Univerzita Karlova v Praze
Právnická fakulta
Katedra občanského práva

DIPLOMOVÁ PRÁCE

Ochrana dat na sociálních sítích

Jana Mikšíčková

Vedoucí diplomové práce: JUDr. Petr Šustek, Ph.D.

Praha 2012

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

V Praze dne 26. listopadu 2012

Jana Mikšíčková

Poděkování

Chtěla bych poděkovat manželům Cruickshankovým a prof. Viktoru Mayer-Schönbergerovi, kteří, aniž by si toho byli vědomi, mě inspirovali k napsání tohoto tématu. Děkuji také panu JUDr. Petru Šustkovi, Ph.D., vedoucímu této diplomové práce, za konzultace a cenné připomínky. Dále bych chtěla poděkovat Mgr. Vojtěchu Lagovi za administrativní podporu a jazykové korekce a Mgr. et Mgr. Heleně Hutirové za podnětné připomínky.

Věnováno Miloslavě a Václavovi Mikšíčkovým.

OBSAH

ÚVOD

Internet se v posledních několika dekádách stal jednou z hybných sil společnosti. Umožnil snadný přístup k nesmírnému bohatství informací a sdílení obrovského množství dat bez ohledu na geografickou lokalitu jeho uživatele. Sociální sítě mu pak daly nový rozměr. Poskytly svým uživatelům novou platformu komunikace a neustálý přísun informací o aktivitách druhých. Sociální sítě se v některých případech staly nástrojem revolučních hnutí k organizování demonstrací[1], ale také nástrojem výzvědné služby k sledování podezřelých osob[2] a prostředkem policie k zajištění důkazů v trestním řízení.

Sociální sítě vytvořily určitou iluzi soukromí, kdy jejich uživatelé s nadšením sdílejí mnohdy i své nejintimnější osobní údaje, aniž by si uvědomovali, jaké konsekvence to později může vyvolat. Ať už jde o poškození dobrého jména, ztrátu zaměstnání nebo třeba doživotní zákaz vstupu na území některých států. Sociální sítě se tak staly pozoruhodným fenoménem, který proměnil vnímání soukromí v dnešní moderní informační společnosti.

Téma ochrany dat na sociálních sítích je tak tématem vysoce aktuálním, na němž je fascinující právě to, jak rychle se sociální sítě rozvíjí a přitom zvláštním způsobem mění společnost. Ochrana dat, resp. osobních údajů na sociálních sítích je často diskutovanou otázkou, které se však v českém právním prostředí zatím nedostalo zasloužené pozornosti, což je pravděpodobně z části způsobeno minimem judikatury k této problematice.

Tato práce nám bohužel nedává dostatečný prostor rozebrat právní úpravu ochrany dat[3] na sociálních sítích v celé její šíři a pokrýt v dostatečném rozsahu komplexnost tohoto tématu. Proto se v rámci daného rozsahu soustředíme pouze na ochranu osobních údajů subjektů údajů, tj. fyzických osob, k nimž se tyto údaje vztahují, na sociálních sítích vzhledem k možnostem likvidace osobních údajů, tj. jejich trvalého smazání, jak z fyzického nosiče, databáze správce, resp. zpracovatele, tak z internetového prostředí kde,

[1] Viz tzv. arabské jaro či hnutí Occupy Wall Street. Bližší informace např. PRESTON, Jennifer: *Protesters Look for Ways to Feed the Web*. The New York Times, 24.11.2011 (tištěná verze z 25.11.2011, str. A28). Dostupné na: http://www.nytimes.com/2011/11/25/business/media/occupy-movement-focuses-on-staying-current-on-social-networks.html (25.11.2012); KANELLEY, Craig: *Occupy Wall Street: Social Media's Role In Social Change*. The Huffington Post, 12.06.2011. Dostupné na: http://www.huffingtonpost.com/2011/10/06/occupy-wall-street-social-media_n_999178.html (25.11.2012); O'DONNELL, Catherine: *New study quantifies use of social media in Arab Spring*. New releases, Research, University of Washington, 12.09.2011. Dostupné na: http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/ (25.11.2012).

[2] Viz LEVINE, Danielle: *Facebook and Social Networks: the Government's Newest Playground for Information and the Laws That Haven't Quite Kept Pace*. 33 Hastings Comm. & Ent. L.J. 481, 2010-2011, str. 485.

[3] Pro obecný úvod do ochrany dat a informací v českém právním prostředí zahrnující výklad těchto pojmů, fyzické a právní prostředky ochrany, trestní a správní delikty a smluvní úpravu doporučujeme kapitolu čtvrtou „*Ochrana dat a informací*" v knize ZEMAN, Jiří; MEISNER, Martin: *Základy softwarového práva*. ASPI, 2011.

jak si ukážeme později, se takový úkol ukázal mnohdy nelehkým a komplikovanějším, než se může na první pohled zdát. V tomto ohledu se budeme zabývat pouze dospělými fyzickými osobami jako uživateli sociálních sítí.[4]

V první kapitole této práce se zaměříme v souvislosti s výše uvedeným tématem nejen na současnou českou právní úpravu dané problematiky, ale také na její evropskou úpravu, jako neodmyslitelný pramen práva nejen našeho právního řadu. Nejdříve se podíváme na právo na soukromí, vývoj ochrany osobních údajů, základní principy jejich ochrany a nezbytnou terminologii ochrany osobních údajů. Dále si položíme otázky, co to vlastně jsou sociální sítě a kde se vzaly a zamyslíme se nad otázkou soukromí na sociálních sítích. Na tento základ navážeme rozsáhlejší kapitolou právního rámce ochrany, jež představuje jádro této diplomové práce. Kapitolu právní rámec ochrany tvoří problematika teritoriality a aplikovatelnosti práva, právní vztah poskytovatele služby sociální sítě a uživatele a především likvidace dat a právní prostředky ochrany. Cílem první kapitoly je popsat stávající právní úpravu a poukázat na některé její nedostatky.

V neposlední řadě také nemůžeme opomenout přípravu nové právní úpravy na úrovni EU, jež má harmonizovat právní úpravy ochrany osobních údajů všech členských států EU a odstranit nedostatky dnešní zastaralé právní úpravy. Předmětem této reformy, kterou analyzujeme v druhé kapitole, je návrh nového nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem takových údajů (Obecné nařízení o ochraně údajů) a návrh směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů. V této práci se budeme zabývat pouze připravovaným Obecným nařízením o ochraně údajů v rozsahu potřebném pro účely této práce. Podíváme se na důvody pro přijetí nové úpravy, obsah předloženého návrhu nařízení a na reakce, které tento návrh vyvolal.

Při zpracování tohoto tématu byly použity metody deskriptivní a analytické, spolu s indukcí, dedukcí, syntézou a komparací (především české a evropské úpravy spolu s předloženým návrhem nařízení).

Právní stav ke dni 26. listopadu 2012.

[4] Působení právnických osob a dětí jako uživatelů sociálních sítí je sice tématem vhodným k dalšímu zpracování, zde však pro něj není prostor. Stejně tak se vzhledem k rozsahu této práce nebudeme zabývat ochranou osobních údajů v souvisloti s používáním softwarových aplikací na sociálních sítích.

Kapitola 1.
Současná právní úprava ochrany dat na sociálních sítích v České republice a Evropské unii

V této kapitole se zaměříme na současnou právní úpravu ochrany dat (osobních údajů) na sociálních sítích v České republice v kontextu evropského práva, především příslušných evropských směrnic, které byly do českého práva implementovány. Nejprve se podíváme na právo na soukromí a jeho právní zakotvení. Dále se budeme zabývat vývojem ochrany osobních údajů v českém právu v souvislosti s vývojem evropským, který české právo nemalou měrou ovlivnil a do značné míry předurčil jeho další vývoj. Následně nastíníme základní principy ochrany osobních údajů jak v České republice, tak na evropské úrovni. Poté si vyjasníme základní pojmy ochrany osobních údajů, pojem a vývoj sociálních sítí a zamyslíme se nad otázkou soukromí na sociálních sítích. Na to tento základ navážeme rozsáhlejší kapitolou právního rámce ochrany, která tvoří klíčovou kapitolu této části diplomové práce a zároveň jádro této diplomové práce. V právním rámci ochrany představíme teritorialitu a aplikovatelné právo, právní vztah poskytovatele služby sociální sítě a uživatele a především likvidaci dat a právní prostředky ochrany.

1.1. Právo na soukromí

Právo na soukromí je jedním je základních práv člověka a občana. Ačkoli tento právní institut nikdy nebyl přesně definován[5], obecně se za právo na soukromí považuje „*právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem, mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob*".[6] Přílišná akcentace pozitivní složky práva na ochranu soukromého života však dle Ústavního soudu vede k neadekvátnímu zúžení takové ochrany.[7]

[5] Jeho definování je věčným právně-filozofickým problémem, proto jeho vyčerpávající definici nenajdeme ani v mezinárodních úmluvách ani v právních předpisech či judikatuře. Právo na soukromí se neustále vyvíjí v závislosti na jeho společenském vnímání. Pro zajímavé úvahy o právu na soukromí v dnešní společnosti viz např. sborník z konference „Právo na soukromí" uspořádaný Vojtěchem Šimíčkem: *Právo na soukromí*, MUNI Press, Brno 2011.
[6] Judikát II. ÚS 517/99 ze dne 1. března 2000.
[7] Tamtéž.

Právo na soukromí je na mezinárodní úrovni zakotveno ve Všeobecné deklaraci lidských práv[8], kde se v čl. 12 praví „*nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům*". Tento pojem byl dále rozpracován v Úmluvě o ochraně lidských práv a základních svobod[9], která stanovila výjimky, kdy je možné do tohoto práva zasáhnout (zásah státním orgánem je přípustný pouze v souladu se zákonem, je-li to nutné k ochraně národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných). Na ně poté navázal Mezinárodní pakt o občanských a politických právech[10].

Tato úprava pak byla přijata do Listiny základních práv a svobod (Listina)[11], kde se v čl. 7 zaručuje nedotknutelnost osoby a jejího soukromí, přičemž omezit soukromí lze pouze, stanoví-li to zákon[12]. Listina právo na soukromí upravuje poměrně komplexně, kdy v dalších článcích rozvádí jeho jednotlivé oblasti. Dále se zaměříme zejména na její čl. 10, který každému zaručuje ochranu lidské důstojnosti, osobní cti, jména, dobré pověsti, ochranu před neoprávněným zasahováním do soukromého a rodinného života a před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Na právní úpravu obsaženou v Listině navazují a konkretizují ji ustanovení občanského zákoníku[13] upravující ochranu osobnosti. V jeho § 11 je mimo jiné uvedeno právo každé fyzické osoby na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. Právní prostředky ochrany upravuje § 13, podle nějž má fyzická osoba právo se domáhat, aby bylo upuštěno od neoprávněných zásahů do práva na ochranu její osobnosti, aby byly odstraněny následky těchto zásahů a aby jí bylo dáno přiměřené zadostiučinění. Nepostačovalo-li by zadostiučinění zejména proto, že byla ve značné míře snížena důstojnost fyzické osoby nebo její vážnost ve společnosti, má fyzická osoba rovněž právo

---

[8] Všeobecná deklarace lidských práv byl přijata 10. prosince 1948 Organizací spojených národů.
[9] Úmluva Rady Evropy o ochraně lidských práv a základních svobod dojednaná v Římě dne 4. listopadu 1950 (ČSFR k ní přistoupila 21. února 1991 s účinností od 18. března 1992).
[10] Pakt OSN z New Yorku ze dne 19. prosince 1966. Dne 23. března 1976 vstoupil v platnost pro tehdejší ČSSR.
[11] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
[12] Neboť jak říká čl. 2 odst. 4 Ústavy České republiky, zákona č. 1/1993 Sb., ve znění pozdějších předpisů: „*Každý občan může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.*" Právo na soukromí je tak jako jedno ze základních práv pod ochranou soudní moci (čl. 4 tamtéž).
[13] Občanský zákoník, zákon č. 40/1964 Sb., ve znění pozdějších předpisů.

na náhradu nemajetkové újmy v penězích. Odpovědnost za škodu způsobenou zásahem do práva na ochranu osobnosti by se řídila ustanoveními o odpovědnosti za škodu.

Jako *lex specialis* vůči Listině a občanskému zákoníku stojí zákon o ochraně osobních údajů (ZoOÚ)[14], z jehož § 1 jasně vyplývá, že hranice ochrany osobních údajů stanoví právě právo na ochranu soukromí. Ustanovení § 10 ZoOÚ je pak zřejmým provedením základního práva na soukromí a přenáší jej do oboru práva správního jako jednoznačně vyjádřenou povinnost, stejně tak jako toto právo, resp. jeho garanci a ochranu, zasazuje do soukromého práva ustanovení § 11 a násl. občanského zákoníku.[15]

1.2. Vývoj ochrany osobních údajů

Ochrana osobních údajů je relativně novým fenoménem. O potřebě vytvoření právní ochrany osobních údajů se začalo uvažovat už po II. světové válce, mimo jiné také v souvislosti se zneužitím matričních osobních údajů dokládajících náboženskou příslušnost Židů nacistickým režimem k jejich identifikaci a následnému vyhlazování.

Později s rozšiřováním a zdokonalováním výpočetní techniky umožnující sofistikovanější sběr, zpracování a následné uchování dat, začaly vznikat první právní normy upravující tento nový fenomén. Od 70. let 20. století se tak postupně začaly objevovat první zvláštní právní předpisy upravující ochranu osobních údajů na úrovni jednotlivých států[16]. Prvním mezinárodním pramenem, který poprvé definoval a systematicky upravil principy ochrany osobních údajů, se však stala až Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108 (Úmluva č. 108)[17] z roku 1981 a její Dodatkový protokol[18]. Úmluva č. 108 stanovila základní pojmy a zásady ochrany a upravila tok údajů přes hranice a spolupráci mezi jejími smluvními stranami. Účelem Úmluvy č. 108 je dle jejího prvního článku zaručit na území

---

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

[15] BARTÍK, Václav; JANEČKOVÁ, Eva: *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8. 2012*. 1. vydání. ANAG, Olomouc 2012, str. 32.

[16] Např. švédský *Datalag* (1973), německý federální *Bundesdatenschutzgesetz* (1977) nebo francouzský *Loi relative à l'informatique, aux fichiers et aux libertés modifiée* (1978).

[17] V originále: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Přijata Radou Evropy ve francouzském Štrasburku dne 28. ledna 1981. Platila od 1. října 1985, přičemž pro ČR vstoupila v platnost až od 1. listopadu 2001, kdy byla publikována pod č. 115/2001 Sb.m.s.

[18] Sdělení č. 29/2005 Sb.m.s. Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku přes hranice. Zveřejněno v č. 15/2005 Sb.m.s. na str. 363.

každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují.

Na Úmluvu č. 108 pak reagoval český zákon o ochraně osobních údajů v informačních systémech z roku 1992[19]. Jeho praktické využití však bylo sporné vzhledem k tomu, že tehdy ještě neexistoval orgán, který by kontroloval jeho dodržování.

Na úrovni Evropské unie pak byla v roce 1995 přijata směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES (Směrnice 95/46/ES) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů[20], která se stala na úrovni EU základním pramenem ochrany osobních údajů. Úkolem Směrnice 95/46/ES je harmonizace právní úpravy členských států v oblasti ochrany základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů; přičemž Směrnice 95/46/ES neumožňuje členským státům omezit nebo zákazat pohyb těchto údajů mezi členskými státy z důvodu této ochrany. Směrnice 95/46/ES vymezuje základní pojmy a zásady, oblast působnosti, obecné podmínky pro zákonnost zpracování osobních údajů, soudní přezkum, odpovědnost a sankce, předávání osobních údajů do třetích zemí a povinnost každého členského státu zřídit na svém území alespoň jeden nezávislý veřejnoprávní orgán dozoru nad takto přijatými předpisy. Tato Směrnice 95/46/ES je v rámci EU dodnes jedním z nejvýznamnějších právních předpisů upravujících ochranu osobních údajů, avšak vzhledem k rapidnímu rozvoji informační společnosti je stále více zpochybňována její aktuálnost.

Reakcí na Směrnici 95/46/ES byl pak v rámci přístupových jednání ČR k EU přijat roku 2000 dnešní zákon o ochraně osobních údajů (ZoOÚ)[21], jehož účelem je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí. Tento zákon upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států. Poskytuje tak obecný rámec pro ochranu osobních údajů a zároveň zřizuje Úřad pro ochranu osobních údajů se sídlem

[19] Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů. Účinný od 1. června 1992.

