mají stránky/osoby s vyšším počtem hlášení, tj. vyšším počtem stisknutí „report button“. Stránky v češtině a reakce na ně nedosahují zpravidla četnosti jiných jazykových verzí a tím se řešení ohlášeného problému může protáhnout.“ Zdroj: horkalinka.net / Facebook: Jak na stížnosti na Facebooku? Dostupný z WWW: <<http://www.horkalinka.net/facebook>>

²³⁶ Dostupný z WWW: <<http://www.facebook.com/help>>

²³⁷ „Horká linka je kontaktní centrum, které přijímá hlášení, týkající se nezákonného a nevhodného obsahu na internetu, jako je dětská pornografie, dětská prostituce, obchod s dětmi, pedofilie, věkově nepřiměřený obsah, sexuální praktiky, rasismus, xenofobie, sebepoškození, výzvy k násilí a nenávisti, šíření drog atd. (...) Horkou linku provozuje CZI s.r.o. v rámci evropského projektu Saferinternet.cz. a ve spolupráci s Národním centrem bezpečnějšího internetu, Českou policií a organizací INHOPE.“ Zdroj: <<http://www.horkalinka.net/>>, informační materiál Horka linka

²³⁸ Dostupný z WWW: <<http://www.horkalinka.net/>>

²³⁹ Policie ČR, Prevence, Dostupný z WWW: <<http://aplikace.policie.cz/hotline/>>

²⁴⁰ Podle zvláštního zákona, který také značně omezuje jeho právní odpovědnost.

čtrnáctileté Alex Boston ze státu Georgia v USA. Nezletilá žákyně prostřednictvím svého zákonného zástupce, zde matky, podala žalobu na několik svých spolužaček spolu se společností Facebook. Dívky zneužily její jméno a podobu, založily dívce falešný profil na sociální síti Facebook, kam tyto jejím jménem zasílaly škodlivý obsah, a jejím jménem také vynášely v textové podobě rasistické a sexuálně explicitní výroky. Když se dívka o profilu dozvěděla, kontaktovala opakovaně společnost Facebook se žádostí o stažení falešného profilu. Protože se tak ani po mnoha upomenutích nestalo, dívka přistoupila k žalobě. Problémem amerického práva dále je, že sice mnoho států přijalo zákony zabývající se šikanou a kyberšikanou, tyto se však ve valné většině případů nevztahují na aktivity mimo prostory školy.²⁴¹ PSISs, jejichž právní odpovědnost je výrazně omezena zvláštními zákony, se nezdá snažit Podmínkami užívání svou limitovanou odpovědnost rozšířit nad rámec zákona.²⁴² Bude-li fyzická osoba dotčena např. zásahem do soukromí sběrem a užíváním dat, může se pro rychlou nápravu obrátit na ÚOOÚ. Ten však jen rozhodne např. o zastavení závadné činnosti PSIS, kterému může případně uložit správní pokutu. Dotčenému se tak ale nedostává žádné satisfakce, a navíc, pokud bude závadný stav „pouze“ porušením práva na ochranu osobnosti, ale nebude v rozporu s výše uvedenými zvláštními zákony, ÚOOÚ k zásahu nepřistoupí. Vzhledem k povaze činnosti PSIS a množství zpracovaných dat v praxi podle zvláštního zákona přichází v úvahu v zásadě pouze vědomá nedbalost PSIS, který se dozvěděl o protiprávní činnosti na svém serveru a nepodnikl nutná opatření.

Občanskoprávní žaloba na ochranu osobnosti je podle autorky této práce právním prostředkem, který pro osobnostní zásahy v kyberprostoru není doposud dostatečně využíván, a to zejména ve vztahu k nezletilým. Podle platného českého práva, by tedy typický postup nezletilého uživatele²⁴³, do jehož osobnostního práva bylo v kyberprostoru zasaženo, byl následující: nejprve by kontaktoval PSIS s upozorněním

²⁴¹ Georgia Girl Sues Classmates For Bullying Her On Facebook [online] *CBS Atlanta* 1. květen, 2012 [cit. 2012-12-11]. Dostupný z WWW: <<http://atlanta.cbslocal.com/2012/05/01/georgia-girl-sues-classmates-for-bullying-her-on-facebook/>>

²⁴² Např. společnost Facebook v podmínkách užívání služby, konkrétně v bodě 16. Spory upozorňuje uživatele: „Pokud vůči nám někdo podá žalobu týkající se vašich kroků, obsahu nebo informací na Facebooku, odškodníte nás v souvislosti s touto žalobou za veškeré škody, ztráty a výdaje jakéhokoli druhu (včetně přiměřených poplatků a nákladů na právní zastoupení).“ Dále v odst. 2 je ještě zdůrazněno, že Facebook neodpovídá za obsah ani informace ukládané na uživatelském profilu, což je sice odpovídá obecně platné právní úpravě, ale odpovědnosti není PSIS zbaven vždy.

²⁴³ Nejčastěji prostřednictvím svého zákonného zástupce

a zároveň co nejdříve podal žalobu k příslušnému obecnému soudu a tento soud požádat o provedení předběžného opatření. V této souvislosti je však nutné připomenout zejména rozhodnutí Vrchního soudu v Praze²⁴⁴, podle kterého předběžné opatření nesmí omezovat svobodu projevu. Mimoto by, tam, kde je to možné, kontaktoval uživatel Úřad pro ochranu osobních údajů (dále také jen jako ÚOOÚ) se žádostí o předběžnou právní ochranu. Tento věc posoudí a případně, tam, kde je to možné, uloží zajištění nápravy, případně spolu se správní pokutou. Ačkoli většina velkých PSISs prostřednictvím jejichž služeb dochází často k zásahům do osobnostních práv, se snaží na základě upozornění obětem podobných jednání co nejrychleji vyhovět, rozhodně není na místě na podobnou reakci spoléhat. V tomto smyslu poskytuje jisté upozornění také česká Horká linka, a to s odůvodněním nízké relevance a rozsahu českého trhu z pohledu např. světových sociálních sítí, které jsou faktory zpomalujícími reakci PSIS na upozornění. Nejen v českém právním prostoru by celý výše uvedený proces mohl trvat od několika týdnů až po roky. Proto se lze zamyslet nad právem tvořeným praxí v informační společnosti. Zásahy v kyberprostoru vyžadují řešení v kyberprostoru.

Problém mezinárodního prvku právních vztahů v kyberprostoru

Řešení porušování práva, vzhledem k předmětu této práce může znesnadňovat skutečnost, že se nezřídka může jednat o soukromoprávní vztahy s mezinárodním prvkem. Příkladem může být situace, kdy nezletilý je oprávněným uživatelem služby, tedy, až na výjimky, je starší 13 let a jeho užívání služby by se teoreticky mělo řídit smluvními podmínkami ve formě Podmínek užívání (služby), které mohou mimo jiné určovat již dopředu také příslušnost zahraničních soudů a práva, kterým se tento vztah řídí. Proti tomu však může stát přímo aplikovatelné právo EU.²⁴⁵ Případy, kdy osobnostní právo nezletilého občana České republiky bude v oblasti kyberprostoru zasaženo fyzickou nebo právnickou osobou sídlící v zahraničí tak budou znesnadněny nejen nutností uvážení jak soudní pravomoci, ale i rozhodného práva. S ohledem na okolnosti bude příslušnost práva a soudu určována různými způsoby.

²⁴⁴ Co 16/ 94, Právní rozhledy č. 3/1995

²⁴⁵ Takovýmito právními předpisy mohou být např. také nařízení Řím I (č. 593/2008), respektive nařízení Řím II (č. 864/2007), které obsahuje normy pro určení rozhodného práva pro smluvní a mimosmluvní závazky, kde obě strany jsou ze zemí EU nebo nařízení Brusel I (č. 44/2001), které se použije pro určení příslušnosti soudu u většiny sporů z oblasti občanského nebo obchodního práva nebo pro rozhodování o uznání a výkonu rozhodnutí z jiných zemí EU.

Význam má ale také judikatura, a to již v samém počátku sporu. Zasahující, v případech sporů mezi uživateli, může, a často bude, jednat anonymně, a bude tak potřeba, aby PSIS poskytl jeho uživatelská data. K tomu však podle interpretece příslušných směrnic, ke které došel Evropský soudní dvůr ve věci *Promusicae*²⁴⁶ „není povinen tam, kde se jedná o občanskoprávní spor. Bude tomu tak v případě, že konkrétní členský stát z vlastní iniciativy nepřijal zákon o vydávání informací PSIS v občanskoprávním řízení“²⁴⁷ V ostatních případech se bude vycházet zejména z mezinárodních dohod, a to jak co se určení příslušnosti práva nebo soudu týče, tak v otázkách uznávání a výkon rozhodnutí.

V případech, kterými se zabývá tato práce, může však také dojít k situaci, kdy zasahujícím bude subjekt se sídlem, resp. pobytem mimo EU a zároveň tento stát, kde je zasahující právně vázán neuzavřel jurisdikční ani jinou podobnou dohodu s Českou republikou nebo jinou zemí EU²⁴⁸. Tuto otázku bude řešit nový Zákon o mezinárodním právu soukromém (NZMPS)²⁴⁹ nabývající účinnosti od 1. ledna 2014. Tématu této práce se budou týkat zejména ustanovení § 101, které upravuje mimosmluvní závazkové poměry vznikající z narušení soukromí a osobnostních práv včetně pomluvy. Ačkoli se tyto spory běžně řídí právem státu, ve kterém k narušení došlo, postižená osoba si může zvolit právo státu, ve kterém má buď obvyklý pobyt nebo sídlo nebo právo státu, ve kterém se dostavil výsledek narušujícího jednání, pokud to původce narušení mohl předvídat anebo práva státu, kde má původce narušení obvyklý pobyt nebo sídlo. V této souvislosti lze připomenout rozhodnutí ve spojených věcech *eDate Advertising GmbH proti X a Olivier Martinez a Robert Martinez proti MGN Ltd.* (viz. dále).

Vzhledem k tomu, že se tato práce také zabývá otázkou možnosti řešení sporů z porušení osobnostních práv na internetu prostřednictvím alternativních způsobů řešení sporů, zmiňme ještě část sedmou tohoto zákona, ustanovení § 117 - § 122, která poměrně volně upravují rozhodčí řízení a uznávání a výkon cizích rozhodčích nálezů. To může mít význam také v těch situacích, kdy se uživatel SIS registrací zaváže ke

²⁴⁶ C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España SAU*

²⁴⁷ *Commission of the European Communities v. Kingdom of Belgium, C-275/04*

²⁴⁸ BRÍZA, P., Nový zákon o mezinárodním právu soukromém je pro praxi přínosem [online] *iDnes*, 18. srpen 2012 [cit. 2012-11-28]. Dostupný z WWW: <http://finance.idnes.cz/novy-zakon-o-mezinarodnim-pravu-soukromem-je-pro-praxi-prinosem-phk-/pravo.aspx?c=A120817_155730_pravo_vr>

²⁴⁹ Zákon č. 91/2012 Sb., o mezinárodním právu soukromém

smluvnímu ujednání s rozhodčí doložkou s určením příslušnosti rozhodčímu orgánu mimo území ČR, resp. mimo EU ale také pro přípravu takové rozhodčí doložky, která by umožňovala rychlé řešení sporů prostřednictvím „rozhodčího soudu pro internet“, tedy formou Online Dispute Resolution (ODR), které nalézáme v ČR již v oblasti spotřebitelských sporů s mezinárodním prvkem vzniklých na internetu.²⁵⁰

Odpověď na otázku, zda se PSIS může rovnat odpovědnostně především vydavateli tištěných médií v USA vyřešil Communication Decency Act, který jasně stanovil, že z pohledu amerického práva, PSIS není vydavatelem. Stejnou otázkou se pak zabýval např. britský Ústavní soud. Zde je situace méně jednoznačná, protože na základě rozhodnutí soudu ve věci *Laurence Godfrey v. Demon Internet Ltd.*²⁵¹, přenos difamačních informací ze serveru uložitelé zpráv představuje publikování kterémukoliv odběrateli těchto zpráv, který složku (nebo feed²⁵²) otevřel. Na druhou stranu ve věci *Metropolitan International Schools Ltd. v. Designtecnica Corp., Google UK Ltd. a Google Inc.*²⁵³ Ústavní soud došel k závěru, že PSIS poskytující službu vyhledavače Google takovou právní odpovědnost za přenos difamačního obsahu nenese. Soud se přiklonil k názoru, že zásadní význam má, že pokud PSIS zavedl a úspěšně aplikuje postupy stažení nahlášeného závadného obsahu (NTD), pak nenese právní odpovědnost za obsah vložený třetí stranou. Roli pochopitelně hraje i povaha konkrétní služby.

Na tomto místě by mělo být připomenuto rozhodnutí Evropského soudního dvora ve spojených věcech *eDate Advertising GmbH proti X a Olivier Martinez a Robert Martinez proti MGN Ltd.*²⁵⁴. Zde přímo velký senát přinesl zásadní právní názor na otázku, nakolik lze ve věci zásahu do osobnostních práv, kde prostředkem zásahu je obsah internetové stránky, užít judikaturu vytvořenou, a doposud se vztahující, na tištěná média. Soud zjišťoval aplikovatelnost rozhodnutí ve věci *Sevilla a další proti PresseAlliance*²⁵⁵, kde soud dospěl k názoru, že žalobu na náhradu nemajetkové újmy lze podat u soudu toho státu, v němž je vydavatel usazen, a to pro rozhodování o celém

²⁵⁰ LOEBL, Z.; Řešení reklamací on-line otevře e-shopům nové trhy [online] *Hospodářské noviny*, 25. květen, 2012 [cit. 2012-09-22]. Dostupný z WWW: <<http://hn.ihned.cz/c1-55872670-zbynek-loebl-reseni-reklamaci-on-line-otevre-e-shopum-nove-trhy>>

²⁵¹ *Laurence Godfrey v. Demon Internet Ltd.*, QBD [1999] 4 All ER 342 [2000] 3 WLR 1020; [2001] QB 201

²⁵² Feed (ang.) je přísun zasílaných aktualizovaných informací od jednoho zdroje podle volby uživatele, např. pravidelné zpravodajství.

²⁵³ [2009] EWHC 1765 (QB)

²⁵⁴ C-509/09 a C-161/10

²⁵⁵ C-68/93

vzneseném nároku. V jiných státech, v nichž byl článek zveřejněn nebo kde došlo k poškození pověsti, žalobce bylo možné variantně rozhodovat o dané újmě jen v rozsahu, v jakém se týkala dotčeného státu.²⁵⁶ V tomto případě, resp. v uvedených spojených věcech však ESD rozhodl, že na kyberprostor nelze aplikovat stejné normy jako na tištěná média, tedy logicky odmítl přístup zohledňující stát, kde byl článek vydán. Soud tak rozhodl z důvodu, že „rozsah šíření obsahu informací na internetu je v zásadě univerzální. Navíc z technického hlediska není vždy možné tento rozsah šíření s určitostí a spolehlivostí kvalifikovat ve vztahu ke konkrétnímu členskému státu (EU), a proto ani ohodnotit újmu způsobenou výlučně v tomto členském státě.“²⁵⁷ Oproti tomu se ESD přiklonil k názoru, že dopad zásahu do osobnostních práv žalobce by měl být vyhodnocen soudem v zemi, kde se nalézá „centrum zájmů“ žalobce. Ačkoli podle obecného předpokladu toto bude země, kde žalobce trvale pobývá, ESD dochází k závěru, že také jiný členský stát EU může být státem, kde lze podat žalobu, pokud „jiné indicie, jako například výkon profesní činnosti, mohou prokázat zvláště úzkou vazbu k tomuto státu“.²⁵⁸ Právní odpovědnost pak soud odvozuje od možnosti vydavatele předvídat, která ze zemí EU je centrem zájmů žalobce. Žalobce může žalovat PSIS nebo jinou osobu právně odpovědnou za obsah konkrétních internetových stránek, které zprávu zveřejnily i v zemi, kde má bydliště nebo která je prokazatelným centrem jeho zájmů a zde také žádat plnou náhradu nemajetkové újmy v penězích, ale žalobce může dále také podat žalobu v každém ze států EU, kde byla informace dostupná na internetu. Každý z těchto soudů se však bude zabývat pouze újmou způsobenou v tomto konkrétním státě.²⁵⁹ Z článku P. Břízy dále vyplývá, že toto zásadní rozhodnutí by se v rozhodovací praxi nemuselo vztahovat pouze na PSIS ve formě internetového šíření tisku. To by kladlo výrazné požadavky na nezávadnost obsahu mnoha internetových stránek.