[20] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. V originále: *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[21] Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, ze dne 4.dubna 2000, který nabyl účinnosti dne 1. června 2000, s výjimkou jeho ustanovení § 16, 17 a 35, jež nabyla účinnosti 1. prosince 2000.

v Praze, jehož úkolem je dohled nad dodržováním právních předpisů v oblasti ochrany osobních údajů. Spolu s výše uvedenou Směrnicí 95/46/ES je tak ZoOÚ základním pilířem právní ochrany osobních údajů v našem právním řádu.

Dále v roce 1997 následovala směrnice 97/66/ES o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru[22] (modifikující dřívější směrnici 95/46/ES pro oblast telekomunikací), kterou reflektuje český zákon o telekomunikacích[23]. Tato směrnice byla roku 2002 nahrazena směrnicí 2002/58/ES o zpracování osobních údajů a ochraně soukromí v oblasti elektronických komunikací (Směrnice 2002/58/ES)[24]. Tato směrnice pak byla novelizována směrnicí 2006/24/ES o ochraně osobních údajů v oblasti elektronických komunikací (Směrnice 2006/24/ES)[25]. Značná důležitost se tu přikládá zejména tzv. Article 29 Working Party, což je zvláštní poradní orgán Evropské komise pro oficiální výklad ochrany osobních údajů.

Na závěr bychom neměli bychom opomenout Chartu základních práv EU[26], která se prostřednictvím Lisabonské smlouvy stala součástí primárního práva EU. Zakotvuje zejména principy obsažené v judikatuře Evropského soudního dvora a vycházející mimo jiné z Úmluvy Rady Evropy o ochraně lidských práv a základních svobod z roku 1950. Obsahuje jak právo na respektování soukromého a rodinného života, obydlí a komunikace, tak i právo na ochranu osobních údajů. Ve svém čl. 8 zaručuje každému právo na ochranu údajů, které se ho týkají. Údaje mají být zpracovány poctivě, pro vymezené účely a na základě souhlasu dotčené osoby nebo na jiném legitimním základě stanovené zákonem. Zahrnuje také právo každého na přístup k údajům, které byly v souvislosti s jeho osobou shromážděny a právo na jejich opravu.

---

[22] Směrnice Evropského parlamentu a Rady 97/66/ES o zpracování osobních údajů a ochraně soukromí v sektoru telekominikací ze dne 15. prosince 1997. V originále: *Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector*.

[23] Zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů.

[24] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronických komunikací. V originále: *Directive on privacy and electronic communications*.

[25] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES. V originále: *Data Protection in Electronic Communications Directive*. K této směrnici kriticky viz VANÍČEK, Zdeněk: *Směrnice o uchování údajů (Nástroj ochrany veřejného zájmu nebo zasahování do soukromí?)*, Právní zpravodaj č. 6/2006, str. 14.

[26] Charta Evropského parlamentu, Rady a Komise byla vyhlášena na Mezivládní konference v Nice dne 7. prosince 2000.

1.3. Principy ochrany osobních údajů

Principy ochrany osobních údajů byly poprvé systematicky upraveny a definovány v Úmluvě č. 108 a jejím Dodatkovém protokolu[27]. Tyto principy jsou všeobecně používány v oblasti ochrany osobních dajů a každá zásada má určitý svůj „obraz" v zákoně či jiném právním předpisu státu, který tuto Úmluvu ratifikoval.[28] Nejinak tomu je také v českém právním řádu, který tyto zásady reflektuje prostřednictvím Směrnice 95/46/ES a ZoOÚ. Jedná se o následující zásady:

❖ Zásada legitimity zpracování[29]

Zásada legitimity zpracování vyžaduje, aby osobní údaje, které jsou předmětem automatizovaného zpracování, byly získány a zpracovány poctivě a v souladu se zákony, přičemž musí být samozřejmě dodrženy základní svobody a práva osob, jichž se osobní údaje týkají, tj. především právo na soukromí.

❖ Zásada omezení účelem (nezbytnosti)[30]

Podle zásady omezení účelem (resp. zásady nezbytnosti) musí být osobní údaje shromažďovány pro stanovené a oprávněné účely, tzn. účely výslovně vyjádřené a legitimní (tj. v souladu s domácím právním řádem). Osobních údajů přitom nesmí být použito způsobem neslučitelným s těmito účely.

❖ Zásada časového omezení[31]

Osobní údaje musí být dle zásady časového omezení uchovány ve formě umožňující zjistit totožnost subjektů údajů pouze po dobu nezbytně nutnou pro naplnění účelu, pro něž jsou údaje shromážděny. Pro určení doby se bude vždy vycházet z konkrétních okolností případu.

---

[27] Viz kapitola 1.2.
[28] Viz MATES, Pavel; JANEČKOVÁ, Eva; BARTÍK, Václav: *Ochrana osobních údajů*. Leges, Praha 2012, str. 9-28.
[29] Čl. 5 písm. a) Úmluvy č. 108. Rovněž čl. 6 odst. 1 písm. a) Směrnice 95/46/ES. Dále také § 5 odst. 1 písm. c) věta první a § 5 odst. 3 ZoOÚ.
[30] Čl.5 písm.b) Úmluvy č. 108. Rovněž čl. 6 odst. 1 písm. b) Směrnice 95/46/ES. Dále § 5 odst. 1 písm. d), g) ZoOÚ.
[31] Čl.5 písm.e) Úmluvy č. 108. Rovněž čl. 6 odst. 1 písm. e) Směrnice 95/46/ES. Dále § 5 odst. 1 písm. e) ZoOÚ.

❖ Zásada potřebnosti a přiměřenosti (proporcionality) dat[32]

Požadavkem zásady potřebnosti a přiměřenosti (resp. proporcionality) dat je, aby osobní údaje byly přiměřené, týkající se účelů, pro něž byly uloženy na nosiče, a nepřesahující tyto účely. Ukáže-li se v některé následné fázi zpracování, že některé osobní údaje již nejsou dále nezbytné, měly by být, pokud je to technicky možné, vymazány z paměťových nosičů.[33]

❖ Zásada průhlednosti[34]

Dle zásady průhlednosti musí být každé osobě umožněno zjistit existenci automatizovaného souboru osobních údajů a získávat v přiměřených intervalech a bez příslušných průtahů nebo nákladů potvrzení o tom, zda jsou v automatizovaných souborech dat uloženy osobní údaje, které se jí týkají, jakož i sdělit jí tyto údaje ve srozumitelné formě. Tato zásada tak klade důraz na plnou a průběžnou informovanost subjektu údajů o všech údajích, které se ho týkají.

❖ Zásada bezpečnosti[35]

Zásada bezpečnosti vyžaduje vhodná bezpečnostní opatření na ochranu osobních údajů uložených v automatizovaných souborech dat proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, jakož i proti neoprávněnému přístupu, změnám nebo šíření. Je tak nutné přijmout přiměřená a dostupná technická, organizační a personální opatření, aby nedošlo k těmto rizikům[36], přičemž tato bezpečnostní opatření mají být přiměřená charakteru zpracovaných osobních údajů a poskytnout tak účinnou ochranu.[37]

---

[32] Čl.5 písm.c) Úmluvy č. 108. Rovněž čl. 6 odst. 1 písm. c) Směrnice 95/46/ES, kde směrnice ještě doplňuje „musí být podstatné". Dále § 5 odst. 1 písm. d), f) ZoOÚ.
[33] KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2003, str. 332 a násl.
[34] Čl.8 písm.a), b) Úmluvy č. 108. Podrobněji v čl. 12 písm. a) Směrnice 95/46/ES a v § 5 odst. 4, § 11 ZoOÚ.
[35] Čl.7 Úmluvy č. 108. Rovněž čl. 17 Směrnice 95/46/ES. Dále § 13 ZoOÚ.
[36] KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2003, str. 332 a násl.
[37] BARTÍK, Václav; JANEČKOVÁ, Eva: *Ochrana osobních údajů v aplikační praxi*. Linde Praha, 2010, str. 159.

❖ Zásada práva přístupu k datům[38]

Zásada práva přístupu k datům spočívá v právu přístupu subjektu údajů ke svým osobním údajům a je obdobná zásadě o průhlednosti (viz výše) s tím, že toto právo může být omezeno pouze na základě zákona, je-li pro to dán zvláštní zájem státu.[39] Toto právo se uplatní také při předávání dat do zahraničí.

❖ Zásada práva na opravu a výmaz[40]

Osobní údaje musí být podle zásady práva na opravu a výmaz přesné a pokud je to potřebné, udržované v aktuálním stavu. Každému má být umožněno docílit, podle povahy případu, opravu těchto údajů nebo jejich vymazání, jestliže byly zpracovány v rozporu s vnitrostátním právním řádem uplatňujícím základní zásady Úmluvy č. 108.

❖ Zásada nezávislého dozoru[41]

V souladu se zásadou nezávislého dozoru je každá smluvní strana Úmluvy č. 108 povinna zřídit na svém území alespoň jeden nezávislý orgán dozoru nad dodržováním příslušných předpisů a opatření, která jsou předmětem Úmluvy č. 108. Dále stanoví pravomoci takového orgánu s tím, že jeho rozhodnutí je možné napadnout stížností a je přezkoumatelné u soudu.

1.4. Základní pojmy ochrany osobních údajů

Než můžeme pokračovat s hlubší analýzou ochrany osobních údajů na sociálních sítích, je třeba si nejprve definovat základní pojmy ochrany osobních údajů. Česká terminologie byla v tomto ohledu s drobnými odchylkami převzata ze Směrnice 95/46/ES do ZoOÚ.

---

[38] Čl. 8 písm. b) Úmluvy č. 108. Rovněž čl. 12 písm. a) Směrnice 95/46/ES. Dále § 12 ZoOÚ.
[39] Pro příklady viz MATES, Pavel; JANEČKOVÁ, Eva; BARTÍK, Václav: *Ochrana osobních údajů*. Leges, Praha 2012, str. 22.
[40] Čl. 5 písm.d), čl. 8 písm. c) Úmluvy č. 108. Čl. 6 odst. 1 písm. d), čl. 12 písm. b) Směrnice 95/46/ES. Dále § 5 odst. 1 písm. c), § 21 ZoOÚ.
[41] Čl. 1 Dodatkového protokolu. Obdobně čl. 28 Směrnice 95/46/ES. Provedeno v § 2, hlava IV-VI ZoOÚ.

❖ Osobní údaj

Klíčovým pojmem je *osobní údaj*. Dle ZoOÚ je to *„jakákoli informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu"*.[42]

Za těchto podmínek tak osobním údajem může být v podstatě jakákoli informace, bez ohledu na její přesnost, pravdivost nebo objektivnost. Podstatným znakem je pouze určitelnost osoby na základě takového údaje. Osobní údajem tedy může být jak jméno, příjmení, kontaktní údaje, rodné číslo nebo jiné číselné označení osoby, tak například její biometrický údaj[43] či IP adresa[44]. Proto při aplikaci zákona v praxi osobní údaj vždy vyjadřuje vztah mezi reálnou fyzickou osobou a určitou hodnotou údaje.[45] Samozřejmě musíme vzít v potaz, že čím více osobních údajů o určitém subjektu údajů správce (definice viz níže) nashromáždí, tím větší vypovídající hodnotu osobní údaje mají jako celek.

Stanovit přesnou hranici pojmu osobního údaje je přesto úkolem nelehkým, ne-li nemožným. Příkladem toho je rozlišení osobního údaje a projevu osobní povahy[46]. Oba pojmy jsou součástí práva na ochranu osobnosti[47] a navzájem se prolínají. Pro posouzení právních prostředků ochrany bude ale jejich rozlišení klíčové. Podle povahy a míry zásahu do soukromí a způsobu užití takových informací se odliší, zda využít veřejnoprávní prostředky ochrany (jde-li o osobní údaj), nebo zda-li se uplatní ochrana soukromoprávní (občanskoprávní žaloba na ochranu osobnosti u projevu osobní povahy), přičemž se tyto právní prostředky ochrany navzájem nevylučují.[48]

❖ Citlivý údaj

Citlivý údaj je speciální podkategorií osobního údaje. Je to „*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě*

---

[42] § 4 písm. a) ZoOÚ.
[43] Jako např. otisk prstu, struktura sítnice, struktura obličeje, hlas apod. Blíže viz BARTÍK, Václav; JANEČKOVÁ, Eva: *Zákon o ochraně osobních údajů s komentářem*. 1. vydání. ANAG, Olomouc 2010, str. 40 - 41.
[44] Viz rozhodnutí Soudního dvora Evropských společenství zn. C-275/06 ze dne 29. ledna 2008; rozsudek Nejvyššího správního soudu sp. zn. 1 As 90/2008-189 ze dne 4. února 2009.
[45] MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav: *Osobní údaje a jejich ochrana*. 2. vydání. ASPI-Wolters Kluwer, str. 18 – 19.
[46] § 11 ObčZ a § 81 odst. 2 nového občanského zákoníku (Nový ObčZ), zákona č. 89/2012 Sb.
[47] Zakotveno v čl. 10 LZPS.
[48] Viz KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2012, str. 51.

subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů".[49] Citlivý údaj tak musí splňovat kritéria osobního údaje, ale vzhledem k větší míře zásahu do soukromí je u něj vyžadován přísnější režim pro jeho zpracování (viz § 9 ZoOÚ).

Citlivé údaje však nejsou pouze doménou ZoOÚ. Český právní řád tyto zvláštní skupiny údajů aproboval nejen do ZoOÚ, ale i do jiných právních předpisů[50]. V některých případech je rozšířil i o další kategorie, které jsou významově blízké a řadě lidí splývají[51]

❖ Anonymní údaj

Významovým protikladem osobního údaje je anonymní údaj, což je „*takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů*"[52]. Zde musíme rozlišit pojmy *anonymní* a *anonymizovaný* údaj. Z anonymního údaje byl subjekt údajů od počátku neurčitelný, zatímco z anonymizovaného se neurčitelným stal terpve dodatečně (např. pro účely statistiky). Je třeba upozornit, že anonymní ani anonymizované údaje nejsou osobními údaji, a proto se na ně jako takové nevztahuje ZoOÚ.

❖ Subjekt údajů

Subjekt údajů je „*fyzická osoba, k níž se osobní údaje vztahují*"[53]. Subjektem údajů je tak člověk od narození (včetně nascitura, tedy počatého dítěte, narodí-li se živé) do smrti[54], včetně podnikajících fyzických osob[55].

❖ Správce

Správce je spolu se subjektem klíčovou postavou celé ochrany osobních údajů. Správcem je „*každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může zmocnit nebo pověřit zpracovatele, pokud*

---

[49] § 4 písm. b) ZoOÚ.
[50] Např. do § 2 odst. 3 antidiskrimančního zákona, z. č. 198/2009 Sb., ve znění pozdějších předpisů.
[51] BARTÍK, Václav; JANEČKOVÁ, Eva: *Zákon o ochraně osobních údajů s komentářem*. 1. vydání. ANAG, Olomouc 2010, str. 37 a násl.
[52] § 4 písm. c) ZoOÚ.
[53] § 4 písm. d) ZoOÚ.
[54] Avšak dle názoru Úřadu smrtí pozbývají platnosti jen ta ustanovení ZoOÚ, v nichž subjekt vystupuje jako účastník občanskoprávních vztahů (viz Úřad k problémům z praxe č. 7/2002 Sb.).
[55] K této otázce blíže viz KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2012, str. 66-68.

zvláštní zákon nestanoví jinak".[56] Správcem tak může být v podstatě kdokoli – jak osoba fyzická, tak právnická, subjekt soukromého či veřejného práva. Pro určení toho, zda je určitá osoba správcem, je podstatná její faktická činnost z hlediska naplňování zákonných kritérií, nikoliv její povaha či právní subjektivita.[57]

❖ Zpracovatel

Zpracovatelem je *„každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle ZoOÚ"*.[58] Zpracovatel je tedy vždy odlišná osoba od správce, která pro správce zpracovává data na základě dohody nebo zákonného pověření a to v souladu s pokyny správce a právními předpisy.

❖ Zpracování osobních údajů

Zpracováním osobních údajů se rozumí *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobích údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace."*[59] Zpracování osobních údajů je jednou z nejdůležitějších legálních definic ZoOÚ, která vymezuje rozsah zákonných práv a povinností, na něž se bude ZoOÚ aplikovat.[60] Aby byla naplněna definice zpracování, je třeba naplnit dvě podmínky: (i) jedná se o operaci (úkon) nebo soustavu operací a (ii) operace musí být systematická. V porovnání se Směrnicií 95/46/ES je „systematičnost" operace vyžadována pouze ZoOÚ, zatímco ve Směrnici 95/46/ES se tento pojem nevyskytuje. Výčet operací je demonstrativní, proto je při posuzování zpracování třeba vycházet z úmyslu správce, resp. zpracovatele, při shromažďování a následném nakládání s osobními údaji.

---

[56] § 4 písm. j) ZoOÚ.
[57] KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2012, str. 78.
[58] § 4 písm. k) ZoOÚ.
[59] § 4 písm. e ZoOÚ.
[60] Viz § 1 ZoOÚ, kde je vymezen předmět úpravy: „*Tento zákon (...) upravuje práva a povinnosti při zpracování osobních údajů a (...)*".

1.5. Pojem a vývoj sociálních sítí

Co to vlastně je sociální síť (SNS)? Ačkoli neexistuje žádná oficiální definice sociální sítě, najdeme celou řadu[61] definic, které se více či méně liší. Obecně můžeme říci, že sociální síť je platforma vyžadující určitý software a služby internetu, kdy se vytváří komunita lidí sdílejících společné zájmy nebo jiné aktivity, kde si uživatelé sítě vytváří svůj osobní profil, jehož prostřednictvím jim je umožněno komunikovat s ostatními členy komunity a sdílet s nimi určitý obsah.

Aby se uživatel mohl stát aktivním členem takové komunity, musí si založit svůj osobní profil. Některé sociální sítě[62] však umožňují i nezaregistrovaným uživatelům pasivní přístup, tzn. jestliže to uživatelé a správce sítě povolí, pasivní uživatel si může prohlížet profily zaregistrovaných uživatelů, číst jejich komentáře nebo se jinak informovat o jejich aktivitách. Pro vytvoření osobního profilu správce sítě obvykle vyžaduje uživatelovo jméno, příjmení, přezdívku, email, dále v závislosti na konkrétní sociální síti uživatel může sdílet také datum narození, adresu, telefon, zaměstnání, dosažné vzdělání, jazykové schopnosti, místo narození, národnost, politické, náboženské či jiné přesvědčení, osobní status, fotografie, zájmy či oblíbené knihy, filmy, hudbu, odkazy na internetové články, videa apod. Tak jako existuje nepřeberné množství sociálních sítí[63], existuje také neomezený okruh dat a informací, které lze na sociálních sítích sdílet. Závisí na každém uživateli, co vše a s jak velkým okruhem uživatelů je ochoten sdílet, tj. veřejně publikovat na sociální síti.

Jak vidíme, model sociálních sítích je tedy založen na sdílení. Čím větší množství uživatelů a sdílených dat, tím se stává sociální síť zajímavější pro nové uživatele[64]. Ekonomové tento jev nazývají „externality sítě" – každý další nový uživatel vstupující na

---

[61] Např. EDWARDS, Lilian; BROWN, Ian: *Data Control and Social Networking: Irreconcilable Ideas?*; Oxford Advanced Learner´s Dictionary, 8th edition, Oxford University Press 2010, str. 1464; či hojně citovaná Wikipedie - pro srovnání: http://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5, http://en.wikipedia.org/wiki/Social_network, http://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet) (11.11.2012).

[62] Typickým příkladem je Facebook nebo LinkedIn.

[63] Pro některé příklady sociálních sítí – viz např. http://www.socialnisite.123abc.cz/ (11.11.2012).

[64] Jak řekl Richardu Lane Greenovi pro článek *Facebook: Líbí se Vám?* Andrew Bosworth, jeden z ředitelů Facebooku: „*Na Facebooku nejste proto, že my jsme úžasní. Na Facebooku jste proto, že úžasní jsou vaši přátelé. Dělají zajímavé věci a vy se o tom chcete dozvědět. Pokud si uvědomujete, že jste právě na Facebooku, zřejmě jsme někde udělali chybu.*" Respekt, edice Fenomén, *Svět technologických novinek*, ve spolupráci s The Economist, vydavatelství Economia, 21.05.2012.

síť, aby sdílel informace, zvyšuje hodnotu sítě pro všechny stávající uživatele.[65] Dalo by se tak říci, že v určitém smyslu fungují sociální sítě jako stále se nabalující sněhová koule. K úspěšné (tzn. „oblíbené“)[66] sociální síti se tak přidává stále více uživatelů a správce je motivován neustále rozšiřovat a vylepšovat služby sítě poskytované uživatelům o nové aplikace. Správce sítě, který neustále neinovuje a nejde s moderními trendy, časem ztratí zájem uživatelů a v důsledku toho zanikne (viz případ MySpace.com). Čím je sociální síť úspěšnější, tím více přiláká investorů, kteří zde umístí svoji reklamu zaměřenou na jednotlivé cílové skupiny podle jejich zájmů a aktivit uveřejněných na síti. Obchodní model sociálních sítí je tak založen na tzv. behaviorálním marketingu[67]. Dalším pozoruhodným jevem je, že jakmile se taková sociální síť stane úspěšnou a doroste do gigantických rozměrů, ostatní její potencionální konkurenti na trhu s ní přestávají soutěžit a radši se s ní spojí.[68]

Sociální sítě jsou konceptem starším, než by se na první pohled mohlo mnohým jejich uživatelům zdát. Za první sociální síť bývá považován systém CBBS[69] vytvořený počítačovými nadšenci roku 1978, kde uživatelé mohli posílat oznámení a plánovat setkání se svými přáteli. Interakce mezi uživateli však byla vzhledem k tehdejšímu technologickému vývoji značně omezena. Ještě předtím než se dostal internet do povědomí široké veřejnosti, vznikla v 70. letech 20. století služba CompuServe umožňující svým uživatelům interakci prostřednictvím sdílení souborů, událostí, diskusních fór či posílání soukromých zpráv. V 80. letech pak za průkopníka sociálních sítí můžeme označit službu AOL, která svým uživatelům mimo jiné umožnila vytvořit si osobní profily s osobními údaji.

Pravý boom sociálních sítí však nastal až v 90. letech v souvislosti s rozšířením počítačů a internetu do domácností běžných uživatelů a také v návaznosti na zpřístupnění

---

[65] Tuto myšlenku dále rozvíjí Viktor Mayer-Schönberger ve své knize *Delete – The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, str. 85 a násl.

[66] Úspěšnost sociální sítě se obecně posuzuje podle množství jejích uživatelů a jejich dlouhodobého přírůstku, včetně času, který zde denně uživatelé stráví.

[67] Prezentace prof. Andrease Wiebe na téma *Privacy in the Workplace - Data Protection in Social Networks* z mezinárodní konference na maďarské Univerzitě v Pecsi, 2.-3. dubna 2012. Dostupné na: http://pawproject.eu/en/sites/default/files/page/15_wiebe_dpsn.pdf (10.11.2012). Pro více informací o reklamě na SNS viz článek Petra Otevřela: *Sociální sítě z pohledu firmy: Co můžete a co ne?* Právní rádce č. 10/2012, Economia 2012.

[68] „*Facebook je internet uvnitř internetu. Je natolik dominantní, že jak samotný Facebook, tak ostatní technologické společnosti přicházejí k poznání, že je mnohem snadnější spojit síly než mezi sebou bojovat.*“ In GREEN, Richard Lane: *Facebook: Líbí se Vám?,* Respekt, edice Fenomén, *Svět technologických novinek*, ve spolupráci s The Economist, vydavatelství Economia, 21.05.2012, str. 18.

[69] Digitalizovaný bulletin založený na systému nástěnky (v originále „*computerized bulletin board system*“) vytvořený Wardem Christensenem a Randy Suess z amerického Chicaga.

technologie www široké veřejnosti. Tak začala éra sociálních sítí Classmates, GeoCities, SixDegrees, blogování či sociální sítě Friends Reunited. Počet uživatelů rapidně rostl.

S novým miléniem bylo k internetu připojeno už téměr 361.000.000 uživatelů internetu[70]. Vznikla sociální síť Friendster, která během prvních tří měsíců překonala hranici tří milionů uživatelů. Později vzniká profesně zaměřená sociální síť LinkedIn (dnes má přes 175 milionů uživatelů) a také sociální síť MySpace, až do roku 2008 jedna z nejpopulárnějších sociálních sítí umožňující sdílet mimo jiné videa a fotografie svých uživatelů. MySpace se však ke své škodě neřídil heslem „inovuj nebo zemři"[71] a stal se tak „dinosaurem" mezi sociálními sítěmi. Jeho uživatelé přešli k jeho mladšímu konkurentovi Facebooku, vytvořeném Markem Zuckerbergem v harvardském kampusu roku 2004, a MySpace tak ztratil svou hodnotu. Facebook se otevřel roku 2006 veřejnosti a stal se jednou z nejnavštěvovanějších světových sociálních sítí (uvádí se, že již dosáhl jedné miliardy uživatelů[72]). Po Facebooku byly velmi úspěšně uvedeny na trh také sociální sítě Twitter a nejnovější Google+.[73]

Sociální sítě se tak postupně staly všudypřítomným kulturním fenoménem; pro mnoho uživatelů také jejich součástí každodenní reality. Význam sociálních sítí s neustále rostoucím počtem uživatelů sílí a přesahuje prostředí internetu. Sociální sítě mimo jiné přispěly a svým způsobem posloužily jako nástroj k urychlení proměny společnosti, jak se ukázalo při svolávání protestů v rámci arabského jara[74]. V mnoha zemích jsou jediným veřejným médiem svobodného vyjádření.

---

[70] Zdroj: http://www.internetworldstats.com/stats.htm (14.11.2012). Pro srovnání: k dnešnímu dni by k internetu mělo být připojeno přes 2.405.000.000 uživatelů, což představuje přes 34% dnešní světové populace. Od roku 2000 je to tedy nárůst o více než 566% uživatelů.

[71] Tento citát (v originále „*innovate or die*") se připisuje Damonu Darlinovi v článku *Innovate or Die on the Net* z roku 1996. Dalo by se říci, že tímto heslem se mimo jiné řídí také dnešní Silicon Valley.

[72] Ovšem v souvislosti s uváděným počtem uživatelů si musíme vždy uvědomit, že někteří uživatelé mohou mít v rámce jedné SNS více než jeden osobní profil (často pod fiktivními jmény).

[73] O vývoji sociálních sítí detailněji viz http://www.digitaltrends.com/features/the-history-of-social-networking/, http://wiki.aktualne.centrum.cz/datarama/socialni-site/, graf http://edudemic.com/wp-content/uploads/2012/03/history-of-social-networks.pdf, http://socialtimes.com/the-history-of-social-media-from-1978-2012-infographic_b89811, chronologicky http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html (14.11.2012).

[74] Blíže viz např. http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/ nebo http://www.newscientist.com/article/mg21428596.400-was-the-arab-spring-really-a-facebook-revolution.html (14.11.2012).

1.6. Otázka soukromí na sociálních sítích

Otázka soukromí a určení jeho hranic vždy zrcadlila jeho vnímání ve společnosti. Nejinak tomu je i v současnosti, kdy zejména v posledních letech v souvislosti s rozvojem informační společnosti dochází k přehodnocení samotného pojmu soukromí a jeho pomyslných hranic. Dříve jsme sdíleli informace z našeho soukromí pouze s okruhem našich nejbližších. Dnes díky internetu a sociálním sítím stejné informace sdílíme s nesrovnatelně větším okruhem osob, které tak mají poměrně detailní informace z našeho soukromí na dosah ruky. V souvislosti s tímto jevem se tak někdy mluví o „zániku soukromí“[75].

Ochrana soukromí, a to nejen na sociálních sítích, tedy předpokládá „*právo kontrolovat fakta o svém vlastním životě*“[76]. Jak upozorňuje ve svém oficiálním prohlášení Spolkový komisař pro ochranu dat a svobodu informací: „*V současnosti je tu nedostatek ochrany proti kopírování jakéhokoli druhu osobních údajů z profilů – ať už dalšími členy sítě, nebo neoprávněnými třetími stranami zvenčí sítě – a jejich využívání pro vytváření osobních profilů, nebo opětovné publikování těchto údajů kdekoli jinde. Může být opravdu těžké – a někdy téměř nemožné – zajistit úplné odstranění informace z internetu jakmile byla již jednou publikována: dokonce i po jejím smazání z původní stránky (tj. sociální sítě), kopie totiž mohou zůstat u třetích stran nebo poskytovatelů služeb sociálních sítí. Osobní údaje z profilů mohou také „prosáknout“ mimo síť, kdy jsou zaznamenány internetovými vyhledávači. Někteří poskytovatelé služeb sociálních sítí navíc zpřístupňují uživatelská data třetím stranám prostřednictvím užití naprogramovaných rozhraní, která jsou pod kontrolou třetích stran.*“[77]

Právo na soukromí tak prodělalo kvantitativní a kvalitativní proměnu: počet zásahů do soukromí v době internetu dramaticky stoupá a díky novým technologiím jsou možné zásahy do soukromí, které si společnost ještě před pár lety nedokázala ani představit.[78] Klasickým příkladem se stal příběh Američanky Stacy Snyder[79], mladé aspirantky na pozici

---

[75] Tento názor zastává například česká filozofka Denisa Kera, podle níž jsme kvůli sociálním sítím o nedotknutelnost našeho soukromí již definitivně přišli a bojovat o ni již nemá smysl. Jak sama uvádí v rozhovoru s Janem Kovalíkem pro Respekt, edice Fenomén, *Svět technologických novinek*, ve spolupráci s The Economist, vydavatelství Economia, 21.05.2012: „*Zachovat si absolutní soukromí a zároveň neustále viset na síti je nemožné.*“ Dle Kery bychom se tedy raději měli soustředit na ochranu tzv. biodat (tj. informací o našich tělech) a poučit se vývojem na sociálních sítích, tedy nastavit lepší pravidla ochrany než bude příliš pozdě.

[76] SCHAUER, Federick: *Internet Privacy and the Public-Private Distinction*. 38 Jurimetrics 555, 1998, str. 556.

[77] Oficiální prohlášení o ochraně soukromí na sociálních sítích („*Draft Resolution on Privacy Protection in Social Network Services*“) německého Spolkového komisaře pro ochranu dat a svobodu informací z 30. mezinárodní konference komisařů o ochraně dat a soukromí pořádané 17. října 2008 ve francouzském Štrasburku, str. 1 prohlášení.

[78] Viz KÜHN, Zdeněk: *Ochrana soukromí v internetové době*. In: ŠIMÍČEK, Vojtěch: *Právo na soukromí*. MUNI Press, Brno 2011, str. 110 a násl.

[79] Stacy Snyder vs Millersville University, zn. Case 2:07-cv-01660-PD.

učitelky, která ve své nerozvážnosti uveřejnila na sociální síti MySpace fotografii z večírku, kde je zachycena v pirátském klobouku s plastovým kelímkem a titulkem „opilý pirát“[80]. Potom, co se vedení její univerzity dozvědělo o této fotografii, odmítli jí vydat závěrečný diplom s odůvodněním, že by byla špatným příkladem svým studentům. Stacy univerzitu zažalovala, ale svoji soudní při tehdy prohrála.

Neměli bychom opomenout také případ šestašedesátiletého Kanaďana Andrewa Feldmara, který jel vyzvednout svého přítele z letiště v americkém Seattlu, ale pohraniční stráží, která si ho prověřila prostřednictvím internetového vyhledávače, mu byl odmítnut vstup na území USA. Důvodem byl jeho článek uveřejněný před 30 lety ve filozoficky zaměřeném časopise, kde popisoval svoji zkušenost s LSD. Nejen že se tehdy nedostal na letiště v Seattlu, ale byl mu trvale zakázán vstup na území USA. [81]

Příběh Stacy a Andrewa se tak stal takřka učebnicovým příkladem nebezpečí, která nám na internetu hrozí ve věku digitalizace, kdy uchovávání dat se stalo samozřejmostí, avšak zapomínání jakousi zvláštností. Paradoxně jsme se tak dostali do situace, kdy lidská paměť časem zapomene, avšak internet nikdy nezapomíná.[82]

V souvislosti s ochranou našeho soukromí na sociálních sítích je tedy třeba si uvědomit, že sociální sítě jsou součástí veřejného prostoru a tak bychom k nim měli také přistupovat. Iluze soukromí, která se tu vytváří, často vede uživatele sociálních sítí k představě, že jim je zachován určitý stupeň anonymity jejich projevu a sdílených informací. Někteří uživatelé se dokonce domnívají, že se mohou skrýt za svoji fiktivní identitu, kterou si na sociální síti vytvořili. Zapomínají však, že je poměrně snadné je dohledat pomocí IP adresy jejich počítače.