Výše popsané rozhodnutí by mohlo posloužit žalobci k tomu, aby žaloval médium v zemi, ve které se nejčastěji zdržuje, a kde je tedy difamační dopad vpádu do jeho osobnostních práv nejzásadnější. Vyřešení spornosti aplikovatelnosti tohoto

²⁵⁶ BŘÍZA, P., Jak na internetové pomluvy [online], *Právo a Byznys*, 50/2012 [cit. 2012-09-23]. Dostupný také z WWW: < <http://zpravy.e15.cz/pravo-a-byznys/jak-na-internetove-pomluvy-833835>>

²⁵⁷ Bod 46 rozhodnutí

²⁵⁸ Bod 49 rozhodnutí

²⁵⁹ BŘÍZA, P., Jak na internetové pomluvy [online], *Právo a Byznys*, 50/2012 [cit. 2012-09-23]. Dostupný také z WWW: < <http://zpravy.e15.cz/pravo-a-byznys/jak-na-internetove-pomluvy-833835>>

rozhodnutí na běžné PSIS nabízí úvaha o uplatnění této konstrukce tam, kde ponese provozovatel odpovědnost jako majitel. Tímto způsobem by je již za pronásledování nebo difamaci žalovat možné bylo.

4.3. Právní úprava ochrany osobnosti nezletilých v EU

Úvod: Prameny evropského práva na ochranu osobnosti

Předmětem této práce, mimo české právní úpravy dané problematiky a exkurzu do práva amerického, je platná právní úprava v EU a především připravovaný balíček regulace ochrany osobních údajů uživatelů internetu v čele s návrhem Komise a Rady č. COM(2012) 11 final²⁶⁰.

4.3.1. Platná právní úprava v EU

Listina základních práv EU (2000)

„Listinou (základních práv EU z roku 2000, *pozn. autorky*) se nerozšiřují pravomoci Unie upravené Smlouvami, nýbrž zakotvují se zejména principy obsažené již v judikatuře Soudního dvora a vycházející kromě jiného z Evropské úmluvy o ochraně lidských práv a základních svobod přijaté Radou Evropy v roce 1950.“²⁶¹ Zásadní význam pro tuto práci má její Článek 8, který zaručuje, že každý člověk má právo na ochranu údajů osobního charakteru, které se ho týkají a dále, že s těmito údaji musí být nakládáno čestně, pouze k přesně danému účelu a na základě souhlasu dotyčné osoby či na základě jiného legitimního opodstatnění uvedeného v zákoně a konečně, že každý člověk má právo na přístup k údajům shromážděných o jeho osobě a na jejich opravu. To má význam zejména vzhledem k názoru autorky této práce, že zásah do práva na ochranu osobních údajů by měl být častěji posuzován jako zásah do práva na ochranu osobnosti.

²⁶⁰ COM(2012) 11 final

²⁶¹ Listina základních práv EU [online]. *Euroskop*. Dostupný z WWW: <<https://www.euroskop.cz/204/sekce/listina-zakladnich-prav-eu/>>

Směrnice 95/46/EC o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Směrnice 95/46/EC (Datová směrnice) vytvořila jednotný základ pro ochranu dat mezi všemi členskými zeměmi EU. „Zavádí právní rámec, jehož cílem je ustavení rovnováhy mezi vysokou úrovní ochrany soukromí jednotlivců a volným pohybem osobních údajů v rámci Evropské unie (EU).²⁶²“ Pro mnoho právních řádů členských zemí EU je typické, že stejný zákon reguluje nakládání s osobními údaji a ochranu soukromí fyzických osob jak ve vztahu k veřejnoprávnímu, tak k soukromému sektoru. Základními úkoly směrnice byla unifikace datového práva v rámci EU, kladení důrazu na obecnost právní úpravy, oproti sektorálnímu modelu v USA a vytvoření základních povinností pro zpracovatele osobních údajů. Nejdůležitějšími oblastmi regulace bylo technologické zabezpečení a povinnost upozornění uživatelů na sběr jejich osobních údajů. Dále směrnice upravuje také pohyb dat a dává uživatelům právo kontroly nad tím, jaké osobní údaje jsou o nich shromažďovány a jak je s nimi nakládáno. Tato práva jsou konkrétně představována právem na informace o shromažďovaných datech, která jsou přenášena, povinností zpracovatele získat výslovný souhlas uživatele s pohybem dat, právem uživatele odmítnout přesun a další nakládání s daty anebo právem uživatele na zanesení změn a oprav do dat. Směrnice dále zahrnuje ustavení národních kontrolních orgánů, právní prostředky vymáhání směrnici zaručených práv a sankce za její porušení. Zcela zásadní význam má pak pro předmět této práce článek 25. Směrnice, který zavazuje směrnici také zpracovatele dat ze zemí mimo EU.

Forma směrnice členskými státy poskytuje logickou volnost v začlenění do národního práva. Tak například směrnice o elektronickém obchodu nebyla do českého práva transponována v plném rozsahu a tak, na rozdíl od providerů v některých jiných členských zemích EU, nemají čeští provideri povinnost informovat příslušný správní orgán o podezření na protiprávní činnost nebo výskyt protiprávních informací²⁶³. Jak říká Peter Sire, z právnické fakulty Moritz College: „Ačkoliv směrnice vedla k mimořádnému sblížení práv na ochranu dat, harmonizace této oblasti práva není ještě ani zdaleka kompletní. Vlastní vymáhání práva se neřídí zněním směrnice. Namísto toho musí členské státy EU přijmout odpovídající prováděcí zákony, které budou

²⁶² Dostupný z WWW:

<http://europa.eu/legislation_summaries/information_society/legislative_framework/124120_cs.htm>

²⁶³ Čl. 15 (2) směrnici Evropského parlamentu a Rady 2000/31/ES

představovat implementaci směrnice. Tyto jednotlivé právní úpravy se budou lišit ať již v detailech nebo i v zásadnějších otázkách. Míra snahy o zajištění vymahatelnosti práva se pak také bude nepochybně lišit v jednotlivých zemích, a to s ohledem na různé náhledy na nejlepší cestu regulace a na různou úroveň dostupných prostředků pro zajištění vymahatelnosti práva a lišící se zkušenosti s touto problematikou.²⁶⁴

Výše nastíněná právní rozštěpenost tak má za následek, že v evropském prostoru nelze mluvit o právu na ochranu soukromí EU, ale pouze o právu evropském, či ještě přesněji o právu evropských zemí. Tento stav má však zásadní důsledky vzhledem k často nevyhnutelnému mezinárodnímu prvku právních vztahů vznikajících v kyberprostoru. V situaci, kdy je tento prostor typický relativní formální nestabilitou, je absence jednotné právní úpravy nežádoucí. Komisařka EU pro spravedlnost Viviane Reding odhaduje, že nadbytečné překážky způsobené individuální aplikací nekonsistentních národních práv na ochranu soukromí vytváří pro společnosti v evropském prostoru mimořádné náklady ve výši 2.3 miliard Euro ročně.²⁶⁵

Lze shrnout, že mimo platného datového balíčku tvoří evropský právní základ ochrany osobnostních práv nezletilých v kyberprostoru, sít tvořená ustanoveními mezinárodních úmluv a dalšími právními nástroji²⁶⁶. Vzhledem k obecně problematictější vymahatelnosti, nejednotné závaznosti a odlišnosti úpravy v jednotlivých členských zemích, a zejména u některých třetích zemí, lze ale konstatovat, že nová právní úprava je nutná, a to nejen z důvodu rychlého vývoje technologií, které má regulovat.

²⁶⁴ SOLOVE, Daniel J., SCHWARTZ, Paul M.; *Information privacy law*. 4. vyd., Aspen Elective Series, Wolters Kluwer Law and Business, 2011. s. 1124. ISBN 0735510407

²⁶⁵ PFANNER, E., A Proposal for E.U.-Wide Data Protection Regulation, *N.Y. Times*, 20. listopad, 2011

²⁶⁶ Nejdůležitějšími nástroji ochrany práv dětí, resp. nástroji umožňujícími vytvoření právního rámce této ochrany jsou: Všeobecná deklarace lidských práv, 1948, Článek 25, 26 odst. 3, Evropská úmluva o ochraně lidských práv a základních svobod, 1950, kde zásadní význam má Článek 8 a která ale neupravuje výslovně právo na ochranu osobních údajů, které se tak vyvinulo pouze judikaturou Evropského soudu; Listina základních práv EU (2000) zejména článek 24. Dalšími podpůrnými relevantními úmluvami jsou: Helsinská deklarace, Mezinárodní pakt o hospodářských, sociálních a kulturních právech, především její článek 10, odst. 3; Mezinárodní pakt o občanských a politických právech 1966, konkrétně článek 16 a 24. Dalšími nástroji, které přímo souvisí s právy dítěte, jsou Ženevská deklarace práv dítěte a Úmluva OSN o právech dítěte, konkrétně článek 6 (2), 12 (1), 13 (1), (2) a), b), 16 (1), (2) a dále Evropská úmluva o výkonu práv dětí, Rada Evropy, č. 160, 1996 a Deklarace OSN o právech dítěte

4.3.2. Návrh reformy právní ochrany uživatelů internetu v EU

Návrh Komise COM(2012) 11 final na jednotnou právní regulaci ochrany osobních údajů uživatelů internetu prošel od svého zveřejnění 25. ledna 2012 podstatnými změnami. Jak z parlamentních diskuzí, tak posléze i z oficiálních vyjádření vyplynulo, že striktní forma nařízení byla opuštěna a právní úprava bude mít měkčí podobu²⁶⁷. Při rozboru změn relevantních pro téma této práce, které Návrhu Komise přináší, je nutné si uvědomit, že ačkoli jistě ještě podlehne mnoha dílčím změnám, jedná se o širokou a stále striktní úpravu, která má potenciál stát na počátku nového přístupu k ochraně osobnosti v kyberprostoru. Srovnání analýzy Návrhu americkou advokátní kanceláří Cooley²⁶⁸ a odborného článku na toto téma, jehož autorem je německý právník Christopher Kuner²⁶⁹ může poskytnout cenný rozměr ve srovnání amerického a evropského přístupu k tomuto zásadnímu právnímu aktu. Ačkoli se v prvních měsících po zveřejnění znění návrhu Komise bylo možné setkat s převážně zamítavými názory z americké strany, nelze než souhlasit s prognózami, které budoucnost této regulace vidí jako významný první krok ke skutečně mezinárodní efektivní právní regulaci kyberprostoru, jejíž implementace bude však založena na nutných kompromisech, a to nejen mezi postojí USA a EU. Výsledkem těchto jednání bude pravděpodobně také revize principů Safe Harbor.

Úprava působí na obě strany, tedy jak na PSISs, kterým dává jasnou zprávu, že EU není ochotna dále podporovat systém převážně samoregulační úpravy ochrany osobních dat, a že doposud velmi volný pohyb v jednání PSISs bude regulován, kontrolován a v případě nesouladu sankcionován, a to vše jednotnou evropskou úpravou, která, zajistí lepší vymahatelnost práva, ale také vyšší úroveň právní jistoty právě pro PSISs. Na uživatele pak působí v tom smyslu, že pokud bude doprovázena náležitou informační kampaní, může efektivně suplovat osvětu v oblasti práv uživatelů. Návrh Komise je symbolickou sumarizací trendů v ochraně uživatelů internetu, který se rozšiřuje i mimo USA a EU. Zájem na daleko výraznější ochraně uživatele lze číst jak z psaného práva, tak judikatury z posledních let např. také v Austrálii, Kanadě nebo Jižní Koreji.

²⁶⁷ srov. rozbor Návrhu

²⁶⁸ čerpáno také výše, Cooley, How Proposed EU-Wide Data Protection Regulation Will Affect U.S. Based Businesses, 12. leden 2012, Dostupný z WWW: <<http://www.cooley.com/showalert.aspx?Show=66023>>

²⁶⁹ z tohoto rozboru čerpáno také srov. dále

Některé z hlavních změn, které Návrh přináší, budou shrnuty v následující části práce. Místní působnost se týká nejen těch, kteří data skutečně zpracovávají, ale i těch, kteří provozují služby zaměřené na obyvatele, tedy nikoli nutně občany EU. Každý takový PSIS musí také mít svého zástupce v EU. PSISs musí pro tyto zajistit dostatečné zázemí pro umožnění plnění procesů zajišťujících ochranu práv uživatelů spočívající v jejich nároku vyplývajícím z evropské právní úpravy osobních údajů na internetu, který obsahuje především právo uživatele, na základě žádosti, na informace o povaze dat a způsobu jejich zpracování, které se ho týká. Veškeré tyto informace musí PSIS uživateli poskytnout nejpozději do 1 měsíce od podání žádosti. V Návrhu lze číst obecnou snahu aktivovat přístup PSISs k ochraně údajů a iniciovat jejich zásadnější podíl na této ochraně, a dále zamezení obcházení práva ze strany PSISs. To vyplývá také z ustanovení, které nárokuje soulad tzv. webové architektury s požadavky Návrhu na ochranu osobních údajů²⁷⁰. Dále musí PSISs vést podrobné záznamy o způsobu zpracovávání osobních údajů uživatelů, které pravidelně zpřístupní a dále dokumentuje každé jednotlivé naložení s osobními údaji a informace o něm na vyžádání předloží národním orgánům, např. ÚOOÚ. Návrh se zabývá také problémem PII²⁷¹, když požaduje výslovný souhlas uživatele se sběrem dat, která jsou takové povahy, že buď samostatně, nebo v kombinaci s jinými daty mohou identifikovat konkrétní osobu nebo na jejichž základě může docházet k vytváření profilu u této, tedy jakési složky o uživateli poskytující mnohovrstevné informace o jeho životě. Dochází tak celkově ke změně systému sdílení z rozšířeného, a v USA v zásadě standardního, opt-out na opt-in. Souhlas může být navíc uživatelem kdykoli odvolán, a to bez nároku PSIS na náhradu vzniklé škody. Na rozdíl od USA, kde dochází k varování o narušení pouze neautorizovaných zásahů do citlivých údajů, Návrh ukládá PSISs povinnost varování u jakéhokoli narušení bezpečnosti kterýchkoli osobních údajů, které mohou sloužit k odcizení identity, nebo mohou vést k fyzické újmě, ponížení nebo zásahu do cti fyzické osoby. Předmětem diskuze je zejména požadavek, aby PSIS takto upozornili Evropské orgány ochrany dat do 24 hodin od narušení. V případech, kdy může takový zásah mít

²⁷⁰ Návrh Komise, Čl. 20.

²⁷¹ Personally Identifiable Information (PII) jsou informace, na jejichž základě lze tyto přiřadit konkrétní fyzické osobě. Jsou základním měřítkem procesů ohrožujících soukromí na internetu. Přesto však chybí v oblasti práva jejich jednotná definice. Absolutní povaze PII, tedy informace buď PII jsou nebo nejsou a k úskalím takového přístupu, který se neslučuje s praxí, se ve své práci věnují Paul Schwartz a Daniel Solove. Schwarz, P. M., Solove, D. J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information, *New York University Law Review*, Vol. 86, p. 1814, 2011

“negativní dopad” na fyzickou osobu, tedy ve většině případů, musí správce dat také upozornit předmětnou fyzickou osobu, pokud neprokáže příslušnému správci dat, že již přijal potřebná opatření. Je zřejmé, že jedním z cílů nové regulace je omezit vyvíjející funkci souhlasu uživatele se sběrem dat. Návrh přináší také mnoho konkrétních, zcela nových norem, jako je třeba založení povinnosti vytvořit a obsadit funkci správce ochrany soukromí v každé společnosti, předmětem jejíhož podnikání jsou právě data, a která má více než 250 zaměstnanců. Článek 18 zaručuje uživateli právo transferu svých dat. To je zásadní zejména pro celé odvětví sociálních sítí. Pokud by provozovatelé/majitelé byly vázány technologicky umožnit přenos celého datového balíčku, tedy kontaktů, autorskoprávně chráněného obsahu, komunikací atd., představovalo by to tolik chybějící motivaci trhem, vedoucí v ideálním případě ke zlepšení zabezpečení soukromí uživatelů těchto služeb informační společnosti. Podstatou OSN je však síť osob. Tak by buď museli všichni tito uživatelé zvolit stejnou novou OSN, nebo by musela existovat propojitelná supersíť. Lze tedy shrnout, že toto ustanovení má smysl pouze pro vnesení dat vnesených do OSN, tedy seznamu e-mailů nebo především fotografií pro jejich další užití. I to by ale v současné situaci představovalo značný přínos pro uživatele. Právo na přenosnost dat myslí na veškeré technologické aspekty tohoto práva, a tak nejenže požaduje po PSISs, aby umožnili uživateli přenést svá data ke konkurenčnímu poskytovateli služby, ale také vyžaduje, aby tato data byla poskytnuta v takovém formátu, který umožní další užití těchto údajů.²⁷² Mezi odborníky z oblasti IT nevládní jednoty co do názoru na proveditelnost tohoto právního nároku Návrhu. Převládá však názor, že pakliže budou přesně definovány požadované jednotné systémy a vývojáři budou motivováni platným právem, bude možné vytvořit data univerzálně přenositelná mezi jednotlivými službami informační společnosti. Správní pokuty jsou ukládány podle poměrně přísného režimu, a to za každé porušení jednotlivého ustanovení Návrhu. Porušitel má objektivní právní odpovědnost. Správní pokuty jsou rozděleny do třech kategorií od 0,5%, přes 1% až po 2% celosvětového ročního zisku společnosti. Toto jsou stále jednotlivé pokuty za jednotlivá porušení.²⁷³ Jedná se o skutečně vysoké částky, zejména u velkých společností jako je Google nebo Facebook, kterým také pokuty budou hrozit nejčastěji. Výše správních pokut zohledňuje také jejich preventivní povahu, spočívající v nastavení

²⁷² Návrh Komise COM(2012) 11 final Čl. 16.

²⁷³ Článek 79(4), (5), (6)

výše pokuty na takovou míru, která společnost „zraní“ a odradí ji od dalších excesů. Návrh umožňuje výjimku, a to především pokud se porušení dopustí fyzická osoba, která data nezpracovává za účelem zisku.

Jedním z problémů Návrhu je dosavadní jazyk, který je na mnoha místech vágní. Další komplikace bude pravděpodobně působit fakt, že některé státy EU, jako je např. Francie anebo Spolková republika Německo, poskytují v současné době širokou osobnostní ochranu a některé z těchto záruk by byly nařízením do budoucna již nezaručitelné.

Právní úprava ochrany soukromí nezletilých v kyberprostoru podle Návrhu

Komise

Co se poskytnutí ochrany soukromí nezletilým týče, vývoj Návrhu se nakonec přiklonil k definici dítěte jako subjektu mladšího 18ti let²⁷⁴. Této kvalifikované skupině by měly být poskytnuty podmínky, zajišťující nadstandardní ochranu jejich dat a osobních údajů v kyberprostoru. Pro tuto osobu musí být jazyk podmínek užívání jednoduchý a srozumitelný, a ke zpracování jejich osobních údajů nebo pro behaviorální advertising potřebuje PSIS výslovný souhlas rodičů nebo zákonných zástupců. Opět připomeňme, že k samotnému zpracování nemusí dojít.²⁷⁵ V souvislosti s behaviorálním marketingem a dalšími metodami komerčního sektoru představujícími potenciální ohrožení soukromí nezletilých osob, se Komise však přiklonila k mírnější regulaci podle modelu amerického práva. Podle Návrhu je v souvislosti s nabídkou služeb informační společnosti přímo dítěti pro účely tohoto nařízení zpracování osobních údajů dítěte mladšího 13 let v souladu se zněním Návrhu pouze tehdy a do té míry, pokud byl souhlas vyjádřen nebo schválen rodičem dítěte nebo jeho zákonným zástupcem. Správce vyvine přiměřené úsilí o získání ověřitelného souhlasu s ohledem na dostupné technologie.²⁷⁶ Základním ustanovením ochrany dětí je tak norma v zásadě shodná s regulací z amerického federálního zákona Children's Online Privacy Protection Act of 1998 (COPPA)²⁷⁷.

²⁷⁴ Návrh Komise COM(2012) 11 final Článek 4 (18)

²⁷⁵ Návrh Čl. 9 § 2 a 19 § 22(1)

²⁷⁶ Návrh Komise COM(2012) 11 final Čl. 8 (1)

²⁷⁷ 15 U.S.C. §§ 6501–6506 (Pub.L. 105-277, 112 Stat. 2581-728)

Z Článku 33 odst. 2 písm. d) dále vyplývá povinnost náležitě péče ve vztahu ke zpracovávání údajů o dětech. Tedy konkrétně, jestliže je zpracování údajů kvůli své povaze, rozsahu nebo účelu spojeno s pravděpodobnými specifickými riziky z hlediska práv a svobod subjektů údajů, správce nebo zpracovatel jednající jeho jménem posoudí zodpovědně dopad plánovaného zpracování na ochranu osobních údajů. Článek 52 odst. 2, který ukládá orgánu dozoru (v ČR ÚOOÚ, *pozn. autorky*) zvyšovat povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováváním osobních údajů, zdůrazňuje, že zvláštní pozornost přitom má věnovat akcím, které jsou určeny speciálně pro děti. Lze pouze doplnit, že ke komplexní ochraně by bylo vhodné začlenit do balíčku také ustanovení tlumočící zájem EU na kladení většího důrazu na ochranu, především nezletilých, před zásahy do jejich soukromí jednáním fyzických osob, které nemusí být nutně PSISs, ale individuálním uživatelem. Dalším prvkem zvláštních právních záruk poskytovaných Návrhem nezletilým je ustanovení článku 17(1), který jim, opět dosti obecně, uděluje zvláštní pozici ve vztahu k novému právu na zapomnění.

Právo na zapomnění: prostředek ochrany osobnosti se zvláštním významem pro nezletilé

Právem na zapomnění, které je jedním z nejzásadnějších nových oblastí regulace Návrhem, se v současné době zabývá také Evropský soudní dvůr z podnětu Španělska, kde jsou žaloby u národních soudů na právo na zapomnění ve své původní formě, tedy práva na výmaz, poměrně časté. Obvykle však spor není řešen občanskoprávní žalobou, ale podáním stížnosti u národního orgánu typu ÚOOÚ, který PSIS vyzve ke stažení informací. Tento úřad, tedy Audiencia Nacional, se v současné době zabývá více než 130 takovými podáními ve věcech práva na zapomnění.²⁷⁸ V uvedeném konkrétním případě se jednalo o 90 fyzických osob, které neúspěšně touto cestou žádaly původně o stažení informací z vyhledavače amerického provozovatele Google. Podobný případ dříve neuspěl, když prvoinstanční soud v Ampostě v únoru 2012 neshledal dostatečný právní základ v žalobě provozovatele kempu, o němž se ve vyhledávači na jednom z prvních míst objevovaly drastické informace o tragickém požáru, ke kterému však na

²⁷⁸ Google Spain wins lawsuit over the „right to be forgotten“ [online] *ISP Liability*. 27. únor, 2012 [cit. 2012-11-27]. Dostupný z WWW: <<http://ispliability.wordpress.com/2012/02/27/google-spain-wins-lawsuit-over-the-right-to-be-forgotten/>>

místě došlo již v 70. letech 20. století²⁷⁹. Případ je zajímavý pro tuto práci vzhledem k povaze svého předmětu, ačkoli žalobcem zde byla právnická osoba.

Jak připomíná A. Acquisti nebo R. Polčák, zapomnění je ze sociologického hlediska spojené s odpuštěním. Tato skutečnost se však promítla také do práva a to např. v podobě již zmiňovaného institutu zahlazení odsouzení. To stejně jako zapomnění má umožnit subjektu pokračovat v životu s ohledem na ontogenetický vývoj a být vnímán, vzhledem k vývoji, který učinil. V rámci běžných společenských vztahů je toto zajištěno přirozenou funkcí paměti a „fyziologie zapomnění“. Internet však nastolil režim univerzální všeobecné časově, místně dostupné okamžité paměti podložené více či méně důvěryhodnými zdroji informací. Jakýkoli čin kohokoli tak již nemůže být zapomenut a může být během několika vteřin vyvolán velmi snadno na veřejnost i po mnoha letech. Toto se týká každé fyzické osoby. Příklad zahlazení je pouze výraznějším modelem této problematiky. Případ, kdy je informace o odsouzení člověka za trestný čin permanentně uložena, zakládá stav, kdy je zahlazení prakticky nerealizovatelné, neboť jej nelze efektivně vynutit. Jako příklad uvedl pak R. Polčák na přednášce Masarykova institutu případ *Moseley*²⁸⁰. „Existuje-li v trestním právu institut zahlazení“ ptá se Polčák, „mělo by se postihovat po určité době ponechávání informací o odsouzených na internetu?“ K tomuto je ovšem nutno dodat, že v recitálu 139 k Návrhu je zdůrazněna relativita nároku na soukromí, jako nároku, který je potřeba hodnotit ve vztahu k ostatním základním právům a svobodám a k veřejným zájmům jako je národní bezpečnost a další. Vzhledem k případu *Moseley* je dále potřeba ve světle recitálu 139 připomenout spojené věci *Volker a Markus Schecke*²⁸¹. Právo na zapomnění se však týká i každodenních aktivit běžných uživatelů na internetu. Příkladem může být užívání sociálních sítí. Služba Facebook zavedla servis Timeline, novou grafickou podobu profilu uživatelů. Jedná se o interaktivní prostředí, kde se v časové přímce jednoduše zobrazují veškeré aktivity uživatele od doby jeho vstupu na Facebook. To, co by tak bylo v klasické interakci zapomenuto, je v prostředí populární

²⁷⁹ *Alfacs Vacances SL v. Google Spain SL* [2012] (Unreported, Court of First Instance of Amposta, 23 February 2012)

²⁸⁰ *Moseley v. News Group Newspapers* [2008] EWHC 1777 (QB), (2008) *The Times*, 30. červen: britský soud rozhodl, že nelze uložit dehonestující video stáhnout z internetu, protože už mezitím existuje ve stovkách kopií a proto by toto rozhodnutí již neposkytovalo požadovanou nápravu. Toto rozhodnutí hodnotí Polčák, jako správné, vzhledem ke stávající právní úpravě.

²⁸¹ *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*. Evropský soudní dvůr, spojené věci C-92/09 a C-93/09 (2010)

sociální sítě vyvolatelné kdykoli a ihned a navíc na jednom místě a velmi přehledně. Lze tak například zjistit, jestli byl uchazeč o brigádu ve 14ti letech anarchistou, jak nová podřízená komentovala v červnu před čtyřmi lety politický vývoj v zemi, či jak často střídala v době puberty partnery.

Právě z tohoto důvodu se Komise rozhodla klást důraz na záruku práva na zapomnění týkající se informací, které byly zpřístupněny, nebo které osoba na internet vložila v době, kdy byla dítětem²⁸². To má zaručit, že např. chyby z dětské nerozvážnosti nebudou formovat životní cestu osoby v dospělosti. Z pohledu českého práva by tato regulace představovala dobrou cestu pro řešení případů porušení práva na ochranu osobnosti, o kterém se postižený dozvěděl pouze s časovým odstupem, což je zejména na internetu, ne zcela nepravděpodobné a dále by řešila otázku změny poměrů. Mimořádné nároky na výmaz pak klade navrhovaná úprava na PSISs v tom smyslu, že jim ukládá iniciativu ke stažení těchto dat z jakýchkoli dalších uložišť resp. prostoru PSISs, kteří tato data převzali. V aktuální verzi Návrhu tato povinnost vyplývá z Článku 17 (2), konkrétně v tom smyslu, že je „originální“ PSIS povinen spojit se se všemi dalšími, kteří informaci převzali, a informovat je, že subjekt požaduje odstranění těchto informací. Problematické je toto ustanovení ovšem ve spojení se Článkem 13, protože tyto snahy PSISs omezuje tento na takovou míru, která „je možná, a nevyžaduje nepřiměřené úsilí“. Článek 17, zakotvující již uvedený právní koncept práva na zapomnění, tedy, podle Návrhu „*Právo být zapomenut a právo na výmaz*“, sice představuje v zásadě rozšíření již existujícího práva subjektu na výmaz, přesto však může vyvolávat protesty PSISs a také později jisté nejasnosti v aplikaci v rámci národního práva. Již nyní se jedná o zřejmě nejkontroverznější inovaci právní úpravy ochrany soukromí na internetu. Ač by tato zřejmě představovala řešení mnoha zásahů do osobnostních práv, nese s sebou jak právní tak filozofickou otázku legitimacy. Ačkoli např. Daniel Solove je zastáncem co nejširší právní záruky reputace občana a Viktor Mayer-Schönberger ve své knize „Delete“ dokonce navrhuje automatizovaný mechanický právně regulovaný a uživatelem nastavitelný systém zapomnění našich dat technologiemi, pro odborníky zastávající konzervativní postoj je takovýto nárok zcela

²⁸² EU. Proposal for a Regulation of the European Parliament and of the Council COM(2012) 11 final, of 25.1 2012, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Článek 17(1). Dostupný také z WWW: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

nepřístupný. V praxi se jistě bude také možné setkat se složitým zvažováním proporcionality práva vůči právu na svobodný přístup k informacím a dalším ústavním právům.