Příkladem nám proto může být případ českého uživatele Rostislava Kocmana, tiskového mluvčího Air Bank, který na Twitteru nerozumě uveřejnil vyfocené pozadí své

---

[80] Foto viz http://www.podcastingnews.com/content/2007/12/myspace-party-pic-cost-stacy-snyder-job/ (11.11.2012). I šest let po uveřejnění této fotografie je první, co se v internetové vyhledávači při zadání jména Stacy Snyder objeví, právě tato fotografie. Jak vidíme, snadno se stane, že to nejhorší, co v životě uděláme, se často může stát tím, čím se na internetu jednou provždy „proslavíme“.

[81] Pro detailnější informace o těchto případech (a řadě jim podobných) viz např. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all (11.11.2012), nebo kniha Viktora Mayer-Schönbergera: *Delete – The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, str. 1 a násl.

[82] K tématu digitalizace, lidské paměti a zapomínání ve věku internetu doporučuji brilantní knihu Viktora Mayer-Schönbergera: *Delete – The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, který nám připomíná, že bychom se znovu měli naučit zapomínat. Za zmínku stojí také jeho inspirativní stejnojmenná přednáška dostupná zde: http://www2.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLecturesAndEvents/player.aspx?id=1109 (11.11.2012).

kolegyně z práce. Pan Kocman se za svůj „tweet" bance omluvil, ale odmítl ho smazat. Banka s panem Kocmanem nakonec rozvázala pracovní poměr, protože Kocmanovo chování považovala za nekorektní.[83] Iluzi „soukromí" na sociálních sítích podlehlo také pět mladíků, kteří byli odsouzeni k podmíněnému trestu odnětí svobody za podněcování rasové nenávisti, jež spočívala v uveřejnění odkazů rasistických hudebních klipů na Facebooku.[84]

Uživatelé často namítají, že pokud nemají co skrývat, nemají se ani čeho bát. Tento tzv. *nothing to hide* argument[85], jak uvádí prof. Solove, zpochybňuje samotnou potřebu soukromí. Ale opravdu neexistuje nic, co bychom chtěli před ostatními skrývat? Nevadilo by nám, kdyby naše korespondence byla komukoli veřejně přístupná? Kdyby všichni znali čísla našich bankovních účtů? Kdyby nás někdo vyfotografoval nahé a fotografie umístil na internet? Každý z nás má co skrývat. Otázkou pouze zůstává, jaké si nastavíme limity našeho soukromí. A právě to bychom si měli uvědomit při používání sociálních sítí.

1.7. Právní rámec ochrany

Sociální sítě představují komplexní právní fenomén, kde se můžeme setkat s celou řadou potenciálních právních problémů pramenících ze zneužití sociálních sítí. Jako demonstrativní výčet můžeme uvést: potencionální odpovědnost za pomluvu třetích stran, ztráta potencionálního/existujícího zaměstnání na základě osobního profilu na sociální síti – zásahy eventuálních/existujících zaměstnavatelů vůči profilům eventuálních/existujících zaměstnanců na sociálních sítích, ztráta dobré pověsti na základě profilu na sociální síti, ztráta identity prostřednictvím „krádeže identity", splynutí hranic mezi osobním a profesionálním životem jednotlivce prostřednictvím sociálních sítí, osobní profil vytvořený na sociálních sítích stále může být dohledatelným prostřednictvím internetového

[83] Pro bližší informace o tomto případu viz http://www.lupa.cz/clanky/profesni-sebevrazda-na-socialnich-sitich-aneb-jak-air-bank-vyhodila-mluvciho/(11.11.2012). Zmíněná fotografie např. zde: http://www.pc-politika.cz/print.php?type=N&item_id=2483 (11.11.2012). Pan Kocman zdaleka není prvním ani posledním zaměstnancem, který byl propuštěn na základě svého komentáře na svém profilu na sociální síti. Pro srovnání viz případ Tomáše Zmundy uveřejněný zde: http://www.tyden.cz/rubriky/domaci/kvuli-facebooku-se-propousti-uz-i-v-cesku_129484.html (21.11.2012).

[84] Více informací na: http://www.rozhlas.cz/zpravy/politika/_zprava/1049783 (11.11.2012).

[85] Blíže viz SOLOVE, Daniel J.: "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, San Diego Law Review, Vol. 44, 2007, GWU Law School Public Law Research Paper No. 289. Dostupné na: http://ssrn.com/abstract=998565; SOLOVE, Daniel J.: *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2007. Dostupné na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1019177 (11.11.2012).

vyhledávače, virtuální identita vytvořená online je těžko odstranitelná dokonce i prostřednictvím sofistikovaných technologií, možnost propojení profilu na sociální síti s dalšími webovými stránkami a daty uživatele (tedy vytvoření virtuálního profilu uživatele), trestné činy vyskytující se díky zneužití osobních informací jednotlivce, jako např. sledování, obtěžování apod.[86]

Sociální sítě tak nelze zařadit do jednoho právního odvětví, ani o nich nelze uvažovat jako o prostředí určitého právního vakua. V rámci sociálních sítí se uplatní právní instituty a právní předpisy jako kdekoli jinde, samozřejmě s přihlédnutím k určitým charakteristickým rysům sociálních sítí. Při aplikaci práva je tu třeba jít napříč právními odvětvími, zejména od práva na soukromí, ochrany osobnosti, závazkových práv, práv duševního vlastnictví, přes mezinárodní právo soukromé až k správnímu právu včetně správních deliktů a práva trestního.

Vzhledem k tématu a zaměření této práce budeme při aplikaci práva vycházet zvláště, avšak ne výlučně, na mezinárodní úrovni z Úmluvy č. 108 a v rámci evopského práva z celé řady směrnic – především ze Směrnice 95/46/ES doplněné o směrnici o určitých právních apektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (Směrnice 2000/31/ES)[87] a Směrnici 2002/58/ES. V rámci českého práva budeme aplikovat především zákon o ochraně osobních údajů (ZoOÚ).

V této kapitole se podíváme nejdříve na teritorialitu ochrany a aplikovatelné právo spolu s jurisdikcí, které se v rámci právního vztahu poskytovatele služeb sociální sítě a uživatele uplatní. Dále se zaměříme na právní vztah poskytovatele služeb sociální sítě a uživatele, zejména na postavení poskytovatele služeb sociální sítě a uživatele, včetně jejich práv a povinností, souhlas uživatele se zpracováním osobních údajů a obecně také na smluvní podmínky, jimiž se právní vztah mezi poskytovatelem a uživatelem řídí. Poté se soustředíme na likvidaci dat a právní prostředky ochrany.

---

[86] MANN, B. L.: *Social networking websites – a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos*. International Journal of Law and Information Technology, 2009, Vol. 17, No.3, str. 252-267.
Dostupné na: http://www.ucs.mun.ca/~bmann/0_ARTICLES/Mann_Social_Netg_IJLIT_08.pdf (16.12.2012).

[87] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých právních apektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (tzv. *E-Commerce Directive*). Tato směrnice byla provedena zák. č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů.

1.7.1. Teritorialita a aplikovatelné právo

Sociální sítě vyvolávají řadu otázek ohledně místní působnosti práva a ochrany poskytované jejich uživatelům. Přitom určení aplikovatelného práva a způsobu řešení případných sporů determinuje ochranu uživatelů a její realizaci v praxi.

Poskytovatelé služeb sociálních sítí často užívají jednotné smluvní podmínky pro všechny své uživatele na celém světě bez ohledu na to, odkud jejich uživatelé pochází, či kde se k sociální síti připojí. Vzhledem k tomu, že největší globální sociální sítě bývají původem z USA, kde mají také své sídlo, nepřekvapí nás, že i jejich smluvní podmínky stanoví jako aplikovatelné právo právě právo jednoho ze států USA (vzhledem k jejich umístění v Silicon Valley, nebo blízkém okolí, zpravidla volí právo státu Kalifornie).[88] Avšak najdeme i výjimky. Například smluvní podmínky sítě YouTube se řídí právem státu uživatele, tedy v případě českého uživatele českým právem, a případné spory by tak byly řešeny rovněž v jurisdikci uživatele, tedy v našem případě před českými soudy. YouTube si však nadále vyhrazuje právo podat předběžná opatření nebo opravné právní prostředky v kterémkoli státě světa. České právo se bude vztahovat také na české sociální sítě.[89]

Nestanoví-li si ve smluvních podmínkách poskytovatel služeb sociální sítě aplikovatelné právo spolu se soudní příslušností či arbitrážní doložkou, k určení jurisdikce se použíjí příslušné právní předpisy[90]. Nesmíme ale zapomenout, že ne vždy je smluvní určení aplikovatelného práva a soudní jurisdikce vykonatelné. Takovým případem budou dohody, resp. jejich příslušná ustanovení, které jsou neplatné nebo jsou v rozporu se závaznými právními předpisy, které omezují určení aplikovatelného práva a soudní jurisdikce[91].

---

[88] Např. Facebook, Twitter, Google+ a LinkedIn zvolili právě právo státu Kalifornie, kde by probíhaly i případné soudní spory. Soudní spory Facebooku, Google+ a LinkedInu by řešil soud v Santa Claře, zatímco Twitter zvolil soud v San Franciscu. Sociální síť Couchsurfing také volí právo státu Kalifornie, avšak případný spor by byl řešen arbitráží v San Franciscu.

[89] Např. Lidé, Spolužáci nebo Líbímseti.

[90] Například nařízení Evropského parlamentu a Rady 593/2008/ES, o právu rozhodném pro smluvní závazkové vztahy (tzv. nařízení Řím I).

[91] Typickým příkladem je spotřebitelské smlouva (Dle čl. 6 odst. 1 Nařízení Řím I: „*smlouva uzavřená fyzickou osobou za účelem, který se netýká její profesionální nebo podnikatelské činnosti, s jinou osobou, která jedná v rámci výkonu své profesionální nebo podnikatelské činnosti, se řídí právem země, v níž má spotřebitel obvyklé bydliště, pokud: a) obchodník provozuje svou profesionální nebo podnikatelskou činnost v zemi, kde má spotřebitel své obvyklé bydliště, nebo b) se jakýmkoli způsobem taková činnost na tuto zemi nebo na několik zemí včetně této země zaměřuje a smlouva spadá do rozsahu této činnosti*“). Pro podrobnější analýzu viz článek P.A. de Miguel Asensia*: Social Networking Sites: An Overview of Applicable Law Issues*. Annali italiani del diritto d´autore, della cultura e dello spettacolo (AIDA), Vol. XX, 2011. Dostupné na: http://eprints.ucm.es/13376/1/pdemiguelasensio-AIDA2011.pdf (12.11.2012).

Podíváme-li se na aplikovatelnost českého práva na ochranu osobních údajů, které se bude vztahovat na některé sociální sítě (viz výše), zjistíme, že dle ustanovení § 3 odst. 5 ZoOÚ, se ZoOÚ vztahuje pouze „*na zpracování osobních údajů, jestliže se právní řád ČR použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území ČR,* nebo *jestliže správce, který je usazen mimo území EU, provádí zpracování na území ČR a nejedná se pouze o předání osobních údajů přes území EU; v tomto případě je správce povinen zmocnit postupem podle § 6 na území ČR zpracovatele*". Správce osobních údajů tak může sídlit v jiném členském státě EU než, kde zpracovává údaje a není tak administrativně omezován více, než je nezbytně nutné (postačí mu zde mít zpracovatele). Samozřejmě ustanovení § 3 odst. 5 ZoOÚ se použije za předpokladu, že se smluvní strany nedohodly na aplikovatelném právu a místě řešení případných právních sporů.

Dále se ustanovení § 3 odst. 5 písm. b) ZoOÚ rozšířilo roku 2004 (novelou č. 439/2004 Sb.) v návaznosti na požadavek Směrnice 95/46/ES o další větu: „*jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území EU, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu EU*". To je případ Facebooku (*Facebook Ireland Limited*), který má svoji evropskou organizační složku v Dublinu, v Irsku.

Klíčovým problémem zůstává vymahatelnost těchto ustanovení. Český Úřad bude těžko účinně vykonávat dozor nad správcem sídlícím mimo EU. Stejně tak se bude uživatel (resp. subjekt údajů) s obtížemi domáhat svých práv na správci sídlícím mimo EU. Problém nevyřeší ani ustanovení zpracovatele, který bude pro správce na území EU zpracovávat data. Ustanoví-li totiž správce zpracovatele v rozporu s § 3 odst. 5 písm. b) ZoOÚ, Úřad bude muset svoji pravomoc vykonat přímo vůči správci sídlícím mimo EU. Tím se vracíme na začátek celého problému. Dalo by se tedy říci, že právní úprava tento problém účinně neřeší a ve snaze najít adekvátní řešení zavádí zákonnou pojistku, která se však snadno dá obejít, a my se tedy s řešením tohoto problému pohybujeme v kruhu.

Další komplikací při vymáhání ustanovení § 3 odst. 5 ZoOÚ je sankce za porušení této právní normy, která v hlavě VII (správní delikty) ZoOÚ chybí. Dokud tedy správce neporuší jinou svoji povinnost dle ZoOÚ, Úřad ho nemůže sankcionovat. Takže i když by se Úřadu podařilo navázat spolupráci se svým zahraničním protějškem, Úřad nemá správce za porušení této povinnosti jak sankcionovat.

Jak vidíme, česká právní úprava se v tomto ohledu ukázala být nedostačující. Tento problém by mohlo vyřešit připravované Obecné nařízení o ochraně údajů, ale o tom více až v kapitole 3.

1.7.2. Právní vztah poskytovatele služby sociální sítě a uživatele

Právní vztah mezi poskytovatelem služeb sociální sítě a uživatelem je založen smlouvou. Tento právní vztah můžeme klasifikovat jako právní vztah závazkový relativní. Dohoda, která tento právní vztah zakládá, je dvoustranným adresným asynallagmatickým právním úkonem, který je zpravidla bezúplatný[92]. Jde o tzv. inominátní smlouvu a podle toho musíme k tomuto právnímu vztahu přistupovat.

V této kapitole se zaměříme především na to, kdo je poskytovatelem služby sociální sítě a kdo je uživatelem, jaká práva a povinnosti se na ně vztahují, podíváme se na souhlas uživatele se zpracováním osobních údajů a na smluvní podmínky tento právní vztah upravující.

i. Poskytovatel služeb sociální sítě

Poskytovatel služeb sociální sítě je považován za správce[93] dle ZoOÚ a Směrnice 95/46/ES a, jak připomíná P.A. de Miguel Asensio[94], zároveň za poskytovatele služeb informační společnosti podle Směrnice 2000/31/ES. Směrnice 2000/31/ES totiž definuje poskytovatele služeb informační společnosti jako „*každou fyzickou nebo právnickou osobu, která poskytuje určitou službu informační společnosti, tj. každou službu poskytovanou zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb*“[95], což vykládá recitál 18 Směrnice 2000/31/ES následovně: „*Služby informační společnosti se neomezují výhradně na služby umožňující uzavírání smluv on-line, ale vztahují se rovněž, pokud jde o hospodářskou činnost, na služby, které nehradí ti, kdo je přijímají, jako např. služby poskytující informace on-line nebo obchodní sdělení nebo ty služby, které poskytují nástroje umožňující vyhledávání dat, přístup k datům a získávání dat. Služby informační společnosti zahrnují rovněž služby, které spočívají v předávání informací prostřednictvím*

[92] Užívání sociálních sítí bývá pro uživatele bezplatnou službou (např. Facebook, Twitter, Google+), ale najdou se i výjimky - některé sociální sítě rozlišují základní bezplatné členství a placené tzv. kvalifikované členství s větším rozsahem poskytovaných služeb (např. LinkedIn).
[93] Naplňuje zákonnou definici správce dle § 4 písm. j ZoOÚ, převzatou z čl. 2 písm. d Směřnice 95/46/ES – blíže viz pojem „správce“ v kapitole 1.4.
[94] DE MIGUEL ASENSIO, Pedro Alberto: *Social Networking Sites: An Overview of Applicable Law Issues*. Annali italiani del diritto d´autore, della cultura e dello spettacolo (AIDA), Vol. XX, 2011, str. 5 a násl. Dostupné na: http://eprints.ucm.es/13376/1/pdemiguelasensio-AIDA2011.pdf (12.11.2012).
[95] Čl. 2 písm, a, b Směrnice 2000/31/ES.

komunikační sítě, v poskytování přístupu ke komunikační síti nebo v shromažďování informací poskytovaných příjemcem služby".