4.3.3. Závěr

Otázkou je, nakolik tento nový právní základ skutečně ovlivní vymahatelnost právních nároků nezletilých v kyberprostoru. Existují názory, že jedním z důvodů, proč se Spojené státy zdráhají přijmout federální zákony upravující ochranu soukromí na internetu v širší míře je také právě evropská zkušenost. Ještě v polovině 90. let, ačkoli Evropa znala tato práva již od let 70. a jejich rozkvět vedený Německem začal na samém počátku let 80., byla totiž nápadnost v těchto věcech, a zde nejen co se nezletilých uživatelů týče, v evropských zemích takřka či zcela nulová.²⁸³

4.4. Právní úprava ochrany osobnosti nezletilých v USA

4.4.1. Vývoj a povaha amerického práva na ochranu osobnosti s důrazem na ochranu soukromí nezletilých v kyberprostoru

Vynález přenosného ručního fotoaparátu se stal symbolem neustálého závodu technologií a práva v USA. Zatímco někteří ze současných právních teoretiků se přiklání k názoru, že soukromí chránit právem již nelze, neboť se toto právo stalo kvůli stupni vývoje technologií nevymahatelným, Warren a Brandeis, postavení ve své době před velmi podobnou situací, ve své práci tvrdí, že o to více je důležité, aby občané měli kontrolu nad informacemi o své osobě. Ve své práci Warren a Brandeis dále především vytvořili základ pro pozdější moderní zformování čtyři žalobních petitů v občanskoprávní žalobě na vpád do soukromí, které později rozpracoval William Prosser, nejprve ve svém odborném článku „Privacy“²⁸⁴, a které jsou od roku 1977 součástí amerického právního řádu²⁸⁵. Jedná se o zásah do soukromí, veřejné odhalení, uvedení osoby ve špatné světlo a užití jména nebo podoby osoby. Z toho vyplývá, že informace osobní povahy, jak písemné, tak obrazové formy lze rozšiřovat výhradně se souhlasem

²⁸³ SCHÖNBERGER, V.-M.; *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, s. 139. ISBN 978-0-691-13861-9

²⁸⁴ PROSSER, W. L.; *Privacy*, *California Law Review*, č. 48 (1960) s. 383

²⁸⁵ USA. The Second Restatement of Torts at §§ 652A-652I (1977)

osoby, které se tyto týkají, pokud ovšem sdílení těchto informací není ve veřejném zájmu.

Mimo nedostačující provázanosti systematiky jednotlivých souvisejících normativních právních aktů, lze příčinu odlišnosti faktického stavu od zamýšleného ohraničení hledat také v příliš široké interpretaci informací, jejichž šíření je ve veřejném zájmu a dále ve složitosti dokazování v těchto případech. Dalším problémem je sektorální povaha amerického psaného práva a širší úprava relevantní právní regulací prostřednictvím práva státního. Pozitivní vývoj by mohla představovat judikatura, které jsme se v této práci již rozsáhle věnovali, problém však představuje její nejednotnost a limitovanost tradičním americkým přístupem k soukromí a důstojnosti fyzické osoby, které byli již také osvětleny. Připomenout lze opět také tradiční silnou nedůvěru k vládní kontrole, příliš širokým pravomocem výkonných orgánů a významnou pozici Prvního a Čtvrtého dodatku americké Ústavy.

4.4.2. Právní rámec ochrany osobnosti nezletilých v kyberprostoru v USA

S ustanoveními, která souvisí s právem na soukromí, se setkáváme v Prvním, Třetím, Čtvrtém, Pátém, Čtrnáctém, a v širším pojetí také v Devátém dodatku americké Ústavy. Právo na soukromí je na státní úrovni zachyceno pouze v ústavách deseti států USA. Největší význam má v této situaci nedostatku psaného práva, mimo zvláštních zákonů a judikatury, Federální obchodní komora - **Federal Trade Commission (FTC)**. Ta byla založena v roce 1914 a jejím hlavním úkolem je především prevence a postih nekalosoutěžního jednání a klamavých obchodních praktik. Později byly pravomoci FTC rozšířeny na ochranu spotřebitele. Ta je zásadní pro ochranu osobnostních práv uživatele internetu. Ochranou spotřebitelů se zabývá Úřad pro ochranu spotřebitelů, který je součástí FTC. FTC má pravomoc kontrolní a vyšetřovací. FTC má dále žalobní pravomoc a pravomoc přijímat regulační opatření pro jednotlivá průmyslová odvětví.²⁸⁶ FTC hrála zásadní roli v prosazování regulace internetu v USA. Jediným významným federálním zákonem věnujícím se ochraně osobnosti nezletilých v kyberprostoru je Zákon na ochranu soukromí dětí z roku 1998 – **Children's Online Privacy Protection Act (COPPA)**. COPPA může však poskytnout pouze omezenou ochranu nezletilému.

²⁸⁶ 15 U.S.C §45(b); 16 C.F.R. § 3.1; 16 C.F.R. § 3.41

Tento zákon poskytuje ochranu před sledováním uživatelských aktivit a pohybu v kyberprostoru a webliningem²⁸⁷, to vše však pouze na komerčních stránkách, které jsou zcela nebo částečně cíleny na děti. Tento zákon definuje dítě, jako fyzickou osobu mladší 13ti let.²⁸⁸ Na těch, jak již víme, nesmí být prováděn výše uvedené aktivity, ani jiný podobný sběr dat bez rodičovského souhlasu nebo souhlasu zákonného zástupce. To znamená, že COPPA neposkytuje tuto ochranu nezletilým dětem starším 13ti let. Lze říci, že zákon má dva důležité cíle. Jedním z nich, tím, který je obecně přijat, jako hlavní, je zajistit ochranu dětí před, v USA ne zcela přiměřeně regulovanou, reklamou. Ta může být, a velmi často je, připravována právě na základě poznatků získaných analýzou osobních údajů, které byly od nezletilých uživatelů, téměř výhradně bez jejich vědomí, získány. Dalším cílem zákona je ale ochránit rodiče, rodiny a domácnosti před neuváženým sdílením osobních údajů nezletilými. Jedná se o zmiňované případy sdílení informací o pobytu rodiny mimo bydliště, sdílení informací o finanční situaci rodiny, uvádění adres atd. Pravdou však je, že to jsou starší, než 13ti-letí nezletilí, kteří tato data také sdílí, a jsou to právě tito, kteří tak činí v nejhojnější míře. „Studie dochází k závěrům, že teenageři²⁸⁹ mohou dokonce představovat, co se týče odhalování osobních informací o záležitostech týkajících se jejich domácnosti, větší bezpečnostní problém než děti mladší 13ti let.“²⁹⁰

COPPA může sloužit jako příklad tvrdé regulace, která má jasný cíl, pochybný přínos a kontroverzní důsledky. Během zasedání Komise pro ochranu dětí na internetu, ustavené na základě COPPA, byl zákon kritizován pro svůj paternalistický předpoklad autoritativního rozhodování vlády o přístupu dětí k informacím. Někteří právní znalci z oblasti ochrany soukromí vidí takový systém jako omezující práva nezletilých uživatelů a potlačující svobodu projevu.²⁹¹ Rozsáhlá studie Jasona Schulze a dalších

²⁸⁷ Weblining je funkce vyhodnocování a třídění informací, které jsou uživateli poskytovány, především vyhledávači, v závislosti na jeho konkrétní virtuální osobnosti, resp. soustavě doposud získaných informací o jeho odhadovaných preferencích.

²⁸⁸ Children's Online Privacy Protection Act of 1998". SEC. 1302. DEFINITIONS (1)

²⁸⁹ Teenagers převzato z ang. textu, kde lze předpokládat, že autor v rozdělení na teenagery, tedy starší 13ti let, vychází z užívání pojmu „tween“, který je novotvarem označujícím pohyblivou hranici věku, původně okolo 12ti let, na pomezí dětství a puberty; Více: Tarrow, Joseph, *The Internet and the family*, 2000

²⁹⁰ ALLEN, A.; *Unpopular Privacy: What Must We Hide?*, Oxford University Press, 2011. s. 179. ISBN 0195141377

²⁹¹ ALLEN, A.; *Unpopular Privacy: What Must We Hide?*, Oxford University Press, 2011. s. 184. ISBN 0195141377

z Kalifornské univerzity Berkeley²⁹² prokázala neefektivnost tohoto zákona, spočívající v tom, že rodiče svolují či dokonce pomáhají svým dětem pod hranicí věku 13ti let užívat internet a registrovat se na nejrůznějších sociálních sítích z důvodu neznalosti podstaty služby a pod tlakem okolí. Marc Rotenberg, výkonný ředitel Electronic Privacy Information Center při zasedání Kongresu, týkajícím se problematiky nezletilých v kyberprostoru požadoval, aby byla věková hranice v zákoně COPPA zvýšena ze 13 na 18 let, protože ani pro tyto teenagery není snadné pochopit často se měnící pravidla podmínek užívání týkající se nastavení soukromí.²⁹³ Alternativou, která byla nabízena např. bývalým zástupcem Informačního Centra pro elektronické soukromí, byl přesun důrazu na vzdělávání nezletilých uživatelů v bezpečném a zodpovědném užívání internetu. S tímto přístupem se lze ztotožnit, ovšem nelze zapomínat na kontrolu internetu a vymahatelnost uživatelských práv. Pouze na bázi prevence a samoregulace bezpečný internet pro nezletilé založit nelze.

Jedním z dalších federálních zákonů, který měl za cíl ochranu soukromí nezletilých na internetu, byl **Children's Internet Protection Act (CIPA)**. Jedná se o zákon, podle kterého musely školy a knihovny, žádající o vládní granty zavést do svých internetových systémů ochranné filtry obsahu, ale i další opatření, jejichž cílem je zajistit ochranu dětí v kyberprostoru, tzv. Opatření pro bezpečný internet, sestávala také z využití kybernetických chův. Byl to způsob, jakým se Kongres pokusil obejít situaci, kdy podle amerického federálního ústavního práva nemůže aktivity na internetu a jeho využití regulovat přímo.

Za jistých okolností by proti zásahu do soukromí nezletilého např. při užívání některých druhů invazivního sledovacího softwaru pro monitorování kybernetických aktivit nezletilého mohl být využit **Zákon o počítačových podvodech a zneužívání počítačů z roku 1986 (Computer Fraud and Abuse Act CFAA)**. Tímto zákonem se mohou řídit případy phishingu a podvodů na internetu. Tento zákon byl původně tvořen se záměrem boje s hackerstvím. V případě *United States v. Drew* soud rozhodl, že CFAA nelze uplatnit v případech kyberšikany, ačkoli se také jedná o zneužití informací,

²⁹² SCHULZ, J. et al., Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act. *First Monday*, Volume 16, Number 11 – 7. listopad, 2011. Dostupný z WWW:

<<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075>>

²⁹³ *Consumer Reports Magazine*, That Facebook Friend might be 10 Years Old, červen 2011, Dostupný z WWW: <<http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm>>

často spojené s podvodem. V některých případech zneužití počítačových kamer, jako např. v případech, kdy školská zařízení sledují své žáky mimo prostory školy nebo kdy je subjekt sledován a zaznamenáván kamerou bez svého vědomí by mohl být užít **Zákon na prevenci video voyeurismu z roku 2004 (Video Voyeurism Prevention Act VVPA)**, který má také své ekvivalenty ve státním právu. Může být užít také na některé případy užívání kamer ve smartphonech.

Zákon o odcizování identity z roku 1998 (Identity Theft and Assumption Deterrence Act ITADA) zase postavil poprvé v historii amerického práva „odcizení identity“ mimo zákon. Tento zákon poskytuje velice širokou definici zneužití identity. Může k němu dojít nejen zneužitím a manipulací s osobními údaji, od jmen až po fotografie, ale také zneužitím přístupového hesla či čísla sociálního zabezpečení. Ze znění zákona lze dokonce dovodit jistý prostor pro právní odpovědnost PSISs. Z Manuálu pro užití informačních zdrojů pro vyšetřování ²⁹⁴ totiž vyplývá, že je v rozporu se zákonem také přenos identifikace (id. údaje), která byla odcizena nebo vyrobena v rozporu se zákonem. Takovým přenosem by mohl být také přenos elektronický.

Jak již bylo vyloženo v souvislosti s konkrétní problematikou, právní regulaci práva na ochranu osobnosti a soukromí nezletilých a jejich ochranu před kyberzločinem poskytuje prostřednictvím zvláštních zákonů především státní právo. Jedná se o zákony regulující jednotlivé oblasti jednání, nově nastalé negativní trendy představující bezpečnostní rizika. Vznikají však často na základě realizovaného tragického zásahu a mimoto neposkytují vzhledem ke struktuře amerického práva efektivní ochranu na federální úrovni. Nejdůležitějším z těchto zákonů se práce již věnovala.

Občanskoprávní žaloba se v americkém právu zdá být vhodnou cestou, jak se dotčený může domoci svých práv nejen na osobě, která se dopustila zásahu do jejich osobnostních práv, ale jak se také domoci svých práv případně na PSIS, který se teoreticky na zásahu podílel nebo se jej sám dopustil. V praxi však podobné Žaloby, zejména proti PSISs, nebývají příliš časté a úspěšné. Mimo známých čtyř žalobních petitů lze ještě využít petitu způsobení psychické újmy a porušení důvěrnosti sdělených informací. Zejména poslední ze jmenovaných by mohly představovat lepší cestu k vymahatelnosti práv, než doposud velmi málo úspěšné žalobní petitů na ochranu

²⁹⁴ 1512 Prohibited Acts – 18 U.S.C. § 1028(a)(2)

soukromí. **Žalobu na ochranu cti a vážnosti tzv. defamation law**²⁹⁵ upravuje americké právo odlišným způsobem od práva kontinentálního. Ačkoli americké federální trestní právo nerozeznává pojem pomluvy, mnoho států pomluvu trestním právem upravuje. Případů v této sféře však bylo v moderní historii Spojených států velice málo. Valná většina států USA uznává tzv. difamacii *per se*, kde se jedná o sdělení takového charakteru, že žalobce nemusí prokazovat jejich difamační charakter. Bez dalšího jsou takto za způsobující újmu subjektu považována především sdělení o tvrzenou chorobu určené povahy, tvrzenou nevěru, trestnou činnost nebo nekalosoutěžní jednání.

V souvislosti s ustanovením § 230 CDA je potřeba ještě zmínit např. rozhodnutí *Zeran v. America Online*²⁹⁶ nebo *Blumenthal v. Drudge*²⁹⁷, kde byla bezvýhradní imunita providerů aplikována, a to i přes všeobecně známou nevoli mnoha soudců k této nutné praxi. Zásadní je potom skutečnost, že imunita se na providery vztahuje i v situacích, kdy jsou na difamační obsah upozorněni a neodstraní jej. Dalším podstatným rozhodnutím je rozsudek kalifornského Nejvyššího soudu ve věci *Barrett v. Rosenthal*²⁹⁸, který judikoval, že uvedená výjimka činí nepřijatelnými žaloby na providery za obsah vyskytující se na jejich platformách, který byl vyložen a náleží třetí straně.

Aspekt mezinárodního prvku právních vztahů v kyberprostoru v souvislosti s osobnostními právy uživatelů dále naráží na zákon z nedávné doby, tzv. **SPEECH Act**²⁹⁹ z roku 2010, který, zjednodušeně řečeno, brání vymahatelnosti zahraničních rozhodnutí ve věcech difamačního obsahu na území USA. Takovým rozhodnutím by se mohl žalobce domáhat svých osobnostních práv pouze v případě, že by bylo v souladu s Prvním dodatkem, což je v praxi velmi těžko představitelné.

Ve chvíli, kdy jsme tak již obeznámeni s evropským právem a judikaturou, s plánovanými legislativními změnami a zároveň s platným právem USA a postojem obou právních oblastí, jeví se komplexnost problematiky osobnostních práv v kyberprostoru zcela zřejmou.

²⁹⁵ Restatement (Second) of Torts, Section 558 and 559, 578, 581 (republishing) proti CDA paragraf 230(c)(1)

²⁹⁶ *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997)

²⁹⁷ *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998)

²⁹⁸ *Barrett v. Rosenthal*, 146 P.3d 510 (Cal. 2006)

²⁹⁹ The Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act

Mezi právní regulací ochrany osobnosti, zejména ochrany soukromí a dobré pověsti, v zemích EU a ve Spojených státech amerických existují zásadní rozdíly. Ty nakonec způsobily obtíže pro obě strany na počátku 90. let 20. století, kdy poprvé americké společnosti začaly využívat dat uživatelů internetu z Evropy. Teprve v roce 2000 se podařilo nalézt únosný kompromis v podobě dohody, na jejímž konci stál soubor pravidel pro technologické společnosti v USA, jak pomocí samoregulačních opatření zabránit konfliktu s právem EU, který jim poskytne jisté kvalifikované postavení, co se nakládání s uživatelskými daty týče. Tato pravidla se nazývají **Safe Harbor Principles**³⁰⁰. Safe Harbor Principles nezajišťují adekvátní vymahatelnost subjektivního práva občana EU, jehož právo na ochranu soukromí nebo dobré pověsti nebo právo na ochranu osobních údajů bylo porušeno americkou společností. Jedním ze základních požadavků při podpisu dohody o Safe Harbor, obsahující podmínky, pod kterými je možné data z EU přenášet do USA, bylo právě zajištění vymahatelnosti práva. Porušení pravidel zpracovávání informací o uživateli ze zemí EU mělo být právně napadnutelné v souladu s § 5 zákona o FTC (FTCA)³⁰¹, jako nekalosoutěžní a klamavé praktiky. Dostí vágně, ale v souladu s běžnou praxí, zní požadavek zajištění bezpečnosti dat. Společnost musí vynaložit péči v rozumné míře k tomu, aby zabránila neautorizovanému přístupu, manipulaci, zveřejnění, zneužití, ztrátě nebo zničení dat. Zásadním a často porušovaným závazkem je, že společnost nesmí užívat získané informace způsobem neslučujícím se s původním účelem, pro který byly získány, pokud nezískají následný souhlas uživatele.

4.4.3. Závěr

Je potřeba připomenout, že stejně jako evropské právo má také americké právo za sebou historický vývoj několika století, a ačkoli je pro něj typická schopnost oproti kontinentálnímu právu relativně snadné adaptace na aktuální problematiku. V pohledu práva na ochranu osobnosti, především soukromí, se od kontinentálního práva liší ve zcela základních koncepcích, které jsou těžko měnné, neboť byly jedněmi ze základních původních hodnot, které stály u zrodu Spojených států amerických. Slovy

³⁰⁰ Srov. Datová směrnice

³⁰¹ Section 5 of the Federal Trade Commission Act (FTC Act), Ch. 311, §5, 38 Stat. 719, *codified at* 15U.S.C. §45(a), která upravuje nekalosoutěžní jednání nebo klamavé obchodní praktiky v mezistátních obchodních stycích.

Jamese Q. Whitmana: „Je pravdou, že máme jen málo důvodů se domnívat, že Američané budou v blízké budoucnosti přesvědčeni k tomu, aby o svých hodnotách uvažovali evropským způsobem. Americké právo nepodporuje obecnou normu společenské důstojnosti, kterou nalézáme v Evropě.“³⁰²

5. Úvahy *de lege ferenda*: Výběr některých návrhů regulace ochrany osobnosti v kyberprostoru

5.1. Technické zneschopnění počítače

Jedním ze, z právního pohledu zajímavých, návrhů je využití regulace soukromí s pomocí technologií, tedy správy digitálních práv (Digital Rights Management – DRM). Tento systém by počítal s tím, že při vložení každé soukromé informace na internet by uživatel zadal kdo, za jakým účelem, za jakých podmínek a na jak dlouho může tato data užívat. Počítač pak rozezná, zda osoba, která chce soubor užít, nejedná v rozporu s metadaty, která pokyny pro užití obsahují.³⁰³ Tato metoda se v zahraničí již poměrně úspěšně aplikuje na ochranu audio a audiovizuálních děl před nelegálním užíváním. Problematickou však zůstává zdlouhavost vyplňování povahy sdílení a možnost kontroly aktivní legitimace uživatele.

S dalším progresivním návrhem přichází Viktor-Mayer Schönberger, který navrhuje technologické zneschopnění počítače k trvalé paměti. To by spočívalo v tom, že při ukládání souboru by jeho tvůrce také zadal jeho „expiraci“, po jejímž vypršení by se soubor automaticky smazal.³⁰⁴ Autor tvrdí, že toto je jediná možnost, jak uměle simulovat přirozený proces zapomnění a připomíná, že některé státní orgány jsou již v současné době povinny po uplynutí určené doby znepřístupňovat nebo skartovat svou dokumentaci. Praktická stránka tohoto návrhu je sporná hned ze dvou úhlů: Většina administrativních činností a záznamů, včetně např. lékařských zpráv, je celosvětově uložena v kyberprostoru. Tištěná kopie není archivována zdaleka vždy. Pokud by tak takový záznam expiroval a ukázal se později potřebným, nebude již dosažitelný. Dalším problémem tohoto návrhu je jeho binární povaha. Je otázkou, zda lze požadovat

³⁰² WHITMAN, J. Q., The Two Western Cultures of Privacy: Dignity versus Liberty, Vol. 113, No. 6. (2004). *The Yale Law Journal*. s.1221.

³⁰³ SCHÖNBERGER, V.-M.; *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, s. 144. ISBN 978-0-691-13861-9

³⁰⁴ SCHÖNBERGER, V.-M.; *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, s. 171-196. ISBN 978-0-691-13861-9

absolutní nenávratné zapomnění ve společnosti. O tuto argumentaci se opírají také odpůrci práva na zapomnění a připomínají, že existuje veřejný zájem na uchování paměti společnosti např. o mnoha historických událostech a souvislostech. Implementace tohoto systému by byla navíc poměrně složitá, protože by se týkala také veškerých dat generovaných nebo již shromážděných PSISs. Mimoto by se musela vypořádat se situací, kdy se jeden osobní údaj týká několika osob. Schönberger však připomíná, že cílem tohoto návrhu je zejména obnovení společenského zapomnění a aplikovat jej nelze bez efektivních právních prostředků klasické ochrany osobnosti a především bez ohledu na právo na soukromí.

5.2. Model zeleného a červeného Internetu

Jonathan Zittrain ve své knize „The Future of the Internet – And How to Stop it“³⁰⁵ představil teorii pro řešení boje s technologickým nebezpečím pro jednotlivce, jako je virová problematika a podobně. Jeho idea dvou typů počítačů – *zeleného*, který obsahuje jen prověřený obsah a jiné uživatelé nedovolí nainstalovat, a *červeného*, tedy volného bez omezení, povolujícího veškeré, třeba i pirátské aktivity, kde ale majitel přistupuje na riziko plné odpovědnosti za následky, nejen na svém počítači. Tuto ideu rozšířil britský technologický kritik a spisovatel Bill Thompson, který ve svém článku „Staying Safe and Taking Risks“³⁰⁶ přijal ideu stejného uspořádání internetu. Tato teorie představuje možnou alternativu vypořádání se s ohrožením nezletilých uživatelů internetu, jejíž regulace právem v demokratickém státě je ale v praxi obtížně představitelná. Nezletilí by měli možnost užívat po určitou dobu pouze zelený, tedy v zásadě cenzurovaný internet. Na červeném internetu by byl neprověřený obsah, a jistě závadný, snadněji dohledatelný, a takový by přirozeně nezletilé lákal k obcházení systému. Je skutečně možné přiklánět se k závěru, že pokud nelze regulovat internet, je nutné regulovat chování jeho uživatelů?

³⁰⁵ ZITTRAIN, J.; *The Future of Internet and How to Stop It*, Yale University Press, 2008. ISBN 9780300124873

³⁰⁶ THOMSON, B., Staying safe and taking risks [online]. *BBC*, 14. květen 2007 [cit. 2012-12-02]. Dostupný z WWW: <<http://news.bbc.co.uk/2/hi/technology/7400158.stm>>

5.3. Ověřování věku uživatele

Omezení uživatele s využitím jeho osobních údajů je volně aplikováno na některých stránkách, jak v USA, tak v evropských zemích. V ČR se s ním lze setkat především na stránkách regulovaných podle zvláštních zákonů. Vždy to jsou stránky propagující alkoholické nápoje, tabákové výrobky nebo obsahující určený mládeži nevhodný obsah. Ověření věku probíhá různými způsoby. Na většině výše uvedených stránek se jedná o prosté zadání data narození. Systém však často umožňuje toto datum po neúspěšném přihlášení měnit. Tak není pro nezletilé dítě problém přístup získat. Další možností je udávání údajů z bankovního účtu, které jsou následně ověřeny. Tento způsob, ač o poznání spolehlivější, může být z právního hlediska problematický, ať již se týká pouhého sdílení takto soukromých informací s neznámým serverem, možnosti jejich dalšího zneužití, ale i možnost překonání této bariéry. Další možnost ověření věku, aplikuje např. virtuální sociální síť Second Life, která požaduje uvedení věku uživatele, resp. jeho data narození spolu se závazkem, že tyto údaje uvedl pravdivě. Jak již bylo řečeno, vzhledem ke snadnosti překonání také takovéto bariéry nelze za podobnými úpravami vidět o mnoho víc než snahu předejít právní odpovědnosti. Další možnost ověření věku představuje, z pohledu ochrany osobnosti v kyberprostoru, problematické užití biometrických údajů, podobným způsobem, jako jich již využívají rodičovské zámky na některých mobilních telefonech a interaktivních televizorech. Co se ověření věku nezletilých dětí týče, je ale nutné připustit, že nelze učinit o mnoho více. V roce 1998 byl s tímto cílem představen neúspěšný návrh zákona Child Online Protection Act (COPA, nikoli COPPA, *pozn. autorky*), který si kladl za cíl kontrolovat přístup nezletilých na internetu k sexuálně explicitnímu obsahu.³⁰⁷

5.4. Vzdělávání

V současné době jak v České republice, tak v dalších evropských zemích, stejně jako v USA probíhá mnoho osvětových kampaní, jejichž cílem je jednak vyškolit uživatele internetu, jak zajistit svou bezpečnost a bezpečnost svých dětí či žáků, a také

³⁰⁷ The Child Online Protection Act (COPA), zákon, který byl jedním ze série zákonů, které měly chránit nezletilé uživatele především před pornografií. Zákon ukládal provozovatelům stránek se závadným obsahem znemožnit nezletilým přístup na tyto na základě ověření věku s využitím bankovních údajů. Kritizovaný zákon byl konečně v roce 2007 po deseti letech soudního přezkumu shledán Nejvyšším soudem protiústavním vzhledem k rozporu s Prvním dodatkem. Není bez zajímavosti, že tento návrh uváděl jako věkovou hranici věk 17 let. Zároveň škodlivý obsah definoval, jako škodlivý nezletilým. Z toho vyplývá definiční nejistota amerického práva v souvislosti s ochranou osobnostních práv v kyberprostoru.

jak se vyhnout, bránit a vyrovnat s následky zásahu do osobnostních práv v kyberprostoru.

Dobrym příkladem snahy o efektivní vzdělávání nezletilých je model fungující v Korejské republice. Korejská vláda přistoupila k alternativnímu způsobu rozvoje informační gramotnosti. Na základních školách jsou děti vyučovány práci s internetem v nejtělejší věku, jako se učí číst. Zároveň jsou však vyučovány, jak používat počítač zodpovědně. Další významnou složkou výuky je internetová etiketa (netiketa) a slušné chování ve veškerých komunikacích v kyberprostoru.³⁰⁸ Důsledkem nadměrného užívání internetu může být zásah do práva nezletilého na rodinný život. Autorka práce se domnívá, že legislativa by měla připravit právní regulaci umožňující vyrovnat se s informačním a konzumním přetlakem na internetu a zároveň uzpůsobit výuku společenské změně spočívající v dominanci technologií v životě nezletilých a v nových požadavcích, se kterými se v pracovním procesu budou díky celkové technologizaci společnosti v budoucnu setkávat.

V České republice se v současné době skupina neziskových organizací a zástupců PSISs zasazuje o zavedení netikety do povinných školních osnov. Důraz na výuku netikety má i mezi právníky své odpůrce, kteří v této metodě vidí umělé zachovávání hodnot, které již nejsou platné.

5.5.Regulace sociálními normami

Julian Togelius naopak prosazuje teorii kognitivního přizpůsobení. Podle něj je efektivním prostředkem ochrany společenský vývoj. Např. v souvislosti s právem na zapomenění upozorňuje, že společnost bude muset více než dřív brát ve svých úsudcích v úvahu, že lidé se mění, a vnitřně udržet odstup od zpráv, které jsou s fyzickou osobou spojeny, ale jedná se o události, které třeba proběhly v době jejího mládí³⁰⁹. Také danah boyd zastává názor, že mladí uživatelé internetu přijdou v budoucnu sami se systémy, které jim umožní vyrovnat se s touto právní nejistotou. Boyd je zastánkyní změny, která

³⁰⁸ Digital Nation [dokumentární film] PBS, 25:00, Dostupný z WWW: <<http://www.pbs.org/wgbh/pages/frontline/digitalnation/view/>>

³⁰⁹ TOGERIUS, J.; Harvard Prof Says Computers Need to Forget [online] *Sloshdot*, 10. květen 2007 [cit. 2012-11-08] Dostupný z WWW: <<http://yro.slashdot.org/comments.pl?sid=234167&cid=19065957>>

vzejde od mladých uživatelů a je přesvědčena, že každá jiná regulace se mine účinkem³¹⁰.

Názoru, že k vyřešení např. problému trvalé paměti internetu postačí nezasahovat do společenského vývoje právní regulací lze odporovat jak argumenty psaného práva, tak výsledky experimentů právních teoretiků specializujících se na ochranu osobnosti na internetu. Např. Alessandro Acquisti z univerzity Carnegie Mellon se dlouhodobě zabývá aplikací behaviorální ekonomiky a experimentální ekonomiky na analýzu procesu rozhodování uživatelů o ochraně svého soukromí, tedy, zjednodušeně řečeno, přístupem uživatelů k hodnotě svého vlastního soukromí, respektive definování ceny, na základě které jsou ochotni riskovat věčnou existencí dat a případné zveřejnění svých soukromých informací. V rámci studie „Příběh peněženky („The Wallet Story“³¹¹) došel např. k závěru, že kyberprostor a jeho trvalá vyvolatelná paměť může zpochybnit představu o přirozeném vývoji společnosti směrem k „odpuštění“ dávných chyb, které by přirozenou pamětí byly již zapomenuty. Jednou ze zajímavých otázek, zejména ve vztahu k tématu nezletilého uživatele, kterou se Acquisti dále zabývá, je, zda jsou lidé skutečně důslední v ochraně svého soukromí, a pokud nejsou, a činí riskantní rozhodnutí v této oblasti, zda je legitimní a možné, aby tato jejich rozhodnutí byla napravována právem³¹².

5.6. Ústava pro sociální síť

Lori Andrews z právnické fakulty Chicago-Kent College vypracovala se svým týmem návrh desetibodové Ústavy pro sociální síť (ÚSS)³¹³, upravující kyberprostor jako samostatnou jurisdikci, kde jeho uživatelé, především uživatelé sociálních sítí jsou vnímáni, jako jeden národ. Práva, která ÚSS zakládá, jsou právo na připojení, právo na svobodu slova a svobodu projevu, právo na soukromí místa a informací, právo na soukromí myšlenek, citů a nálad, právo na kontrolu nad vlastním obrazem, resp. podobou, právo na spravedlivý proces, právo na nezaujatou porotu, právo na správný

³¹⁰ WINTER, J.; The advantages of amnesia: From the Internet to the iPod, technology is bringing rapid advances in memory. What society needs now are new ways to forget. *Boston Globe*, 23. září 2007 [cit. 2012-12-20]. Dostupný také z WWW: <<http://www.highbeam.com/doc/1P2-8717181.html>>

³¹¹ Výsledkem experimentu bylo, že to pozitivní, co člověk učinil je zapomenuto, třebaže se tak stalo nedávno, resp. tomu není přikládána pozornost, zatímco jednání vnímané negativně v paměti druhých přetrvává a hraje roli v úsudku o druhém významnější než to dobré, a to třebaže převažovalo v jeho životě posléze to pozitivní a k negativní události došlo již dávno.