Ačkoli služba sociální sítě je poskytovaná uživatelům zpravidla bezplatně (přinejmenším její základní funkce a členství v ní), z citovaného recitálu (zejména jeho poslední věty) je zřejmé, že definice služby informační společnosti je dostatečně obecná na to, abychom ji mohli vztahnout i na služby sociální sítě.

ii. Práva a povinnosti poskytovatele služeb sociální sítě

Jak vidíme, na poskytele služeb sociální sítě se tedy musíme dívat jak na správce, tak na poskytovatele služeb informační společnosti, z čehož poskytovateli služeb sociální sítě plyne celá škála práv a povinností.

Poskytovatel služeb sociální sítě má jako *poskytovatel služeb informační společnosti* především informační povinnosti vůči uživateli - mimo jiné obecnou informační povinnost, kdy musí umožnit uživatelům snadný, přímý a trvalý přístup k těmto informacím: svému jménu a zeměpisné adrese, kde je usazen; kontaktní údaje; identifikační údaje z rejstříku, v němž je zapsán a příslušnému kontrolnímu orgánu, je-li třeba[96]. Poskytovatel musí také poskytnout smluvní ustanovení a obecné obchodní podmínky uživateli v takové formě, aby je uživatel mohl uchovat a reprodukovat[97]. Všechny tyto povinnosti poskytovatele mají vést k ochraně uživatele a zpřístupnit tak uživateli informace nezbytné k uplatnění této ochrany.[98]

Poskytovatel služeb sociální sítě jako *správce dle ZoOÚ* má celou řadu nejrůznějších povinností vůči subjektu údajů. *Při zpracování osobních údajů* je správce povinen stanovit účel, prostředky a způsob zpracování osobních údajů; zpracovat pouze přesné osobní údaje a je-li třeba, aktualizovat je; shromažďovat a zpracovávat osobní údaje pouze ke stanovenému účelu a v rozsahu k tomu nezbytném (přičemž shromažďování musí být transparentní); uchovávat osobní údaje pouze po dobu nezbytnou k účelu zpracování osobních údajů a neslučovat osobní údaje získané k rozdílným účelům.[99] Při zpracování osobních údajů pak správce musí dbát na to, aby subjekt údajů neutrpěl újmu na svých právech (zejména na

[96] Čl. 5 odst. 1 Směrnice 2000/31/ES.
[97] Čl. 10 odst. 3 Směrnice 2000/31/ES.
[98] Většina těchto povinností poskytovateli více či méně bývá dodržována.
[99] § 5 ZoOÚ. Správcovy povinnosti ohledně souhlasu subjektu údajů rozebereme dále v této kapitole.

právu na lidskou důstojnost) a dohlížet na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.[100]

Při shromažďování osobních údajů musí správce informovat subjekt údajů o rozsahu a účelu zpracování osobních údajů, o tom kdo a jakým způsobem bude mít k těmto údajům přístup a zda je poskytnutí těchto údajů povinné či dobrovolné. Správce má dále povinnost informovat subjekt údajů o právu subjektu údajů na přístup k osobním údajům a právu na jejich opravu.[101] Obdobným způsobem se tyto povinnosti při zpracování a shromažďování osobních údajů vztahují také na správcova případného zpracovatele osobních údajů.[102]

Z uvedeného vyplývá, že zákonodárce se snaží ochránit subjekt údajů před případným zneužitím osobních údajů při zpracování a shromažďování osobních údajů a předcházet tak případným škodám a újmě na právech subjektu údajů. Zároveň je tu zřejmá snaha o posílení právního postavení subjektu údajů vůči správci v souvislosti s právem na informace.

Poskytovatel služeb sociální sítě má jako správce také povinnost umožnit subjektu údajů bezodkladný *přístup k informacím*[103], pokud o to subjekt údajů požádá. Obsahem takové informace vždy bude sdělení o účelu zpracování osobních údajů; o osobních údajích, které jsou předmětem zpracování; povaze automatizovaného zpracování a jejich příjemci.

Poskytovateli služeb sociální sítě jako správci osobních údajů náleží ještě celá řada dalších povinností, mimo jiné povinnost *zabezpečit zpracování osobních údajů*[104] tak, aby nemohlo dojít k jejich zneužití, ztrátě nebo zničení.

iii. Uživatel sociální sítě

Podle Směrnice 2002/58/ES se uživatelem rozumí „*jakákoli fyzická osoba používající veřejně dostupnou službu elektronické komunikace* (tedy včetně sociálních sítí) *pro soukromé či obchodní účely, přičemž není nezbytně nutné, aby byla účastníkem této služby*“[105].

Uživatel služeb sociální sítě je jednak považován za subjekt údajů[106], ale jak upozorňuje dr. Wong[107], poměrně snadno se také sám může stát správcem osobních údajů

[100] § 10 ZoOÚ.
[101] § 11 odst. 1, 2 ZoOÚ.
[102] § 7 ZoOÚ.
[103] § 12 ZoOÚ. Tuto povinnost správce za něj může splnit zpracovatel osobních údajů.
[104] § 13 ZoOÚ.
[105] Čl. 2 písm. a) Směrnice 2002/58/ES.
[106] Splňuje definici subjektu údajů podle § 4 písm. d ZoOÚ - blíže viz pojem „subjekt údajů“ v kapitole 1.4.

(jak podle ZoOÚ, tak podle Směrnice 95/46/ES). Směrnice 95/46/ES (z nichž vychází i český ZoOÚ) byla totiž přijata v době, kdy se problémy, které by později mohly z této definice správce vyvstat, nepředvídaly.[108]

V případech, kdy uživatel zpracovává pouze své vlastní osobní údaje, bude považován za subjekt údajů. Avšak jakmile začne zpracovávat osobní údaje jiných osob, je třeba zvážit, zda ho můžeme považovat za správce, nebo jestli na něj lze použít výjimku z ZoOÚ, resp. Směrnice 95/46/ES. Z této výjimky plyne, že se na uživatele ZoOÚ ani Směrnice 95/46/ES nebude vztahovat, zpracovává-li osobní údaje druhých výlučně pro svoji osobní potřebu[109].

V praxi se tak objevují případy, kdy jeden uživatel sociální sítě (příp. fyzická osoba, která služby sociální sítě ani neužívá) žaluje jiného uživatele sociální sítě jako správce, jako tomu bylo například v případu *Applause Store Productions Limited and Firsht v Raphael*[110] z Velké Británie. Pan Firsht, který nebyl uživatelem sociální sítě Facebook, žaloval svého dřívějšího přítele pro pomluvu, která spočívala v uveřejnění falešného profilu na Facebooku, vytvoření facebookové skupiny pomlouvající a zpochybňující solventnost Firshtovy společnosti Applause Store Productions a v následném poškození dobrého jména pana Firshta i jeho společnosti. Falešný profil obsahoval Firshtovu fotografii a směs pravdivých i nepravdivých informací o panu Firshtovi (včetně informací ohledně jeho sexuální orientace, osobní stavu, politického a náboženského přesvědčení a datum narození). Pan Firsht pomocí soudního příkazu přiměl Facebook k odstranění falešného profilu a skupiny. Žalovaný Raphael byl poté dohledán podle IP adresy svého počítače, z něhož falešný profil i skupinu uveřejnil na síti. Pan Firsht nakonec spor vyhrál a žalovaný Raphael mu pak musel zaplatit vysoké odškodnění (£52.000). Tento případ mimo jiné ukázal, jak snadné je na sociálních sítích vytvořit falešný profil jiné osoby a tuto osobu veřejně dehonestovat. Na druhou stranu se také potvrdilo, jak snadné je dohledat pachatele.

---

[107] WONG, Rebecca: *Social Networking: Anybody is a Data Controller* (21.09.2008). Dostupné na: http://ssrn.com/abstract=1271668 a WONG, Rebecca: *Social Networking: A Conceptual Analysis of a Data Controller* (30.12.2009). Communications Law, Vol. 14, No. 5, pp. 142-149, 2009 Dostupné na: http://ssrn.com/abstract=1529738

[108] Není se čemu divit – sociální sítě sice v době přijetí Směrnice 95/46/ES již existovaly, ale ještě zdaleka nebyly tak rozšířené a neposkytovaly takovou škálu možností, jak naložit s osobními údaji, jako je tomu dnes. Koho by tehdy napadlo, že o 10, 15 let později budou moci uživatelé zpracovávat osobní údaje druhých (jako např. fotografie, videa, kde je označen jiný uživatel, psát komentáře a vytvářet profily tvářící se jako komentáře či profil jiného uživatele)?

[109] Viz čl. 3 odst. 2 Směrnice 95/46/ES a § 3 odst. 3 ZoOÚ.

[110] Applause Store Productions Ltd. & Anor v Raphael [2008] EWHC 1781 (QB) (24. července 2008). Uvádí se jako jeden z prvních případů pomluvy a ochrany soukromí týkající se Facebooku, který se dostal až před soud.

Prokázalo se také, jak je důležité jednat rychle, než bude příliš pozdě a nepravdivé údaje se rozšíří po síti a vymknou další kontrole.

Také Česká republika již má svůj první případ falešného profilu[111], který se dostal až před soud. Dle obžaloby důchodkyně *Anna Stolínová* v dubnu 2010 na Facebooku vytvořila a zneužila falešný profil krajské šéfky libereckých komunistů *Dany Lysákové*. Obžalovaná Stolínová vytvořila falešnou emailovou adresu a následně profil, který se z počátku velmi podobal skutečnému profilu poškozené Lysákové a působil autentickým dojmem. Časem se však na profilu začaly objevovat zesměšňující fotografie zobrazující poškozenou. Dále tu byly umístěny komentáře a názory, které byly cynické a rozcházely se s názory poškozené. Poškozené tak byla způsobena újma nejen v soukromém, ale také jejím profesním životě, kdy se musela vzdát kandidatury do krajského zastupitelstva. Motivem obžalované bylo podezření z nevěry poškozené s manželem obžalované. Poškozená se nejdříve snažila přesvědčit manžele Stolínovy, aby profil smazali. Poté se obrátila na správce Facebooku s žádostí o smazání profilu. Ti profil však smazat odmítli s tím, že nemohou ověřit pravost profilu, a proto ho nemohou ani smazat. Poškozená se tedy nakonec obrátila na policii, která případ začala vyšetřovat. Reakcí obžalované bylo smazání falešného profilu (v březnu 2011). Policie poté dohledala nejen IP adresu počítače obžalované, ale také všechna „smazaná" data. Obžalovaná byla nakonec odsouzena za poškození cizích práv[112] k podmíněnému trestu odnětí svobody. Ačkoli je toto rozhodnutí soudu v ČR významné svým prvenstvím a je pravděpodobné, že podle něj budou soudy postupovat i v budoucnu, tento případ zároveň poukázal také na to, jak dlouho může na sociální síti trvat, než dojde k zastavení neoprávněného zásahu do cizích práv.

Nesmíme opomenout také významné rozhodnutí Evropského soudního dvora (ESD) ve věci *Lindqvist*[113,] kde ESD objasnil aplikaci Směrnice 95/46/ES na publikování osobních údajů na internetových serverech. Švédka Lindqvist v rámci počítačového kurzu vytvořila webovou stránku obsahující své osobní údaje a osobní údaje 18 dalších

---

111 Rozhodnutí Okresního soudu v Liberci z července 2012 (blíže viz článek Lucie Kavanové: *Ukradli mi moje já*. Respekt, ročník XXIII., č. 33, 11.08.2012.

112 § 181 zák. č. 40/2009 Sb., trestník zákoník, ve znění pozdějších předpisů. Soudce R. Skýba k rozsudku řekl: „*Byl to první případ svého druhu, neměl jsem se o co v minulosti opřít. Rozhodoval jsem se mezi pomluvou a poškozením cizích práv. O klasickou pomluvu ale nešlo – ty nesmysly o sobě jako by šířila sama oběť. Poškození cizích práv klasicky bývají případy, kdy někdo zneužije cizí občanský průkaz a třeba si na něj něco půjčí. Tohle bylo podobné – Stolínová se vydávala za Lysákovou a těmi výroky ohrozila její politickou kariéru.*" Článek Lucie Kavanové „*Ukradli mi moje já*" pro Respekt, 11.08.2012, blíže informuje o policejním vyšetřování a výskytu krádeží identity na sociálních sítích.

113 Rozhodnutí ESD ve věci Bodil Lindqvist zn. C-101/01 ze dne 6. listopadu 2003. Dostupné na: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d5e261466ff1ec4042a955f4c5ea6bf753.e34KaxiLc3eQc40LaxqMbN4Oa3uOe0?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=60220 (11.11.2012).

dobrovolníků (jméno, příjmení, telefonní čísla, zájmy a povolání) z jejich farnosti, kde mimo jiné uvedla, že si jedna dobrovolnice poranila nohu. Paní Lindqvist se domáhala výše uvedené výjimky čl. 3 odst. 2 Směrnice 95/46/ES (zpracování dat výlučně pro osobní potřebu). ESD však jednání paní Lindqvist kvalifikoval jako zpracování osobních údajů automatizovanými prostředky, na něž se tato výjimka nevztahuje vzhledem k tomu, že uveřejněné osobní údaje byly na internetu komukoli přístupné. Dle ESD se tato výjimka aplikuje „*pouze na aktivity, které jsou vykonávány v rámci soukromého nebo rodinného života jednotlivců, což zjevně není případ zpracování osobních údajů spočívající v publikaci na internetu tak, že tyto údaje jsou přístupné neurčitému počtu lidí*".

Závěrem tak můžeme dovodit, že publikuje-li někdo osobní údaje druhých bez jejich souhlasu na internetu (sociální sítě nevyjímaje), kde k těmto údajům bude mít přístup neomezený počet osob, výjimku pro osobní potřebu nebude možné použít. Dá se předpokládat, že u sociálních sítích tak ve většině případů nebude možné na tuto výjimku spoléhat a na uživatele publikující osobní údaje druhých bez jejich souhlasu tak bude nahlíženo jako na správce[114], čemuž budou odpovídat také jejich povinnosti a případné sankce za jejich porušení. Z výše uvedných případů tak vyplývá, že při publikování osobních údajů druhých je třeba zvýšené obezřetnosti a rychlého jednání v případě neoprávněného zpracování osobních údajů.

iv. Souhlas

Aby mohl správce (tzn. poskytovatel služby sociální sítě, příp. uživatel zpracovávající osobní údaje jiného uživatele) zpracovávat osobní údaje, potřebuje k tomu souhlas subjektu údajů[115]. Souhlas subjektu údajů je „*svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů*".[116] Souhlas subjektu údajů musí být tzv. informovaným souhlasem, což znamená, že správce musí při udělení souhlasu subjekt informovat o účelu zpracování, vymezit, ke kterým osobním údajům je souhlas dáván, a kdo a po jak dlouhou dobu bude tyto osobní údaje zpracovávat.[117] U citlivých údajů[118] se navíc vyžaduje, aby tento informovaný souhlas byl výslovný[119]; platí tu

[114] O právech a povinnostech uživatele jako správce – blíže viz „Práva a povinnosti poskytovatele služby sociálních sítí" v téže kapitole výše.
[115] § 5 odst. 2 ZoOÚ.
[116] § 4 písm. n) ZoOÚ.
[117] § 5 odst. 4 ZoOÚ.
[118] Viz kapitola 1.4., kde je vymezen pojem „citlivý údaj".
[119] § 9 písm. a) ZoOÚ.

tedy přísnější režim. Informovaný souhlas u citlivých údajů je tedy souhlasem kvalifikovaným, který musí být výslovný a jednoznačný – jeho konkludentnost nestačí.