³¹² ACQUISTI, A.; *Privacy & Behavioral Economics: The Paradox of Control & Other Studies*, 15. říjen, 2010 *Carnegie Mellon University*

³¹³ Dostupný z WWW: <<http://www.socialnetworkconstitution.com/the-social-network-constitution.htm>>

postup a na upozornění, svoboda před diskriminací a svoboda sdružování. Také Viktor-Mayer Schönberger ve své publikaci „Delete“ připomíná snahy již Warrena a Brandeise včlenit do amerického práva konkrétní individuální osobnostní práva na soukromí fyzických osob. Připomíná však také, že zůstává otázkou, jak přesně by taková práva byla strukturována. Také by bylo potřeba zajistit nanejvýš spolehlivé právní mechanismy napomáhající vymahatelnosti práv, protože za současné situace je již jen pouhé určení osoby, která se zásahu dopustila velice nesnadné. Srovnává také s touto ideou situaci v Evropě, zmiňuje právo na informační sebeurčení a zdůrazňuje, že „právo na soukromí informací nelze již chápat jako binární právo na souhlas, jako absolutní „ano“ či „ne“, ale (...) jako právo určující spíše „jak“ nežli „zda“ se osoba bude podílet na sdílení informací.“³¹⁴ Aplikace Ústavy pro sociální sítě je v praxi těžko představitelná, nicméně poskytuje přehledný základní právní rámec pro regulaci soukromí a dalších osobnostních práv v kyberprostoru.

5.7. Úvaha autorky

Řešením není, podle autorky práce, sektorální právní úprava práva na ochranu jednotlivých osobnostních hodnot pro dané situace, jakou známe z USA, ale obecnější právní úprava, která zaručí schopnost obsáhnout, alespoň do jisté míry, také očekávaný technologický vývoj, která však musí být také schopna regulovat přeshraniční tok dat a komunikací, a jejíž znění musí být zároveň natolik pečlivě formulováno, aby nedávalo prostor pro obcházení práva či pochybnosti ve výkladu.

V USA by bylo problematické obecnou úpravu prosadit. Toto řešení by tak prozatím bylo vhodnější pro evropské teritorium, ačkoli by se zásadním způsobem dotýkalo amerických společností. Spolupráce s PSISs je nutná především při samotné tvorbě práva, za účelem nalezení ideálního kompromisu, který právo bude činit flexibilním s ohledem na očekávaný rozvoj technologií, efektivním, ale zároveň proveditelným z technického hlediska. Součástí ideální legislativy pro ochranu osobnosti nezletilých je zákonné zakotvení forem vzdělávání a výchovy o nových technologiích a jejich hrozbách. V procesním právu je pak zřejmě vhodné zvážit alternativy, které lze poskytnout dotčenému oproti klasickému občanskoprávnímu procesu, který, jak bylo naznačeno v této práci, nemusí být, vzhledem k povaze

³¹⁴ SCHÖNBERGER, V.-M.; *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, s. 137. ISBN 978-0-691-13861-9

prostředí kyberprostoru, pro řešení osobnostních právních sporů, ve své současné podobě ideální. Při úvahách o případném možném vybudování orgánu pro alternativní řešení zásahů do ochrany osobnosti v kyberprostoru je však potřeba mít na paměti, že se stále jedná o klasický institut občanského práva, a posuzován by tak měl být vždy s převahou expertního názoru právníka a nikoli technologicky či jinak vzdělané osoby. Vzhledem k nepředvídatelnému směru rozvoje technologií bude vhodné podrobovat jakýkoli právní systém zabývající se ochranou osobnosti nezletilých v kyberprostoru revizím ve světle nových objevů a inovací. V souvislosti s tím lze také navrhnout setrvalé vzdělávání v nových teoriích na poli kybernetického práva, které mohou být podle potřeby v nutné míře začleněny do existujícího systému regulace. Lze tedy shrnout, že základními elementy při tvorbě nového právního rámce ochrany osobnostních práv v kyberprostoru by měl být důraz kladený na legislativu, vzdělávání, spolupráce s PSISs, uplatnění alternativních způsobů řešení sporů (ODR), častá revize platného práva a testování nových právních prostředků³¹⁵.

5.7.1. Otázka uživatelského průkazu

Podle platného českého práva nezletilý nemůže volit, pít alkohol ani řídit automobil do 18ti let. Internet není jiný, než výše zmiňované vozidlo: uživatel může způsobit újmu sobě i ostatním. To, že ví, jak automobil ovládat, neznamená, že zná také pravidla silničního provozu. Fakticky právní regulace užívání internetu nezletilými funguje téměř výhradně na bázi ad hoc rozhodnutí v diskreční pravomoci PSISs, a to převážně na základě upozornění. Autorka této práce se domnívá, že internet by se mohli nezletilí učit užívat jako již zmíněný dopravní prostředek, na základě provizorního „technologického průkazu“. Oboustranně výhodná by byla spolupráce s PSISs. Stejně, jako např. v Korejské republice by se děti vzdělávaly nejen v informatice, ale také v netiketě a bezpečném pohybu v kyberprostoru. Takto by měla být omezena i anonymita v kyberprostoru. Technologický průkaz by bylo možné podmíněčně nebo nepodmíněně na určitou dobu odebrat, což by fakticky představovalo možnost užívat pouze ekvivalent zeleného internetu, tedy internetu neobsahujícího závadný obsah a to bez výhod Webu 2.0, tedy bez možnosti po síti komunikovat s okolím. Užívání internetu nezletilými před nabytím plnohodnotného technologického průkazu by mělo být

³¹⁵ Legislation, Education, Cooperation, Alternative dispute resolution, Revision and Testing of alternative legislative solutions (LECART)

sledováno v součinnosti s PSISs. Regulace by byla možná, co se týče škodlivého obsahu, ale také behaviorálního marketingu. PSISs by museli dále podíl reklamního prostoru věnovat na propagaci bezpečného užívání internetu, vzdělávání a vhodných aktivit pro mládež mimo síť, jako je sport nebo jiná zájmová činnost. Nezletilé děti by mohly získávat bonusy a odměny za správné užívání internetu. Pokud např. čas tráví také na vzdělávacích stránkách a nepřesahují doporučený denní limit užívání internetu, mohou na internetu dostat nekopírovatelné bonusy: hudbu, mini hry, aplikace, pozdravy od svých vzorů atp. PSISs, kteří se do programu zapojí, by mohli být motivováni daňovými úlevami nebo dobrým PR pro společnost a možností „vychovat si“ svou všudypřítomností nové uživatele. U PSISs, kteří nejen nespolupracují, ale jejich podnikatelská činnost vychází z prokazatelně závadného obsahu, by mohli být negativně motivováni nastavením podobného znevýhodňujícího režimu, jaký je nastaven např. pro výrobce a distributory tabákových výrobků. Pokud by se neprůchodnou ukázala varianta zeleného internetu, mohla by být aplikovatelná mírnější varianta „dětského internetu“, tedy kombinace zvláštní oddělené registrace, jako u Teen Second Life a ratingu stránek za pomoci známek hodnotících vhodnost obsahu a úroveň bezpečnostního rizika z pohledu ochrany osobních údajů. Problémem zůstává otázka Webu 2.0. V ideálním případě by komunikační prvek internetu měl být před dosažením technologického průkazu omezen. Rodič by měl povinností stejným způsobem zajistit také smartphone dítěte. Rodiče by měli mít nárok na bezplatnou technickou podporu. Systém by mohl nejen zajistit primární pozitivní funkci internetu, jako prostředku osobního rozvoje a přístupu k hodnotným informacím, ale také pomoci dítěti vybudovat si správné komunikační návyky od soukromí, přes efektivní užívání až po předcházení pirátství. Ve spolupráci se školou by mohli rodiče dítěti navolit, jaké dotované programy a vzdělávací hry jsou pro něj, na základě jeho studijních výsledků, vhodné, a to nejen na bázi on-line doučování, ale především za účelem rozvoje přirozeného studijního zaměření či talentu. Regulovány by měly být také herní a internetové kavárny. Ideálně by do nich neměl být nezletilý, který u sebe nemá platný technologický průkaz, vpuštěn ani jako divák. Dodržování by mělo být zajištěno hrozbou vysokých pokut a častých kontrol.

S vědomím zde uvedeného, je však potřeba upozornit, že podobně nastavený režim ochrany osobnosti nezletilých dětí v kyberprostoru by byl velice striktní, závislý

na kontrolních subjektech, které by se tak mohly stát cenzory, a mimoto by omezoval právo nezletilých na svobodu projevu či budování sociálních vazeb v kyberprostoru. Systém by navíc mohl podléhat manipulaci. Nalezení vhodnějšího přijatelného kompromisu tak bude jedním z úkolů rozvíjejícího se oboru kybernetického práva.

6. Závěr

Subjekty, kterými se tato práce zabývala, byly nezletilí, příslušníci expertní generace informační společnosti, která je typická znalostní dominancí kyberprostoru nad generací autorit, a zároveň jí nejsou dostupné dostatečně účinné právní prostředky ochrany v kyberprostoru často ohrožovaných osobnostních práv.

Jako každá inovace, jsou služby informační společnosti pouhými nástroji v rukou člověka. Není vyloučeno, že i s podpůrným právním systémem, zajišťujícím vymahatelnost práva na ochranu osobnosti na internetu, dojde časem k regulaci Webu 2.0 za pomoci nových sociálních norem či užitím „nudges“³¹⁶, a zároveň ke zpomalení informačního boomu procesem „odpojování“³¹⁷ uživatelů od technologií. Navrhované alternativní využití institutu ochrany osobnosti by umožňovalo rychlejší, efektivnější, diskrétnější a citlivější ochranu zaručených práv nejen nezletilých, ale všech uživatelů za stavu, kdy se společnost doposud nepřizpůsobila možnostem, které kyberprostor a inovace poskytují.

³¹⁶ Nudges (ang.) pobídky uživatelů, způsob, jakým je motivování rozhodování uživatele v kyberprostoru k většímu důrazu na ochranu svého soukromí a redukování sdílení resp. motivování k zodpovědnému sdílení. Jedná se především o nástroje webové architektury, které jsou protipólem k ovlivňování uživatelů ke komerčním účelům známému z internetu.

³¹⁷ ŚLUSARSKI, P.; The joy of disconnection. *Warsaw Business Journal*, Volume 181, Number 39, 2012. 1-7. říjen. s. 12, 13

Summary

The research study for this thesis was initiated because of an interest of the author in the field of *personality rights* protection, her experience as an average user of modern technologies and her interest in the ways innovations influence the evolution of modern society, foremost the youngest generation or the so called “digital natives“. Thanks to their fast development, new technologies have become a part of every aspect of human life, both public and private. From politics through economy to medicine, arts or family matters. The most important field of law dealing with internet communication and e-commerce is information privacy law.

This thesis aims to highlight that the most active segment of internet users are tech-savvy youth. Many of the third party activities in cyberspace, both social and business, possess potential threat to minors. Legal issues in cyberspace include cyber security breaches, fraud, stalking, privacy invasion, defamation, sexual crimes victimizing children, as well as commoditization of personal data and behavioral marketing in forms which represent illicit business practice.

Presently, any such potential or actual thread or a dispute involving the users of Internet services is regulated either by laws that often seem to be rather vague and inconsistent or by self-regulatory rules set by Internet service providers (ISPs). Thus, the level of protection of minors is often in hands of the service provider that only might need to comply with the Safe Harbor Principles or similar compromise *sui generis* or national laws either stemming from EU data protection framework or in combination with traditional privacy laws, alternatively this is governed by relatively tolerant US privacy laws.

The aim of the thesis is to provide a complex introduction into user activities of minors in cyberspace and to point out how these can endanger their *personality rights*. Furthermore, by illustrating this issue through case studies, this thesis will analyze current legal measures provided to deal with this problem within the discretion of courts in the EU and in the U.S.A. This thesis also contains analysis of the legal framework of privacy laws in the Czech Republic, privacy/data protection regulation in the EU, and will introduce the system of legal regulation of the problem at issue in the United States along with the examination of the applicability of these systems in cyberspace.

This thesis will address both law in force and some of the most important legal acts expected to come in force in the near future. Any future legal regulation of privacy and other *personality rights* in cyberspace requires new framework that will be better applicable in the age of the new information society.

This thesis recognizes the difficulty of the topic and therefore reviews not only the present laws but also focuses on the historical development, both legal, and technological. The legal analysis will point out some questionable aspect of current law and will discuss some of the most interesting theories on the protection of *personality rights* in cyberspace.

This thesis is composed of the results of the research based on the examination and analysis of the Czech and foreign literature, statutory law, case law and interdisciplinary studies and it outlines in the end a summary of findings that might serve as a “checklist” or suggestions for any future legislative proposals in the area of legal protection of *personality rights* of minors in cyberspace. In this respect the purpose of this paper is to argue in favor of deeper interdisciplinary research and cooperation in the case of any future legislative initiative in this field.

The goal of the study is to provide an introduction to the field of current services of the new information society used by minors, point out the problems of the applicability of the relevant law in this field, to analyze expected and anticipated policy and legal regulation of *personality rights* in cyberspace and to present a list of theoretical alternatives for the future solutions of civil law infringement into *personality rights* of minors in cyberspace.

Seznam použité literatury

Judikatura

ČR

- nález Ústavního soudu ze dne 4. října. 1995 sp. zn. I. ÚS 15/95
nález Ústavního soudu ze dne 8. února 2000 sp. zn. I. ÚS 156/99
nález Ústavního soudu ze dne 1. března 2000 sp.zn. II ÚS 517/99
nález Ústavního soudu ze dne 11. listopadu 2005 sp. zn. I. ÚS 453/03
nález Ústavního soudu ze dne 17. července 2007 sp. zn. IV. ÚS 23/2005
Rozsudek Nejvyššího soudu České republiky ze dne 8. srpna 2007, sp. zn. 30 Cdo 2782/2007
Usnesení Nejvyššího soudu České republiky ze dne 16.8 2007, sp. zn. 30 Cdo 2082/2007
Usnesení Nejvyššího soudu České republiky ze dne 31. 1. 2008, sp. zn. 30 Cdo 2072/2007
Rozsudek Nejvyššího soudu České republiky ze dne 31.1 2008, sp. zn. 30 Cdo 336/2007
Rozsudek Nejvyššího soudu České republiky ze dne 12. 11. 2008, sp. zn. 31 Cdo 3161/2008
Rozsudek Vrchního soudu v Praze ze dne 2. 3. 2011, č. j. 3 Cmo 197/2010-82
Rozsudek Vrchního soudu v Olomouci ze dne 28. 1. 2009, sp. zn. 1 Co 119/2008
Rozsudek Krajského soudu v Brně ze dne 31. 10. 2007, sp. zn. 24 C 48/2004

USA

- Olmstead v. United States*, 277 U.S. 438 (1928)
Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931)
Wheaton v. Peters, 33 U.S. 591, 634 (1834)
Griswold v. Connecticut, 381 U.S. 479 (1965)
Eisenstadt v. Baird, 405 U.S. 438 (1972)
Roe v. Wade, 410 U.S. 113 (1973)
Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997)
Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998)

M.G. v. Time Warner, Inc. 89 Cal. App. 4th 623, 632 (Cal. Ct. App. 2001)
Cannon v. Mathis, S02G0361 (Ga. Sup. Ct., Nov. 25, 2002)
Stephen J. Barrett, et al. v. Ilena Rosenthal, S122953, 40 Cal.4th 33 (Cal. Sup. Ct., November 20, 2006)
Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006)
Moreno v. Hartford Sentinel, Inc., 172 Cl. App. 4th 1125 (Cal. Ct. App. 2009)
United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)
Catsouras v. Department of California Highway Patrol, 181 Cal. App. 4th 875 (Cal. Ct. App 2010)
Pazdera v. Pazdera, 794 N.W.2d 926 (Wis. Ct. App 2010)
Minnesota v. Melchert-Dinkel, 2011 WL 893506 (Minn. Dist. Ct. 2011)
Williamson v. State, 2011 Ark. App. 73 (Ark. Ct. App. 2011)
People v. Hartus, 2012 NY Slip Op 22175 [36 Misc 3d 868]

ESLP

Rozhodnutí ESLP z 18. října 2005, *Stephane Laurent Perrin v. United Kingdom*, 5446/03
Rozhodnutí ESLP z 2. prosince 2008, *K.U. v. Finland*, Application no. 2872/02

Velká Británie

Laurence Godfrey v. Demon Internet Ltd., QBD, [1999] 4 All ER 342, [2000] 3 WLR 1020; [2001] QB 201
Murray v. Big Pictures (UK) Ltd. (CA), [2008] EWCA Civ 446
Moseley v. News Group Newspapers [2008] EWHC 1777 (QB), (2008)
Kaschke v. Gray and Hilton [2010] EWHC 690

Spolková republika Německo

OLG Frankfurt/M. z 11. září 1986 – 6 U 171/85

Španělsko

Alfacs Vacances SL v Google Spain SL [2012] (Unreported, Court of First Instance of Amposta, 23. únor 2012)

ESD

Lindqvist v. Sweden C-101/1

Productores de Música de España (Promusicae) v. Telefónica de España SAU C-275/06

Commission of the European Communities v. Kingdom of Belgium, C-275/04

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, spojené věci C-92/09 a C-93/09 (2010)

Satamedia, C-73-07 (2008) ECR I-09831

Právní předpisy

Česká republika

Ústavní pořádek České republiky

Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Zákony

Zákon č. 40/1964 Sb., Občanský zákoník

Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

Zákona č. 99/1963 Sb., občanský soudní řád

Zákon č. 500/2004 Sb., správní řád

Zákon č. 141/1961 Sb., o trestním řízení soudním

Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů

Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,

Zákon č. 91/2012 Sb., o mezinárodním právu soukromém

Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů

Zákon č. 94/1963 Sb., o rodině ve znění pozdějších předpisů

Evropská Unie

Listina základních práv EU (2007/C 303/01)

Smlouva o fungování Evropské unie (SFEU)

Proposal for a Regulation of the European Parliament and of the Council COM(2012) 11 final of 25.1 2012, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Nařízení Řím I (č. 593/2008), respektive nařízení Řím II (č. 864/2007)

Nařízení Brusel I (č. 44/2001)

Směrnice Evropského parlamentu a Rady

95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údaj a o volném pohybu těchto údajů

2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu

2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací ve znění směrnice 2009/136/ES

2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

směrnice Evropského parlamentu a Rady 2002/20/ES ze dne 7. března 2002 o oprávnění pro sítě a služby elektronických komunikací

2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení ve znění směrnice 2009/140/ES

2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, ve znění směrnice 2009/140/ES

směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

Velká Británie (UK)

UK. Defamation Bill, Dostupný z vládních stránek WWW:

<<http://services.parliament.uk/bills/2012-13/defamation.htm>>

Kanada

Kanada. Criminal Code of Canada, R.S. 1985. Dostupný také z WWW:

<http://www.efc.ca/pages/law/cc/cc.html>

USA

Ústava Spojených států amerických

The Child Online Protection Act (COPA)

Children's Online Privacy Protection Act of 1998 (COPPA)

Communication Decency Act (CDA)

Identity Theft and Assumption Deterrence Act

Video Voyeurism Prevention Act

Computer Fraud and Abuse Act

Children's Internet Protection Act

The Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act

Tyler Clementi Higher Education Anti-Harassment Act

Megan's Law

Alicia Law

Monografie, komentáře, kolektivní monografie, sborníky

ALLEN, A.; *Unpopular Privacy: What Must We Hide?*, Oxford University Press, 2011.
ISBN 0195141377

ANDREWS, Lori B.; *I know who you are and I saw what you did: social network and the death of privacy*, Free Press, 2012. ISBN 978-1-4516-5051-8

COOLEY, T.M.; *A Treatise on the Law of Torts* (2d ed. 1888)

- ECKERTO VÁ, L.; DOČEKAL, D.; *Bezpečnost dětí na internetu*, Computer Press, Brno, 2013, ISBN: 978-80-251-3804-5
- FRIED, Ch. Pivacy. *The Yale Law Journal*, 1968, Vol. 77., No. 3, 474, 477
- JEHLIČKA, O.; ŠVESTKA, J. a kol: *Občanský zákoník. Komentář*. 3. vydání, Praha, C.H. Beck, 1996. ISBN 80-7179-063-X
- KNAP, K.; ŠVESTKA, J.; JEHLIČKA, O.; PAVLÍK, P.; PLECITÝ, V.; *Ochrana osobnosti podle občanského práva*, 4. vydání, vyd. Linde Praha a.s., 2004. ISBN 80-7201-484-6
- KOPECKÝ, K.; KREJČÍ, V.: *Rizika virtuální komunikace*, (2010), NET University, ISBN: 978-80-254-7866-0
- KUNER, Ch.; The European Commission's Proposed Data protection Regulation“ A Copernical Revolution“ in European Data Protection Law. *Bloomberg Privacy and Security Law Report*. 2012, 11, PVL R 215. ISSN 1538-3431
- LAUDON, K.; Markets and Privacy, *NYU Working Paper*, 1993, No. 2451/14257
- LIEVENS, E.; *Protecting children in the digital era: the use of alternative regulatory instruments*, Leiden; Boston: Martinus Nijhoff Publishers, 2010. ISBN 9789004184770
- NIEMZ, K. et al., Prevalence of Pathological Internet Use among University Students and Correlations with Self-Esteem, the General Health Questionnaire (GHQ), and Disinhibition, [online] *CyberPsychology & Behavior*. 6. prosince 2005, [cit-2012-09-18] , Volume: 8 vydání 6, s. 562-570. Dostupný také z WWW: <<http://online.liebertpub.com/doi/abs/10.1089/cpb.2005.8.562>>
- PALFREY, J.; GASSER, U.; *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books, 2008. ISBN 978-0-465-00515-4
- PARSON, J. M.; An examination of massively multiplayer online role-playing games as a facilitator of internet addiction, [online] *Iowa Research Online*. 2005 [cit. 2012-08-11]. Dostupný také z WWW: <<http://ir.uiowa.edu/etd/98/>>
- PEUKERT et al., Internet- and computer game addiction: phenomenology, comorbidity, etiology, diagnostics and therapeutic implications for the addictives and their relatives,

- Psychiatr Prax.* [online] 2010, Epub 2010, červenec 37(5) [cit. 2012-07-14] s. 219-24.
Dostupný z WWW: <<http://www.ncbi.nlm.nih.gov/pubmed/20597036>>
- POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí*, Brno, 2006.
221 s. Doktorandská práce. Masarykova Univerzita, Právnická fakulta, Katedra
obchodního práva. Vedoucí práce Petr Hajn. Dostupný také z WWW:
<http://is.muni.cz/th/21177/pravf_d/disertacni_prace_-_text.pdf>
- POLČÁK, R.; *Internet a proměny práva*, Auditorium, Praha 2012
- PROSSER, W. L.; *Privacy, California Law Review*, (1960) Vol. 48 No. 3 s. 383
- ROWBOTTOM, J. The rant, vent and converse: protecting low level digital speech,
Law Journal: Cambridge Law Journal, 2012, 71(2), 355-383 s.
- SAMUELSON, P.; *Privacy as Intellectual Property? Stanford Law Review*, květen 2000,
Stan. L. Rev. 1125
- SCHÖNBERGER, V. M.; *Delete: The Virtue of Forgetting in the Digital Age*.
Princeton University Press, 2009. ISBN 978-0-691-13861-9
- SCHULZ, J. et al., Why Parents Help Their Children Lie to Facebook About Age:
Unintended Consequences of the 'Children's Online Privacy Protection Act. *First
Monday*, Volume 16, Number 11 – 7. listopad 2011. Dostupný z WWW:
<<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075>>
- SCHWARZ, P. M.; *Property, Privacy, and Personal Data. Harvard Law Review*. 2004,
2055
- SOLOVE, D. J.; SCHWARTZ, P. M. *Privacy law fundamentals*, The International
Association of Privacy Professionals (IAPP), 2011. ISBN 978-0-979501-9-1
- SOLOVE, Daniel J., SCHWARTZ, Paul M.; *Information privacy law*. 4. vyd., Aspen
Elective Series, Wolters Kluwer Law and Business, 2011. ISBN 0735510407
- ŠVAŇHAL, R.; *Poznámky k ochraně osobnosti nezletilých osob, Právní Praxe*
10/2000, 2000. s. 635-643
- WANG, F. F.; *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US
and China*, Bournemouth University, Cambridge University Press, 2010. ISBN:
1139488457

WARREN, S. a BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*. 1890, IV, 15.

WHITMAS, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Faculty Scholarship Series*, 2004, Vol. 113, No. 6. (2004). Dostupný také z WWW: <<http://www.yalelawjournal.org/pdf/113-6/WhitmanFINAL.pdf>>

ZITTRAIN, J.; *The Future of Internet and How to Stop It*, Yale University Press, 2008. ISBN 9780300124873

ZLATUŠKA, J.; Informační společnost. *Zpravodaj ÚVT MU*. 1998, roč. VIII, č. 4, s. 1-6. ISSN 1212-0901. Dostupný také z WWW: <<http://www.ics.muni.cz/bulletin/articles/122.html>>

Časopisecké články (off-line a on-line)

7,500 Online Shoppers Unknowingly Sold Their Souls. [online], *Fox News* 15. duben, 2010 [cit-2012-07-21]. Dostupný z WWW: <<http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/>>

Alarming increase in Facebook related divorces in 2011. [online] *Divorce. Online Blog.*, 28. prosinec, 2011 [cit. 2012-11-02]. Dostupný z WWW: <<http://blog.divorce-online.co.uk/?p=2338>>

AVILA, J. et al. A Family Nightmare. [online] *abc News*, 16. listopad 2007 [cit. 2012-08-12]. Dostupný z WWW: <<http://abcnews.go.com/TheLaw/story?id=3872556&page=1>>

BENNETT, J; A Tragedy That Won't Fade Away, [online] *NEWSWEEK*, 25. duben, 2009, [cit. 2012-08-12]. Dostupný z WWW: <<http://www.newsweek.com/2009/04/24/a-tragedy-that-won-t-fade-away.html>>

Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers. [online] *American Academy of Matrimonial Lawyers*, 10. únor, 2010 [cit. 2012-11-02]. Dostupný z WWW: <<http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social-networking-evidence-says-survey->>>

BOSKER, B.; Facebook's Randi Zuckerberg: Anonymity Online Has to Go Away [online] *Huffington Post*, 26. září 2011 [cit. 2012-12-11]. Dostupný z WWW:

BŘÍZA, P.; Nový zákon o mezinárodním právu soukromém je pro praxi přínosem. [online] *iDnes*, 18. srpen 2012 [cit. 2012-11-28]. Dostupný z WWW: <http://finance.idnes.cz/novy-zakon-o-mezinarodnim-pravu-soukromem-je-pro-praxi-prinosem-phk-/pravo.aspx?c=A120817_155730_pravo_vr>

CÍSAŘOVÁ, Z.; *Elektronická data a cloud computing z pohledu autorského práva a ochrany osobních údajů*. Univerzita Karlova v Praze, Právnická fakulta (2012), s. 32

COHEN, D.; Mom disciplines daughter with humiliating Facebook Timeline cover image, [online]. *Allfacebook*, 26. duben 2012 [cit. 2012-07-21]. Dostupný z WWW: <http://allfacebook.com/cover-image-discipline_b87219>

Consumer Reports Magazine, That Facebook Friend might be 10 Years Old. červen 2011, Dostupný také z WWW: <<http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm>>

DOBEŠOVÁ, P.; SZOTKOWSKI, R.; Stručný přehled vybraných podmínek užívání Facebooku, [online] *e-bezpečí*, 2. leden, 2013, [cit. 2013-13-01] Dostupný z WWW: <<http://www.e-bezpeci.cz/index.php/temata/socialni-sit/587-struny-pehled-vybranych-podminek-uivani-facebooku>>

ESSERS, L.; Regulators confirm Facebook deleted all EU facial recognition data, [online] *PCW World*, 7. únor, 2013 [cit. 2013-02-12]. Dostupný z WWW: <<http://www.pcworld.com/article/2027598/regulators-confirm-facebook-deleted-all-eu-facial-recognition-data.html> >

Facebook: Karla James' death revealed to mother. [online] *BBC News*, 20. září 2012 [cit. 2012-12-21] Dostupný z WWW: <<http://www.bbc.co.uk/news/uk-wales-south-east-wales-19662314>>

Georgia Girl Sues Classmates For Bullying Her On Facebook, [online] *CBS Atlanta*, 1. květen, 2012 [cit. 2012-12-11]. Dostupný z WWW: <<http://atlanta.cbslocal.com/2012/05/01/georgia-girl-sues-classmates-for-bullying-her-on-facebook/>>

GOMSYN, A.; Daughter 'Begged' for Spanking Instead of Mom's Embarrassing Web Photo [online]. *abc news*, 21. květen 2012 [cit. 2012-12-02]. Dostupný z WWW: <<http://abcnews.go.com/blogs/lifestyle/2012/05/daughter-begged-for-spanking-but-author-posted-embarrassing-web-photo-instead/>, Mom Disciplines Daughter With Humiliating Facebook Timeline Cover Image>

HOF, R.; Second Life's First Millionaire. [online], *Bloomberg Business Week*, 26. listopad 2006 [cit. 2012-09-14]. Dostupný také z WWW: <http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_firstname.htm>

Huge Disparity in Facebook's Ads Display and Ads Revenue. [online] *Webmaster BNXS*, 11. leden, 2011 [cit. 2012-10-12]. Dostupný z WWW: <<http://bnxs.com/huge-disparity-in-facebook%E2%80%99s-ads-display-and-ads-revenue/>>

Chlapec ukradl v on-line hře postavu bojovníka, zadržela ho policie, [online] *novinky.cz*, 16. leden, 2011, [cit. 2012-08-21] Dostupný z WWW: <<http://www.novinky.cz/krimi/290172-chlapec-ukradl-v-on-line-hre-postavu-bojovnika-zadrzela-ho-policie.htm>>

JAMES, S., COHEN, L; Tightening the Net: defamation reform and ISPs. [online] *Lexology*, 6. červen 2012 [cit. 2012-09-08]. Dostupný také z WWW: <http://www.lexology.com/library/detail.aspx?g=b0577392-ba57-414e-a481-4f7ae68724e6>

JANÁK, M., Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu. [online]. *IT Právo*, 2009 [cit. 2012-11-19]. Dostupný z WWW: <http://www.itpravo.cz/index.shtm?l?AA_SL_Session=8bab7c81254d3179ff720eb355e677c0&sh_itm=556af04eed0e>

JANUŠ, J.; Rozhovor s R. Polčákem: Hodně z toho, s čím lidé souhlasí na sítích, je nemravné nebo neplatné. *Právní rádce*. (2012) 10/2012. S. 12-15