Správce musí být schopen prokázat souhlas subjektu údajů se zpracováním osobních údajů po celou dobu jejich zpracování[120] Nezíská-li správce od subjektu údajů souhlas se zpracováním osobních údajů, nesmí tyto osobní údaje zpracovávat. Totéž platí pro kumulaci osobních údajů, kdy správce bez souhlasu subjektu údajů nesmí k osobním údajům přiřazovat další osobní údaje subjektu údajů, aniž by k tomu měl souhlas subjektu údajů.[121]

Zákon stanoví výjimky, kdy souhlasu subjektu údajů nebude třeba. Tak je tomu v případě, kdy správce provádí zpracování nezbytné pro: (i) dodržení právní povinnosti správce, (ii) pro plnění smlouvy, (iii) ochranu životně důležitých zájmů subjektu údajů, (iv) ochranu práv a právem chráněných zájmů správce; nebo (v) se jedná o zpracování výlučně pro účely archívnictví, (vi) poskytuje osobní údaje veřejně činné osobě nebo (vii) jde o oprávněně zveřejněné osobní údaje v souladu se zvláštním předpisem.[122] Při udělení souhlasu se zpracováním osobních údajů musí být subjekt údajů informován, o které osobní údaje se jedná, o účelu jejich zpracování, kdo bude správcem a po jak dlouhou dobu je bude zpracovávat.

Souhlas uživatel na sociálních sítích obvykle vyjádří prostřednictvím zakliknutí příslušného políčka, kde se uvádí, že souhlasí se smluvními podmínkami, podmínkami příslušné aplikace, nebo změnou nastavení svého profilu a podobně. Avšak otázkou zůstává, zda-li opravdu můžeme mluvit o informovaném souhlasu v případě adhezní smlouvy, jejíž smluvní podmínky jsou komplikované, běžnému uživateli nesrozumitelné a které většina uživatelů ani nečte. Přesto v praxi tento problém poskytovatelé neřeší a považují takový souhlas za dostatečný.

Ve vztahu uživatel – uživatel (příp. třetí osoba) se na druhou stranu nezřídka vyskytují problémy se zveřejňováním a šířením informací, fotografií, či videí označujících nebo jinak indentifikujících ostatní uživatele (resp. třetí osoby, které služby sociální sítě neužívají) bez jejich předchozího souhlasu. Chybí tu tak ochrana *ab initio*. Uživatelé, jichž se taková data týkají, se na uživateli, který data uveřnil/rozšířil po síti, mohou dožadovat smazání takových dat až *post factum*, jedná se tedy o následnou ochranu. Problémem je, že jakmile byla jednou data zveřejněna na internetu, nikdy nemáme jistotu, že smaže-li je

[120] § 5 odst. 4 ZoOÚ.
[121] § 5 odst. 5 ZoOÚ.
[122] § 5 odst. 2 ZoOÚ.

uživatel-původce, odstraní se tak i všechny ostatní stopy dat z internetu. Zveřejněná data může mezitím někdo zkopírovat, uložit a rozšířit dále, nebo mohou zůstat ve vyrovnávací paměti (tzv. cache[123]) internetového vyhledávače.

v. Smluvní podmínky

Součástí smlouvy mezi poskytovatelem služeb sociální sítě a uživatelem jsou smluvní podmínky[124]. Smluvní podmínky jsou předem dané poskytovatelem a jsou zpravidla pro všechny uživatele sociální sítě na celém světě stejné. Jedná se tedy o adhezní smlouvu mezi poskytovatelem a uživatelem, do níž uživatel nemá možnost jakkoli zasahovat. Uživatel tak má dvě možnosti: a) chce-li užívat jím vybranou sociální síť, musí bezvýhradně souhlasit se smlouvou včetně jejích smluvních podmínek tak, jak jsou mu předloženy - uživatel uzavře smlouvu s poskytovatelem a začne užívat služby vybrané sociální sítě; nebo b) uživatel chce užívat jím vybranou sociální síť, ale s pomínkami smlouvy nesouhlasí a v dané podobě na ně není ochoten přistoupit - uživatel smlouvu neuzavře a nebude oprávněn vybranou sociální síť užívat (může si však najít jinou alternativní síť). V praxi ale drtivá většina uživatelů (právníky nevyjímaje) smluvní podmínky nečte. Vzhledem ke komplikovanosti a nepřehlednosti smluvních podmínek je pravděpodobné, že průměrný uživatel by smluvním podmínkám ani nerozuměl.

Další otázkou je případná jazyková bariéra, která může vzniknout při čtení smluvních podmínek. Smluvní podmínky celosvětově nejrozšířenějších sociálních sítí (jako je např. Facebook, Twitter, LinkedIn, atd.) jsou uživateli dostupné zpravidla v několika jazycích, přičemž rozhodnou jazykovou verzí bývá verze anglická[125]. Například Facebook operuje ve více než 100 světových jazycích, avšak zdaleka ne ve všech těchto jazycích zpřístupňuje také své smluvní podmínky.[126] Snadno tak může vzniknout jazyková bariéra,

---

[123] Cache je vyrovnávací paměť – v případě internetových vyhledávačů tzv. mezipaměť, v níž zůstávají zaznamenány předchozí vyhledávané informace (čímž se zrychluje další vyhledávání a snižuje zátěž serverů).

[124] Smluvní podmínky bývají poskytovateli nazývány různě: Prohlášení o právech a povinnostech (v originále „*Statement of Rights and Responsibilities*“) – Facebook; Podmínky služby („*Terms of Service*“) – Twitter; Smluvní podmínky („*Terms of Service*“) - Google+; Smlouva s uživatelem („*User Agreement*“) – LinkedIn; Podmínky použití („*Terms of Use*“) – Couchsurfing.

[125] Není divu, když tyto sociální sítě sídlí v USA, řídí se americkým právem, volí americkou jurisdikci a samozřejmě potom bude i pro jejich smluvní podmínky rozhodující anglická verze.

[126] Smluvní podmínky Facebooku jsou dostupné např. v češtině, němčině, dánštině, bulharštině, finštině, hindštině či hebrejštině, avšak nedostupné jsou např. ve velštině, estonštině, litevštině, běloruštině, sanskrtu či arménštině. Pro uživatele, v jejichž jazyce smluvní podmínky dostupné nejsou, je základní nastavení smluvních podmínek v angličtině.

kdy si uživatel neznalý nabízených jazyků smluvní podmínky nepřečte, ani kdyby o to opravdu měl zájem.

Podíváme-li se na obsah smluvních podmínek, zjistíme, že smluvní podmínky jednotlivých poskytovatelů mají určité společné rysy. Poskytovatelé v maximálním právem umožněném rozsahu omezují svoji odpovědnost za škodu vůči uživatelům a třetím osobám, nezaručují uživatelům trvalý a nerušený přístup ke službám sociální sítě a bez předchozího upozornění mohou uživateli omezit přístup nebo smazat jeho účet. Poskytovatelé si dále vyhrazují právo na využití poskytnutých osobních údajů k cílené reklamě a marketingu. Uživatelé se zavazují poskytovateli udělit celosvětově platnou nevýhradní bezplatnou licenci k obsahu chráněném právem duševního vlastnictví publikovanému na sociálních sítích. Uživatelé dále výslovně souhlasí s předáním jejich osobních údajů do zahraničí. Poskytovatelé také věnují část podmínek bezpečnosti sociálních sítí, kde nabádají uživatele k tomu, aby na sociálních sítích nejednali protiprávně, nezasahovali do práv druhých, atd. Tato ustanovení mají však spíše deklaratorní hodnotu etického kodexu. Případným postihem poskytovatele vůči uživateli je v tomto ohledu smazání uživatelova profilu, příp. jeho části, což uživateli nezabrání vytvořit si obratem nový profil.

Zvážíme-li možná řešení těchto problémů, v případě poskytovatelů služeb sociální sítě by mohlo pomoci připravit jednoduché, srozumitelné a stručné smluvní podmínky v co nejvíce jazykových mutacích, kterým by rozuměl každý průměrný uživatel (bez potřeby předchozího právního vzdělání) a technicky zajistit, aby si je uživatel musel přečíst dříve, než se do sociální sítě zaregistruje (tzn. ne odkazem na přiložený dokument, ale aby se podmínky vždy zobrazily na obrazovce před uživatelem).

Chyba však není zdaleka pouze na straně poskytovatele. Také uživatelé by si měli uvědomit, jak nezodpovědné je uzavřít smlouvu a neseznámit se s jejím obsahem. Od uživatelů bychom měli požadovat větší míru zodpovědnosti, soudnosti a respektu také vůči ostatním uživatelům, zejména co do obsahu, který o nich uveřejňují či šíří.[127]

Závěrem můžeme říci, že ze smluvních podmínek poskytovatelů je zjevné, že mají ochránit především poskytovatele služeb sociální sítě.[128] Případy, kdy by se uživatelé

[127] Jak poučuje své uživatele např. Facebook v čl. 5. odst. 7, 8, 9 Prohlášení o právech a povinnostech.

[128] Zajímavý je v tomto ohledu spor rakouského studenta práv Maxe Schremse s Facebookem. Pan Schrems podal cca 22 stížností irskému Úřadu pro ochranu osobních údajů, kde napadá celou řadu smluvních podmínek Facebooku a poukazuje na jejich rozpor s evropským právem a nepochopení evropské ochrany uživatele. V současné době vyjednává s Facebookem a snaží se dojednat nápravu. Podle posledních informací

domáhali neplatnosti ustanovení smluvních podmínek jsou spíše vzácné.[129] Ve většině případů uživatelé nevědí ani nemají zájem na tom, aby žalovali jejich oblíbenou sociální síť (a riskovali, že se jich sociální síť zbaví a oni tak ztratí kontakt se svými přáteli).[130] Prof. Edwards navrhuje, že mnohem lepší a efektivnější přístup, než napadání smluvních podmínek uživateli sociálních sítí, by byla státní regulace sociálních sítí prostřednictvím právních předpisů, které by odpovídajícím způsobem přiměly poskytovatele upravit svůj software – a svůj „kód".[131]

1.7.3. Likvidace dat

Jak jsme si ukázali v předchozích kapitolách, jakmile jsou jednou data uveřejněna na internetu, je velmi těžké, ne-li nemožné, je z internetu odstranit. Ačkoli smazání dat z původního datového nosiče může být snadné, smazání všech stop, která tato data na internetu zanechala, se ukázalo být úkolem velmi obtížným[132]. V případě uveřejnění nežadoucích dat je tak třeba reagovat rychle, než budou data rozšířena dále (než budou zkopírována uživateli internetu, umístěna na další internetové servery, zanesena v cache internetových vyhledávačů atd.).

Nabízí se tedy otázka, co lze dělat, když subjekt údajů chce odstranit své osobní údaje uveřejněné na sociální síti. Jedná-li se o osobní údaje uveřejněné subjektem údajů, subjekt údajů je může smazat sám. Pokud tyto osobní údaje mezitím zkopírovali další uživatelé a začali je šířit dále (nebo je tito uživatelé sami uveřejnili na sociální síti), teoreticky je můžeme všechny požádat o smazání těchto údajů. Samozřejmě, čím více byly tyto osobní údaje rozšířeny, tím bude náročnější jejich odstranění realizovat. Kdokoli začne tyto osobní údaje zpracovávat (např. umístí je na internetu nebo je bude šířit dále), bude považován za

---

to vypadá, že pan Schrems bude Facebook nakonec žalovat pro porušení evropského práva na ochranu soukromí a zpracování osobních údajů. Rozhovor s panem Schremsem: http://www.ceskapozice.cz/zahranici/evropa/sokujici-fakta-o-facebooku-nasich-osobnich-udajich (21.11.2012).

[129] Přesto takové případy existují – viz např. *Bragg v Linden Labs*, Inc., 487 F. Supp. 2d 593 (E.D.Penn. 2007) pennsylvánské rozhodnutí z 30. května 2007 č. 06-4925, kde se pan Bragg dovolal neplatnosti arbitrážní doložky (soud uznal, že SNS Linden Labs byla výjimečná a pan Bragg tedy za ní neměl alternativní náhradu).

[130] EDWARDS, Lilian; WAELDE, Charlotte: *Law and the Internet*. 4th edition. Hart Publishing, 2009, str. 483.

[131] Tamtéž.

[132] Viz případ jihokorejské slečny, která odmítla uklidit výkaly svého psa v metru. Někdo dívku vyfotografoval a fotografii umístil na oblíbenou jihokorejskou stránku. Dívka se „proslavila" jako „개똥녀" („*Dog poop girl*"). Bohužel nezareagovala dostatečně rychle a fotografie se mezitím začala šířit internetem a do médií (zejména v Jižní Koreji a USA), dodnes dostupné např. zde: http://www.famouspictures.org/index.php?title=Dog_Poop_Girl (17.11.2012). Tato fotografie je dnes rozšířená na tolika serverech, že by ji již nebylo možné z internetu zcela odstranit. Navíc byla dívka dle fotografie tehdy identifikována a její osobní údaje uveřejněny na internetu.

správce (neaplikuje-li se na něj výjimka užití výlučně pro osobní potřebu dle § 3 odst. 3 ZoOÚ, která se však dle judikatury[133] na publikaci osobních údajů na internetu nevztahuje).

Nebude-li možné tímto způsobem údaje ze sociální sítě smazat, subjekt údajů se může obrátit na poskytovatele služby sociální sítě a žádat jejich odstranění.[134] Uveřejní-li osobní údaje poskytovatel, bude posuzován jako správce a subjekt údajů ho může požádat o jejich odstranění.

Zákon o ochraně osobních údajů k tomu říká, že správce je oprávněn uchovávat osobní údaje pouze po dobu nezbytně nutnou k účelu jejich zpracování[135]. Jakmile tento účel pomine, správce je povinen provést likvidaci osobních údajů. Likvidací osobních údajů se rozumí *„fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování“*[d36]. Správce je také povinen zlikvidovat osobní údaje, kdykoli o to subjekt údajů požádá[137], pozbyde-li správce právní titul k zpracování osobních údajů, nebo uloží-li mu tuto povinnost Úřad jako nápravné opatření k provedené kontrole[138]. *„Výsledkem likvidace dat musí být jejich faktické zničení či znepřístupnění pro správce i jakýkoliv další subjekt. Rovněž je nutno podotknout, že dle definice zpracování obsažené v § 4 písm. e) ZoOÚ je i samotnou likvidaci nezbytné považovat za zpracování osobních údajů, resp. za jednu, byť z časového hlediska poslední, zpracovatelskou operaci.“*[d39] Pro posouzení, zda byly osobní údaje řádně zlikvidovány, bude jedním z rozhodujících kritérií míra a spolehlivost jejich vyloučení z dalšího zpracování.[140]

Každý subjekt údajů, který zjistí nebo se domnívá, že správce provádí zpracování jeho osobních údajů v rozporu s jeho ochranou soukromého či osobního života nebo v rozporu se zákonem (zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování), může požádat správce o vysvětlení a požadovat, aby správce odstranil tento stav (především opravou, doplněním nebo likvidací údajů).[141] Je-li žádost subjektu

---

133 Viz již dříve zmiňované rozhodnutí ESD ve věci *Bodil Lindqvist* zn. C-101/01 ze dne 6. listopadu 2003.
134 Obdobně případ falešného profilu v kapitole 1.7.2 „uživatel“ výše.
135 § 5 odst. 1 písm. e) ZoOÚ.
136 § 4 písm. i) ZoOÚ.
137 § 20 odst. 1 ZoOÚ. Samozřejmě nestanoví-li zákon jinak (např. archívnictví, občanské, trestní, správní řízení, apod.).
138 § 40 odst. 2 ZoOÚ.
139 KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář.* 1. vydání. C.H. Beck, Praha 2003, 2012, str. 275.
140 MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav: *Osobní údaje a jejich ochrana.* 2. vydání. ASPI-Wolters Kluwer, Praha 2008, str. 253.
141 § 21 odst. 1 ZoOÚ.

oprávněná, správce musí neprodleně závadný stav odstranit (tedy v našem případě osobní údaje smazat).[142]

Překvapivě, ustanovení § 20 ZoOÚ[143] o likvidaci osobních údajů nebylo nikdy novelizováno (tj. od roku 2000) a jeho porušení nezakládá skutkovou podstatu žádného správního deliktu podle ZoOÚ. Porušení § 20 ZoOÚ tedy nelze sankcionovat. Správním deliktem[144] je pouze porušení § 5 odst. 1 písm. e) ZoOÚ[145], tedy uchování osobních údajů správcem déle než je nezbytné k účelu jejich zpracování. Za tento správní delikt může Úřad uložit fyzické osobě pokutu ve výši do 1.000.000,- Kč, právnické osobě pokutu ve výši do 5.000.000,- Kč. Byl-li tímto správním deliktem fyzickou osobou jako správcem nebo zpracovatelem a) ohrožen větší počet osob svým neoprávněným zasahováním do soukromého a osobního života subjektu údajů, nebo b) porušena povinnost pro zpracování citlivých údajů, Úřad může uložit fyzické osobě pokutu ve výši do 5.000.000,- Kč, právnické osobě pokutu ve výši do 10.000.000,- Kč. [146]

Správním deliktem není ani případ, kdy správce nevyhoví námitce subjektu údajů ohledně zpracování osobních údajů subjektu údajů v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem.[147] V takovém případě by se tedy subjekt údajů musel domáhat ochrany svého práva občanskoprávní žalobou[148], nebo najít jiné porušení ZoOÚ správcem, které by subjekt mohl uplatnit ve správním řízení před Úřadem.