JOHNSON, B.; Privacy No Longer a Social Norm, says Facebook Founder. [online] *The Guardian*, 11. leden 2010 [cit. 2012-17-08]. Dostupný z WWW: <<http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>>

Just How Many Facebook Friends Do You Need? [online]. *Newsweek Magazine*. 15. říjen, 2012 [cit. 2012-20-10]. Dostupný z WWW:

<<http://www.thedailybeast.com/newsweek/2012/10/14/just-how-many-facebook-friends-do-you-need.html>>

K právu na soukromí a rodinný život (II. ÚS 517/99). *Soudní rozhledy: Z aktuálních nálezů Ústavního soudu*. 3/2000

KEMÉRYOVÁ, Z.; České děti přitahuje internet. Podceňují riziko anonymního seznamování. [online]. *Ihned*, 21. červenec 2012 [cit. 2012-11-05]. Dostupný z WWW:

<<http://zpravy.ihned.cz/cesko/c1-56609270-ceske-deti-pritahuje-internet-podcenuji-riziko-anonymniho-seznamovani>>

KIRKPATRICK, M.; Google, Privacy and the Explosion of New Data. [online]

Techonomy, 4. srpen 2010 [cit. 2012-08-09]. Dostupný z WWW:

<<http://techonomy.typepad.com/blog/2010/08/google-privacy-and-the-new-explosion-of-data.html>>

LEE, A.; Apple Hit with Class Action Lawsuit Over Minors' Purchase Of In-App Goods. *Huffington Post* [online] 16. leden 2011, [cit. 2012-08-21]. Dostupný také z WWW: <http://www.huffingtonpost.com/2011/04/15/apple-hit-with-class-acti_n_849936.htm>

LOEBL, Z.; Řešení reklamací on-line otevře e-shopům nové trhy. [online] *Hospodářské noviny*, 25. květen, 2012, [cit. 2012-09-22]. Dostupný z WWW: <<http://hn.ihned.cz/c1-55872670-zbynek-loebl-reseni-reklamaci-on-line-otevire-e-shopum-nove-trhy>>

MAAG, CH.; A Hoax Turned Fatal Draws Anger but No Charge. [online] *The New York Times*. 28. listopad, 2007 [cit.-2012-07-28]. Dostupný z WWW:

<http://www.nytimes.com/2007/11/28/us/28hoax.html?pagewanted=print&_r=0>

MAREŠ, D.; 81280 K limitaci odpovědnosti providera v prostředí internetu – 1. část. [online]. *Epravo*, 16.3 2012 [cit. 2012-11-08]. Dostupný z WWW:

<<http://www.epravo.cz/top/clanky/k-limitaci-odpovednosti-providera-v-prostredi-internetu-1-cast-81280.html>>

MATEJKA, J.; ČERMÁK, J.; Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah. [online]. *ITPrávo* 2001, [cit. 2012-09-23]. Dostupný z WWW:<<http://www.itpravo.cz/index.shtm?x=48792>>

MATYSZCZYK, Ch.; School shows off its laptop surveillance tactics. [online] *CNET*, 26. únor 2010 [cit. 2012-12-19]. Dostupný z WWW: <http://news.cnet.com/8301-17852_3-10460729-71.htm>

MICHELL, A., P.; Gamer Killed Over Virtual Legend of Mir 3 Sword. [online]. *The Internet Patrol*, 14. říjen, 2010 [cit. 2012-05-14]. Dostupný z WWW: <<http://www.theinternetpatrol.com/gamer-killed-over-virtual-legend-of-mir-3-sword/>>

Ministerstvo školství dostalo pokutu 450 tisíc za únik dat o Romech [online] *Eurozpravy*, [cit. 2012-08-12]. Dostupný z WWW: <<http://domaci.eurozpravy.cz/skolstvi/53026-ministerstvo-skolstvi-dostalo-pokutu-450-tisic-za-unik-dat-o-romech/>>

MORÁVEK, J., BURIAN, D.; *Předávání osobních údajů do zahraničí: Česká a Evropská právní úprava, otázky a odpovědi*, Linde Praha, a.s., 2012, s. 170

MORRIS, K.; BlogTV and the sad, avoidable path to Amanda Todd's suicide. [online] *The Daily Dot*. 15. říjen 2012 [2012-12-27]. Dostupný z WWW: <<http://www.dailydot.com/news/blogtv-amanda-todd-suicide/>>

MUSKAL, M.; Rutgers suicide: Tyler Clementi's parents won't sue in webcam case, [online] *Los Angeles Times*. 5. říjen 2012 [cit. 2012-10-09]. Dostupný z WWW: <<http://articles.latimes.com/2012/oct/05/nation/la-na-nn-clementi-parents-wont-sue-rutgers-20121005>>

Na internetu přibývá dětí i starých. [online], *ManagerWebIHNed.cz*, 19. červen 2012 [cit. 2013-02-12]. Dostupný z WWW: <<http://managerweb.ihned.cz/c1-56207930-na-internetu-pribyva-deti-i-starych>>

NERADOVÁ, V.; Ochrana osobnosti, Zamyšlení nad otázkou zohlednění „plynutí času“ při uplatnění nároků z titulu ochrany osobnosti. *Právní rozhledy*. 2011, PR 102/2011. s. 362, 363

OTEVŘEL, P.; Sociální síť z pohledu firmy: Co můžete a co ne?, *Právní rádce*. (2012) 10/2012. s. 8-11

OTTERBEIN, N.; It's not just Lower Merion!: Bronx school watches unwitting students via Webcam. [online]. *City Paper*, 26. únor 2010 [cit-2012-08-12]. Dostupný z WWW:

<http://www.citypaper.net/blogs/nakedcity/its_not_just_lower_merion_bronx_school_watches_unwitting_students_via_webcam.htm>

PETERKA, J.; *Slovník Jiřího Peterky* [online]. Praha. [cit. 2012-08-24]. Dostupný z WWW: <<http://www.earchiv.cz>>

PFANNER, E., A Proposal for E.U.-Wide Data Protection Regulation, *N.Y. Times*, 20. listopad, 2011

POLČÁK, Radim. Lex Informatica - užitečnost práva a budoucnost informační sítě. In Vladimír Zoufalý. *XX. Karlovarské právnícké dny*. 1. vyd. Praha: Leges, 2012. s. 236-249, ISBN 978-80-87576-16-8

QUAN, D., Amanda Todd: Mother of girl's accused tormentor lashes out at online 'lynch mob'. [online]. *canada.com*, 17. říjen 2010 [cit. 2012-12-21]. Dostupný z WWW: <<http://www.canada.com/news/Amanda+Todd+Mother+girl+accused+tormentor+lashes+online+lynch/7400570/story.htm>>

ROMOLINI, J.; Best Facebook update of all time, posted by a dad. [online] *Shine*, 4. srpen 2011, [cit. 2012-07-20]. Dostupný z WWW: <<http://shine.yahoo.com/work-money/best-facebook-update-of-all-time-posted-by-a-dad-2520529.htm>>

ROSEN, J.; Google's Gatekeepers, *The New York Times*, 30. listopad, 2008

Rozhovor s Vladimírem Smejkaem. Elektronické důkazy – současnost či budoucnost českého soudnictví? *Bulletin Advokacie* 2012 9/2012, s. 11

Son learns of father's suicide through scarring Twitter photos. [online] *The Dot Com*, červen 2012 [cit. 2012-11-18]. Dostupný z WWW:<<http://www.dailydot.com/news/son-father-suicide-twitter-photos/>>

State of Audience Targeting Industry Study, [online] *Audience Science Press Release*, leden, 2011 [cit. 2013-01-10]. Dostupný také z WWW: <<http://www.audiencescience.com/uk/press-room/press-releases/2011/state-audience-targeting-industry-study-50-advertisers-set-boost-spen>>

STRAWBRIDGE, M., Netiquette - Internet etiquette in the age of the blog, Software Reference Ltd., 2006; *Business Know-how*, Five Rules of Twitter Etiquette, Dostupný z WWW: <<http://www.businessknowhow.com/internet/twitter-etiquette.htm>>

SVOBODA, P.; Průzkum Intel: Na sociálních sítích vytváříme své „lepší já“ [online], *UltraYou, Intel* [cit. 2012-11-05]. Dostupný také z WWW: <<http://www.playzone.cz/clanky/pruzkum-intel-na-socialnich-sitich-vytvarime-sve-lepsi-ja>>

ŠLUSARSKI, P. The joy of disconnection. *Warsaw Business Journal*, volume 181, Number 39, 2012. 1-7. Říjen

THOMSON, B., Staying safe and taking risks. [online]. *BBC*, 14. květen 2007 [cit. 2012-12-02]. Dostupný z WWW: <<http://news.bbc.co.uk/2/hi/technology/7400158.stm>>

TOGERIUS, J.; Harvard Prof Says Computers Need to Forget. [online] *Sloshdot*, 10. květen, 2007, [cit. 2012-11-08]. Dostupný z WWW: <<http://yro.slashdot.org/comments.pl?sid=234167&cid=19065957>>

Tři mladé Němky spáchaly sebevraždu. [online], *idnes.cz*. 17. srpen 2011 [cit. 2012-09-23]. Dostupný z WWW: <http://zpravy.idnes.cz/tri-mlade-nemky-spachaly-v-lese-spolecnou-sebevrazdu-p00-/zahranicni.aspx?c=A110816_212723_zahranicni_brm>

Village Sleuth Unmasks US Internet Predator Behind Suicide Pacts. [online] *Algeria.com*, [cit-2012-09-12]. Dostupný z WWW: <<http://www.algeria.com/forums/computer-internet/27173-village-sleuth-unmasks-u-s-internet-predator-behind-suicide-pacts.html>>

WAGNEROVÁ, E.; *Právo na soukromí: Kde má být svoboda, tam musí být soukromí*, Právo na soukromí., MUNI Press, Mezinárodní politologický ústav Masarykovy univerzity, 2011.

WARMAR, M., EU Privacy regulations subject to „unprecedented lobbying“. [online] *The Telegraph*, 8. únor 2012, [cit. 2012-07-12]. Dostupný z WWW: <<http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.htm>>

WINTER, J.; The advantages of amnesia: From the Internet to the iPod, technology is bringing rapid advances in memory. What society needs now are new ways to forget.

Boston Globe, 23. září 2007 [cit. 2012-12-20]. Dostupný také z WWW:

<<http://www.highbeam.com/doc/1P2-8717181.html>>

ZAHRADNÍČEK, J.; 88471. Odpovědnost poskytovatelů služeb informační společnosti - několik postřehů k závěrům Vrchního soudu v Praze v kauze „PROLUX“. [online]

EPrávo, 14.2. 2013 [cit. 2013-03-02]. Dostupný z WWW:

<<http://www.epravo.cz/top/clanky/odpovednost-poskytovatele-sluzeb-informacni-spolecnosti-nekolik-postrehu-k-zaverum-vrchniho-soudu-v-praze-v-kauze-prolux-88471.html>>

ŽALUD, V.; Princip země původu ve směrnici o elektronickém obchodu, aneb bude v budoucnu platit na internetu tradiční mezinárodní právo soukromé? [online]. *Via Legis: Blog o právu a právní vědě*. 6. květen 2010 [cit-07-22-2012]. Dostupný z WWW:

<<http://vialegis.blogspot.cz/2010/05/princip-zeme-puvodu-ve-smernici-o.html>>

Ostatní literatura

ACQUISTI, A.; Privacy & Behavioral Economics: The Paradox of Control & Other Studies, 15. říjen, 2010 *Carnegie Mellon University*

ČERMÁK, J. et al.; Global Privacy Handbook 2011 Edition, *Baker & McKenzie* (2011)

Electronic Frontier Foundation. Dostupný z WWW: <<https://www.eff.org>>

EU Kids Online, Dostupný z WWW:

<<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx>>

Facebook, <<http://www.facebook.com/help>>

GPEN, Dostupný z WWW: <<https://www.privacyenforcement.net/public/activities>>

HENDRYCH, D. a kol.; Právní slovník, 3.vydání, 2009. *Beck-online*

Horká linka, <<http://www.horkalinka.net/>>

John D. and Catherine McArthur Foundation, Living and Learning with New Media: Summary of Findings from the Digital Youth Project, listopad 2008 [cit. 2012-07-14].

Dostupný z WWW: <www.digitalllearning.macfound.org/ethnography>

LESSIG, L.; The Laws of Cyberspace. [prezentace na konferenci, video] *Taiwan Net '98*, 1998

MACEK, J.; POLČÁK, R.; ŠKOP, M.; *Normativní systémy v kyberprostoru* (úvod do studia). Brno: Masarykova univerzita v Brně, 2005

PEW Internet 2010: Generations 2010. *Pew Research Center*. Dostupný také z WWW: <<http://pewinternet.org/Reports/2010/Generations-2010.aspx>>

Policie ČR, Prevence, <<http://aplikace.policie.cz/hotline/>>

Sexting a právo. *Projekt Nebud' obět'*, <<http://www.sexting.cz/>>

Symbio, <<http://www.symbio.cz/slovník/bannerova-slepota-banner-blindness.htm>>

ÚOOÚ, <<http://www.uoou.cz/uoou.aspx?menu=4>>

Wikipedie: Otevřená encyklopedie, <http://cs.wikipedia.org/wiki/Phishing>

Abstrakt

Cílem této práce je poskytnout úvod do problematiky ochrany osobnosti v kyberprostoru. Subjektem práce je segment nezletilých uživatelů služeb informační společnosti. Práce poskytuje sumarizaci uživatelských aktivit dětí a mládeže v kyberprostoru a analýzu potenciálních hrozeb pro osobnostní práva, které některá jednání v prostoru těchto služeb představují. Dále práce poskytuje porovnání a analýzu platné právní úpravy osobnostních práv v kontextu kyberprostoru a nových technologií, zejména práva na soukromí, a to v České republice, v rámci EU a v USA, a také náhled do očekávaných změn v této oblasti, daných aktuálním legislativním vývojem. Práce obsahuje případové studie, které si kladou za cíl osvětlit rozhodovací praxi soudů a poukázat na následky některých z nejzávažnějších zásahů do osobnostních práv nezletilých v kyberprostoru.

Práce představuje postoj, který klade důraz na širší využití občanskoprávního institutu ochrany osobnosti také pro tyto případy a interdisciplinární spolupráce při tvorbě nové legislativy. Práce poskytuje výčet některých alternativ, které by mohly přispět k zajištění poskytnutí větších právních záruk nejen nezletilým uživatelům Webu 2.0 a nových technologií, ale každému jejich uživateli.

Abstract

The purpose of this paper is to provide an introduction to the problems of the protection of *personality rights* in cyberspace. The subject of this study is a segment of minor users of Information and Communications Technology (ICT) services. This paper provides a summary of youth users' activity in cyberspace and an analysis of potential threats to their *personality rights* that use of such services represent. Furthermore this paper provides a comparative analysis of the legal regulation of *personality rights* in the context of cyberspace and new technologies in the Czech Republic, EU, and The United States. This thesis is also exploring the expected changes stemming from current legislative development.

This paper contains case studies that aim to explain the case law and to shift the focus on the aftermath of some of the gravest invasions of privacy of minors while in cyberspace.

This study argues that importance should be given to the protection of *personality rights* through civil law measures and to the interdisciplinary cooperation on the legislative process. This paper provides a list of possible alternatives which might give better legal guarantees, not only to minors using of Web 2.0 and new technologies but to all users.

Klíčová slova / Keywords

Kyberprostor / Cyberspace

Osobnostní práva / Personality Rights

Děti / Children