Podíváme-li se pro srovnání na smluvní podmínky Facebooku („Prohlášení o právech a povinnostech“, poslední revize ze dne 8. června 2012) a jejich úpravu likvidace dat, zjistíme, že odstraníme-li obsah chráněný duševním vlastnictvím (fotografie, videa, autorské texty[149] apod.), skončí sice licence Facebooku k tomuto obsahu a obsah bude odstraněn z našeho profilu, avšak nebude odstraněn například z profilů či soukromých zpráv ostatních uživatelů, s nimiž byl obsah sdílen. Facebook dále upozorňuje, že tohle

---

142 § 21 odst. 2 ZoOÚ.

143 § 20 ZoOÚ: „*Správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů podle §21. Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.*“

144 § 44 odst. 2 písm. d), § 45 odst. 1 písm. d) ZoOÚ.

145 § 5 odst. 1 písm. e) ZoOÚ: „*Správce je povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné.*“

146 § 44 odst. 3, 5, 6, § 45 odst. 3, 4 ZoOÚ.

147 § 21 ZoOÚ.

148 Viz následující kapitola.

149 Neměli bychom zapomenout, že tato autorská díla mohou obsahovat osobní údaje uživatele.

odstranění obsahu bude provedeno obdobným způsobem jako odstranění obsahu do „koše“ našeho počítače. To znamená, že odebraný obsah může nadále existovat v záložních kopiích Facebooku po „přiměřeně dlouhou dobu“, kterou však Facebook blíže nespecifikuje (tento obsah však nebude dostupný ostatním uživatelům).

Facebook si dále vyhrazuje právo odebrat jakákoli data na něm zveřejněná, pokud se domnívá, že to porušuje jeho zásady nebo smluvní podmínky. Proti odebrání dat je možné „odvolat se“ Facebooku a dožadovat se jejich opětovného uveřejnění.

Velmi zajímavá je také deaktivace účtu uživatele. Uživatel může kdykoli deaktivovat svůj osobní účet (profil). Deaktivace vypne profil uživatele, odebere jeho jméno a obrázek z *téměř* veškerého obsahu, který uživatel na Facebooku kdy sdílel. Některé informace však mohou být stále viditelné pro ostatní (např. jméno uživatele v jeho seznamu přátel a v odeslaných zprávách). Nadále tedy na Facebooku zůstanou například zprávy, fotografie, či videozáznamy, které uživatel sdílel se svými přáteli. Uživatel svůj účet může opět kdykoli aktivovat a tím zcela obnovit svůj účet do jeho původní podoby.

Od deaktivace účtu je třeba rozlišit trvalé odstranění účtu. Pro trvalé odstranění účtu uživatel musí vyplnit příslušný formulář a poté již nikdy nebude moci obnovit svůj účet, ani k němu získat přístup jiným způsobem. *Většina* informací, které jsou s účtem spojeny a mohou potenciálně vést k odhalení totožnosti uživatele, jsou z databáze Facebooku odstraněny. Mezi tyto informace patří e-mailová adresa, poštovní adresa a přezdívka uživatele. Některé údaje, které by mohly uživatele identifikovat jako konkrétní osobu, však mohou být zachovány (např. jméno uživatele, pokud odeslal zprávu jinému uživateli). Kopie některých materiálů (fotografie, poznámky apod.) mohou zůstat na serverech Facebooku z technických důvodů, avšak tyto materiály jsou odděleny od veškerých osobních identifikátorů a zcela nepřístupné jiným uživatelům na Facebooku. Avšak kde máme jistotu, že Facebook, resp. ostatní sociální sítě, naše data skutečně zlikviduje? A jak to budeme kontrolovat?

V případě smrti uživatele Facebook tzv. „zvěční jeho profil“. Profil uživatele bude nadále existovat a bude mu poskytována obdobná ochrana jako za jeho života s tím, že bude omezen přístup k některým jeho projevům osobní povahy učiněným za života. „Přátelům“ uživatele zůstane možnost psát komentáře na jeho profil (tzv. „zeď“), aby tak uctili jeho památku. Facebook také umožňuje rodinným příslušníkům zesnulého uživatele deaktivovat jeho účet.

Pozoruhodný je v tomto ohledu případ manželů Strassenových z USA, kteří se úspěšně domohli soudního příkazu na vydání všech osobních účtů na sociálních sítích jejich nejmladšího syna Benjamina. Benjamin spáchal sebevraždu v roce 2011 a všechen jeho majetek zdědili jeho rodiče. Protože Benjaminovi rodiče chtěli mít plný přístup k účtům Benjamina na všech sociálních sítích, které užíval, a dozvědět se tak více o jeho myšlenkových pochodech před jeho sebevraždou, obrátili se na soud, kde se dožadovali soudního příkazu na vydání přístupových hesel k Benjaminovým účtům. Soudce tehdy neměl relevantní precedent, z kterého by vycházel při svém rozhodování, proto zvážil, zda je Benjaminův „digitální majetek" součástí dědictví. Soudce našel analogii v bankovních účtech a v určitých podobnostech jejich úrovně ochrany soukromí a soudní příkaz vydal (nejen k Benjaminovým účtům u sociálních sítí, ale také k jeho emailu a blogům). Dle posledních informací se Benjaminovi rodiče snaží přimět Facebook k předání Benjaminova účtu. Zatím neúspěšně. Jejich smluvní podmínky to neumožňují, ale lze považovat za více než pravděpodobné, že se Facebook nakonec přeci jen bude muset podřídit. Mezitím se podařilo získat přístup k Benjaminovu emailu Gmail u společnosti Google.[150] Otázkou je, zda by si zemřelý přál, aby někdo po jeho smrti měl přístup k jeho nejintimnějším informacím.

Závěrem můžeme shrnout, že ačkoli existují způsoby, jak odstranit data uživatele ze sociální sítě, odstranění dat nebude kompletní a data uživatele (ať už jsou to jeho osobní údaje, nebo jiná data) zůstanou v určitém, byť omezeném, rozsahu přístupná ostatním uživatelům, se kterými uživatel svá data sdílel[151]. Data uveřejněná uživatelem také mohou zůstat v cache internetových vyhledávačů, což uživatel sám nemá možnost jakkoli odstranit[152].

Žijeme v digitálním věku, kdy každý z nás zanechává stopy dat o své existenci a o svém soukromí na internetu (včetně sociálních sítí) a ne vždy si uvědomujeme, že jakákoli data, která o nás budou kdy uveřejněna na internetu, tam s velkou pravděpodobností také

---

[150] Pro více informací viz článek Jessicy Hopper: *Digital Afterlife: What happens to your online accounts when you die?* Rock Center, 01.06.2012. Dostupné na: http://rockcenter.nbcnews.com/_news/2012/06/01/11995859-digital-afterlife-what-happens-to-your-online-accounts-when-you-die? (21.11.2012).

[151] Může se jednat o zprávy či komentáře, které uživatel sdílel s ostatními, fotografie a videozáznamy, kde je uživatel zachycen, odkazy na webové stránky, které uživatel poslal na profily svých „přátel", atd.

[152] Návod jak technicky odstranit svá data z interntetu, najdete zde: JACOBSSON PUREWAL, Sarah: *Erase Yourself From the Web.* PCWorld, 30.03.2011. Dostupné na: http://www.pcworld.com/article/223682/erase_your_web_presence.html (21.11.2012).
Můžete tak odstranit velké množství svých dat z internetu, avšak nelze je, jak autor článku sám upozorňuje, odstranit zcela.

jednou provždy zůstanou. Likvidace dat, ať už z internetových vyhledávačů, sociálních sítí, nebo dat uchovávaných správci, je úkolem technicky náročným a jeho výsledky nám nikdy nezaručí, že všechna data byla zcela odstraněna. Právo nám sice poskytuje určitý stupeň ochrany našeho soukromí a zpracování našich osobních údajů včetně jejich následné likvidace, ale jak jsme si ukázali, tato ochrana není dostačující a současná legislativa nám není schopna zaručit kompletní ochranu našeho soukromí v prostředí internetu, resp. sociálních sítí.

Nabízí se zdánlivě jednoduché řešení – jednoduše sociální sítě, příp. internet, nepoužívat. Nejlepším řešením se tak v současné době jeví prevence (alespoň do té doby, než bude přijata potřebná nová právní úprava). To, co nikdy nebude zveřejněno na internetu, z něj nebude muset být také nikdy složitě odstraňováno.

1.7.4. Právní prostředky ochrany

Právní prostředky ochrany poskytované subjektům údajů můžeme rozlišit na prostředky soukromoprávní a veřejnoprávní. Soukromoprávní prostředky ochrany spočívají převším v žalobách na ochranu osobnosti podle § 13 ObčZ a dále v uplatnění nároku subjektu na náhradu škody. Veřejnoprávní prostředky ochrany se dále dělí na správněprávní a trestněprávní prostředky ochrany. Správněprávní prostředky představují ochranu a dozor Úřadu nad zpracováním osobních údajů správci, přičemž je Úřad oprávněn provádět kontroly, ukládat správcům nápravná opatření a nestačí-li, pak pokuty za správní delikty. Je-li třeba, Úřad v rámci ochrany spolupracuje se svými zahraničními protějšky. Trestněprávní ochrana je založena na trestním stíhání pachatele za trestné činy spáchané na sociálních sítích. Vzhledem k tomu, že trestněprávní prostředky ochrany jsou považovány za *ultima ratio*, přednostně se uplatní správněprávní prostředky ochrany a trestněprávní prostředky se využijí až v případě, kdy správněprávní prostředky neposkytují dostatečnou ochranu. Je třeba podotknout, že veřejnoprávní a soukromoprávní prostředky ochrany se navzájem nevylučují. V této kapitole se detailněji zaměříme na jednotlivé právní prostředky ochrany.

i. Soukromoprávní prostředky ochrany

Subjekt údajů má vůči správci[153] nárok na odstranění závadného stavu (spočívajícího především v blokování, opravě, doplnění nebo likvidaci osobních údajů[154]), na omluvu nebo jiné zadostiučinění, včetně případného zaplacení peněžité náhrady.

Vznikla-li subjektu údajů škoda[155], k uplatnění nároku subjektu k náhradě této škody se použijí příslušná ustanovení o náhradě škody podle občanského[156], resp. obchodního zákoníku[157].

Vznikla-li subjektu údajů jiná než majetková újma, postupuje se při uplatňování jeho nároku podle ustanovení o ochraně osobnosti § 13 ObčZ.[158] Subjekt údajů má v takovém případě právo domáhat se, aby bylo upuštěno od neoprávněných zásahů do jeho práva na ochranu osobnosti, aby byly odstraněny následky těchto zásahů a aby mu bylo dáno přiměřené zadostiučinění.[159] Není-li takové zadostiučinění dostatečné, má subjekt právo na náhradu nemajetkové újmy v penězích.[160], přičemž výši náhrady určí soud.[161] Po smrti subjektu údajů jeho právo na ochranu osobnosti může uplatnit jeho manžel, partner[162], děti a není-li jich, tak jeho rodiče (tzv. postmortální ochrana).[163]

Odpovědnost podle § 13 ObčZ není vyloučena ani v případě nezletilosti správce, případně jeho omezení či zbavení způsobilosti k právním úkonům, ani v případě tzv. omluvitelného omylu (správce údaje uveřejnil nebo šířil v dobré víře nebo v nevědomosti z lehkomyslnosti). Nejedná-li se o osobní údaje, ale o defamatorní tvrzení týkající se uživatele, původce defamatorních tvrzení se zprostí odpovědnosti, prokáže-li pravdivost těchto tvrzení. Ochrana § 13 ObčZ se uplatní vždy bez výjimek, jedná-li se o zásah do osobního soukromí fyzické osoby ryze intimní včetně jejího rodinného života (v takovém případě (ne)pravdivost tvrzení nehraje roli).[164]

---

153 Ustanovení o povinnostech správce se v tomto ohledu dle § 26 ZoOÚ vztahují i na osoby, které shromáždily osobní údaje neoprávněně.
154 § 21 odst. 1 písm. b) ZoOÚ.
155 § 25 ZoOÚ.
156 § 16, § 42, § 106,§ 415 a násl. ObčZ.
157 § 12, § 373 a násl. obchodního zákoníku, zákon č. 513/1991 Sb., ve znění pozdějších předpisů.
158 § 21 odst. 3 ZoOÚ.
159 § 13 odst. 1 ObčZ.
160 § 13 odst. 2 ObčZ.
161 § 13 odst. 3 ObčZ.
162 Dle zákona č. 115/2006 Sb., o registrovaném partnerství a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.
163 § 15 ObčZ.
164 Blíže viz ŠVESTKA, Jiří a kol.: *Občanský zákoník I. § 1 – 459. Komentář.* 2. vydání. C.H. Beck, Praha 2009, str. 185.

Občanskoprávním prostředkem ochrany osobnosti ve smyslu § 13 ObčZ je žaloba na ochranu osobnosti. V žalobním petitu se lze domáhat, aby soud konstatoval neoprávněný zásah nebo nepravdivost tvrzení. V případě trvalého nebo pokračujícího neoprávněného zásahu lze využít negatorní (tzv. zdržovací) žaloby na upuštění od neoprávněného zásahu (zásah musí být v žalobním petitu dostatečně individualizovaný). Trvají-li následky neoprávněného zásahu (i kdyby zásah již skončil) a je-li možné tyto následky přijatelným způsobem odstranit, lze podat žalobu restituční (tzv. odstraňovací), kde se poškozený bude domáhat odstranění trvajících následků neoprávněného zásahu (např. odstranění fotografie, videozáznamu, kde je poškozený zachycen apod.).

Alternativním řešením je satisfakční žaloba, v jejímž žalobním petitu se bude poškozený domáhat přiměřeného zadostiučinění (tzv. morální satisfakce). Přiměřené zadostiučinění může spočívat v omluvě, odvolání defamatorního výroku, v povinnosti odstranit následky neoprávněného zásahu nebo ve výroku soudu, že k porušení práva na ochranu osobnosti skutečně došlo. Přiměřené zadostiučení určí soud dle okolností případu (charakteru, způsobu, intenzitě, trvání zásahu, atd.).

Nepostačí-li v daném případě přiměřené morální zadostiučinění, přistoupí soud k náhradě nemajetkové újmy v penězích (tzv. materiální satisfakce). Materiální satisfakce se uplatní vždy vzhledem k okolnostem případu a k závažnosti vzniklé újmy. Ustanovení §13 odst. 2 ObčZ demonstrativně uvádí značnou míru snížení důstojnosti fyzické osoby nebo její vážnosti ve společnosti. Není tedy vyloučeno, aby soud přiznal materiální satisfakci i v jiných případech, odůvodňují-li to okolnosti případu. Výše materiální satisfakce je ponechána rozhodnutí soudu, proto v tomto ohledu zákon nestanoví žádné limity.

Kromě žaloby na ochranu osobnosti přichází v úvahu i mimosoudní vyrovnání, smír nebo náhrada škody podle § 16 a § 420 a násl. ObčZ.[165] Výběr občanskoprávního prostředku ochrany osobnosti je v tomto ohledu ponechán poškozenému, který si sám zvolí dle charakteru a intenzity zásahu prostředek ochrany pro něj nejvhodnější.[166]

[165] § 16 ObčZ: „*Kdo neoprávněným zásahem do práva na ochranu osobnosti způsobí škodu, odpovídá za ni podle ustanovení tohoto zákona o odpovědnosti za škodu.*“

[166] Pro srovnání stávající právní úpravy ochrany osobnosti s úpravou, která by měla vstoupit v účinnost od 1.1.2014 viz § 77 a násl. Nového ObčZ.

ii. Veřejnoprávní prostředky ochrany

❖ Správněprávní prostředky ochrany

Jedním z veřejnoprávních prostředků ochrany poškozeného je právo domáhat se, aby byla odpovědná osoba uznána vinnou ze spáchání *správního deliktu* podle hlavy VII ZoOÚ. Podle § 29 odst. 1 ZoOÚ Úřad mimo jiné (i) provádí dozor nad dodržováním zákonných povinností při zpracování osobních údajů, (ii) přijímá podněty a stížnosti na porušení zákonných povinností při zpracování osobních údajů a informuje o jejich vyřízení, (iii) projednává přestupky a jiné správní delikty a uděluje pokuty podle ZoOÚ, ale také (iv) poskytuje konzultace v oblasti ochrany osobních údajů a (v) spolupracuje s obdobnými úřady jiných států, orgány EU a orgány mezinárodních organizací působících v oblasti ochrany osobních údajů.

Subjekt údajů se tedy může se svojí stížností nebo podnětem ohledně porušení zákonných povinností správcem, resp. zpracovatelem, vyplývajících ze ZoOÚ obrátit na Úřad. Zjistí-li Úřad, že k porušení zákonných povinností skutečně došlo, uloží inspektor Úřadu správci, resp. zpracovateli, opatření, která je třeba učinit, aby byly nedostatky zjištěné kontrolou odstraněny a zároveň uloží lhůtu k jejich odstranění. Opatření k nápravě uložené inspektorem Úřadu musí být dostatečně určité a jasné, aby správce, resp. zpracovatel, věděl, co má dělat, aby uložené opatření řádně a včas splnil.[167] Nápravné opatření vyvolá zamýšlený účinek, pokud byl konrolní protokol, jímž bylo opatření uloženo, řádně doručen kontrolovanému.[168] Kontrolovaný může proti nápravnému opatření podat správní žalobu[169]. Splnění nápravného opatření lze na kontrolovaném vymáhat pořádkovými pokutami[170] do výše 25.000,- Kč (lze uložit opakovaně) nebo v rámci exekuce[171].

Pokud inspektor Úřadu uložil opatření v podobě likvidace osobních údajů, jsou osobní údaje až do likvidace blokovány. Proti uložení likvidace může správce podat námitku k předsedovi Úřadu. Do doby, než bude o námitce rozhodnuto, musí být osobní údaje blokovány. Proti rozhodnutí předsedy lze podat žalobu podle předpisů o správním soudnictví. Do doby, než bude soudem rozhodnuto, jsou údaje blokovány. Kontrolovaný je dále povinen ve stanovené lhůtě podat zprávu o přijatých opatřeních. [172]

---

[167] Viz rozsudek Nejvyššího správního soudu sp. zn. 2 As 74/2009 Sb.
[168] Viz rozsudek Nejvyššího správního soudu sp. zn. 1 As 131/2011 Sb.
[169] Dle § 65 odst. 1 soudního řádu správního, zákona č. 150/2002 Sb., ve znění pozdějších předpisů. Správní žaloba by se podávala podle sídla Úřadu, tedy u Městského soudu v Praze.
[170] § 39 odst. 2 ZoOÚ.
[171] Podle hlavy XI správního řádu, zákona č. 500/2004 Sb, ve znění pozdějších předpisů.
[172] § 40 ZoOÚ.

Jednotlivé správní delikty jsou pak upraveny v hlavě VII ZoOÚ, kde jsou rozděleny na správní delikty fyzických a právnických osob. Porušením povinnosti mlčenlivosti se dopustí přestupku fyzická osoba, která (a) je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru, (b) vykonává pro správce nebo zpracovatele činnosti na základě dohody, nebo (c) v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji.[173] Za tento přestupek může Úřad uložit pokutu do výše 100.000,-Kč.[174]

Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů a) nestanoví účel, prostředky nebo způsob zpracování nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona, b) zpracovává nepřesné osobní údaje, c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu, d) uchovává osobní údaje po dobu delší než nezbytnou k stanovenému účelu, e) zpracovává osobní údaje bez souhlasu subjektu údajů (mimo případy uvedené v zákoně), f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, g) odmítne subjektu údajů poskytnout požadované informace, h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů, i) nesplní oznamovací povinnost podle ZoOÚ.[175] Těchto správních deliktů se může dopustit také právnická osoba, u níž je navíc přidána další skutková podstata: „*nevede přehled případů porušení ochrany osobních údajů podle § 88 odst. 7 zákona o elektronických komunikacích*“.[176] Za tento přestupek může Úřad fyzické osobě uložit pokutu do výše 1.000.000,-Kč[177] a právnické osobě pokutu do výše 5.000.000,-Kč[178].

Jak fyzická[179], tak právnická osoba[180] se, jak bylo uvedeno v předchozí kapitole, mohou dopustit přestupku tím, že při zpracování osobních údajů a) ohrozí větší počet osob svým neoprávněným zasahováním do jejich soukromého a osobního života, nebo b) poruší povinnosti pro zpracování citlivých údajů. Za tento přestupek může Úřad fyzické

[173] § 44 odst. 1 ZoOÚ.
[174] § 44 odst. 4 ZoOÚ.
[175] § 44 odst. 2 ZoOÚ.
[176] § 45 odst. 1 ZoOÚ.
[177] § 44 odst. 5 ZoOÚ.
[178] § 45 odst. 3 ZoOÚ.
[179] § 44 odst. 3 ZoOÚ.
[180] § 45 odst. 2 ZoOÚ.

osobě uložit pokutu do výše 5.000.000,-Kč[181] a právnické osobě pokutu do výše 10.000.000,-Kč[182].

Právnická osoba (resp. poskytovatel služeb sociální sítě) za správní delikt neodpovídá, prokáže-li, že vynaložila veškeré úsilí, které bylo možno požadovat k zabránění porušení právní povinnosti. Odpovědnost právnické osoby za správní delikt zanikne, jestliže Úřad o správním deliktu nezahájil řízení do jednoho roku ode dne, kdy se o něm dozvěděl, nejpozději však do tří let ode dne, kdy byl spáchán. Obdobná právní úprava se použije u podnikající fyzické osoby při jejím podnikání nebo v přímé souvislosti s ním.[183]

V prvním stupni správní delikty dle ZoOÚ projednává Úřad, který při rozhodování o výši pokuty přihlíží především k závažnosti, způsobu, době trvání, následkům a okolnostem protiprávního jednání. Udělí-li Úřad pokutu, je povinen ji také vybrat.[184]

❖ Trestněprávní prostředky ochrany

Dalším veřejnoprávním prostředkem ochrany jsou trestněprávní normy stanovící sankce za jejich porušení, tj. pokud pachatel naplní všechny znaky skutkové podstaty, spáchá *trestný čin* (za předpokladu, že tu nejsou dány okolnosti vylučující protiprávnost). Ačkoli se na sociálních sítích může vyskytnout celá řada trestných činů z různých hlav zvláštní části trestního zákoníku[185], zde se v souvislosti s ochranou osobních údajů soustředíme především na hlavu II. (trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství) díl 2. (trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství) trestního zákoníku.

V hlavě II. dílu 2. trestního zákoníku najdeme celkem pět trestných činů. Jako první trestní zákoník uvádí trestný čin *neoprávněné nakládání s osobními údaji*[186]. Základní skutková podstata v odstavci prvním za pachatele označuje toho, „*kdo byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.*“ Druhá základní skutková podstata je uvedena v odstavci druhém, kde se říká, že „*stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že*

[181] § 44 odst. 6 ZoOÚ.
[182] § 45 odst. 4 ZoOÚ.
[183] § 46 odst. 1, 3, 5 ZoOÚ.
[184] § 46 odst. 2, 4, 6, 7 ZoOÚ.
[185] Trestní zákoník, zákon č. 40/2009 Sb., ve znění pozdějších předpisů.
[186] § 180 trestního zákoníku, zákon č. 40/2009 Sb., ve znění pozdějších předpisů.

neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají."

Následujícím trestným činem je *poškození cizích práv*[187], jehož základní skutková podstata spočívá v způsobení vážné újmy na právech tím, že a) pachatel uvede někoho v omyl, nebo b) využije něčího omylu.[188]

Dalším trestným činem je *porušení tajemství dopravovaných zpráv*[189]. Tento úmyslný trestný čin má dvě základní skutkové podstaty. První základní skutková podstata za pachatele označuje toho, „*kdo úmyslně poruší tajemství a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením, b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data*". Podle druhé základní skutkové podstaty pak bude pachatelem ten, „*kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo b) takového tajemství využije*".

Dále sem patří trestný čin *porušení tajemství listin a jiných dokumentů uchovávaných v soukromí*[190], jehož základní skutkovou podstatu naplní ten, „*kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty*".

Posledním trestným činem v tomto díle je *pomluva*[191] spočívající v sdělení nepravdivého údaje o někom jiném. Tento nepravdivý údaj musí být způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu.

---

[187] § 181 tamtéž.
[188] Viz výše uvedený rozsudek Okresního soudu v Liberci ve věci falešného profilu na Facebooku v kapitole 1.7.2. „uživatel sociální sítě".
[189] § 182 tamtéž.
[190] § 183 tamtéž.
[191] § 184 tamtéž.

Trestné činy v tomto díle mají obdobné kvalifikované skutkové podstaty, které obsahují spáchání trestného činu: (i) členem organizované skupiny, (ii) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, (iii) ze zavrženíhodné pohnutky, (iv) vůči jinému pro jeho skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je skutečně nebo domněle bez vyznání, (v) úřední osobou nebo vydáváním se za ni, (vi) v úmyslu získat pro sebe nebo pro jiného značný prospěch/ prospěch velkého rozsahu, (vii) způsobením značné škody / škody velkého rozsahu nebo značné újmy na právech/ újmu na právech velkého rozsahu.

Mezi tresty za trestné činy v tomto dílu můžeme zařadit peněžitý trest, zákaz činnosti a trest odnětí svobody v nejvyšší sazbě až ve výši deseti let.

Stručné shrnutí

V této části diplomové práce jsme se zaměřili na současnou právní úpravu ochrany osobních údajů na sociálních sítích a poukázali jsme na některá specifika, která tuto problematiku provází. Upozornili jsme také na určité v praxi se vyskytující nedostatky, které však současná právní úprava dostatečným způsobem neřeší. Závěrem tedy můžeme konstatovat, že je patrná nezbytnost nové právní úpravy, jenž by byla schopna reflektovat aktuální nevyřešné otázky v souvislosti s technologickým vývojem a proměnou společnosti.

Kapitola 2.

Připravovaná reforma ochrany dat v rámci EU

V předchozích kapitolách jsme se zabývali současnou právní úpravou ochrany osobních údajů a ukázali jsme si, že vykazuje mnohé nedostatky, které je třeba odstranit. Těchto nedostatků si je vědoma také Evropská komise, která dva roky připravovala celoevropskou reformu ochrany osobních údajů. Návrh této reformy Evropská komise prezentovala 25. ledna 2012. V této části diplomové práce se proto v kapitole první podíváme na okolnosti a důvody, jenž k přípravě reformy vedly, a dále na účel a cíle této reformy. V druhé kapitole nastíníme aktuální znění předloženého návrhu reformy. V třetí kapitole se zaměříme na reakce, které předložený návrh reformy vyvolal, ať již v kruzích politických, obchodních či právních.

2.1 Potřeba reformy

V předchodchozích kapitolách jsme poukázali na nedostatky současné právní úpravy ochrany osobních údajů. Tyto nedostatky se projevují mimo jiné u souhlasu subjektu údajů se zpracováním dat, v informovanosti subjektu a časté netransparentnosti zpracování osobních údajů, mnohdy problematické vymahatelnosti ochrany a především v úpravě likvidace dat a jejich kompletním odstranění nejen ze sociálních sítí, ale také z jiných datových nosičů a internetových serverů.

Základ dnešní evropské právní úpravy ochrany osobních údajů byl položen v 90. letech přijetím a následnou implementací Směrnice 95/46/ES do právních řádů členských států EU. Přestože existoval společný evropský základ úpravy ochrany osobních údajů, každý členský stát si při implementaci směrnice vytvořil do jisté míry vlastní právní úpravu a akcentoval různé její principy a pravidla. Výsledkem tohoto procesu je dnešních 27 více či méně podobných právních úprav ochrany osobních údajů.

Od poloviny 90. let, kdy byla Směrnice 95/46/ES přijata, se však mnohé změnilo. Nejvýraznější změnou se stalo rozšíření a masové užívání internetu a sociálních sítí díky drastickému rozvoji technologií a globalizace. Tento trend přinesl nesmírné komunikační možnosti, snadný přístup k nezměrnému množství informací díky důmyslným

internetovým vyhledávačům a v podstatě neomezený prostor pro ukládání dat. Technologie a nové komunikační možnosti proměnily společnost.

Lidé však začali ve stále větší míře sdílet své osobní údaje na internetu. Podle průzkumu Eurobarometru[192] se 74% Evropanů domnívá, že odhalování jejich osobních údajů je stále více součástí moderního života. Nejdůležitějším důvodem pro odhalení, resp. zpřístupnění osobních údajů se podle Eurobarometru ukázal být přístup k internetových službám, jak pro užívání sociálních sítí, tak pro nakupování online (79%). U uživatelů sociálních sítí je vyšší pravděpodobnost, že odhalí své jméno (79%), fotografie (51%) a národnost, resp. státní příslušnost (47%). Pouhá čtvrtina uživatelů sociálních sítí cítí naprostou kontrolu nad svými osobními údaji. Jenom třetina Evropanů si je vědoma, že v jejich zemi existuje státní úřad pro ochranu jejich práv k osobním údajům. Pouze pětina uživatelů důvěřuje internetovým společnostem jako jsou internetové vyhledávače, sociální sítě a služby emailu. 70% Evropanů má obavy, že jsou jejich osobní údaje svěřené společnostem užívány k jinému účelu, než k němuž byly shromážděny. 75% Evropanů chce odstranit své osobní údaje na webové stránce kdykoli se rozhodnou tak učinit. Přestože se většina evropských uživatelů internetu cítí odpovědná za to, aby sami bezpečně zacházeli se svými osobními údaji, 90% Evropanů je pro rovná práva ochrany osobních údajů napříč EU.

Jak vidíme z průzkumu Eurobarometru, je zjevné, že většina Evropanů pociťuje nedostatek ochrany jejich osobních údajů v internetovém prostředí, nedůvěřuje internetovým společnostem a chce posílit a sjednotit jejich práva na ochranu osobních údajů v celé EU.

Viviane Reding, vice-prezidentka Evropské Komise pro spravedlnost, základní práva a občanství, připomíná[193], že data se stala měnou dnešní moderní digitalizované ekonomiky. Avšak aby tato měna mohla být řádně využita k inovacím, růstu a konkurenceschopnosti, je třeba ji chránit, posílit její stabilitu a důvěru uživatelů v ochranu jejich osobních údajů. Proto potřebujeme reformu ochrany osobní údajů.

---

[192] *Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union.* Zpráva publikována v červnu 2011. Dostupné na: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (22.11.2012).

[193] Viz přednáška Viviane Reding na téma *The importance of strong data protection rules for growth and competitiveness.* Přednáška z 01.03.2012, Shaw Library, Old Building, The London School of Economics and Political Science. Dostupné na: http://www2.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLecturesAndEvents/player.aspx?id=1379 (21.11.2012).

Evropská komise tedy připravila návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem takových údajů (Obecné nařízení o ochraně údajů), který představila dne 25. ledna 2012, a zároveň návrh směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů. Dále se budeme zabývat pouze Obecným nařízením o ochraně údajů (Nařízení).

Účelem Nařízení je posílit ochranu osobních údajů v EU a zajistit subjektům údajů kontrolu nad jejich osobními údaji, tak aby k nim měli přístup, mohli je volně přesouvat a smazat, pokud budou chtít. Subjekty údajů by měly být okamžitě informovány o ztrátě, krádeži nebo napadení jejich osobních údajů. Nařízení by mělo také usnadnit přeshraniční tok dat a především sjednotit ochranu osobních údajů v celé EU. Nařízení by se tak mělo stát po Směrnici 95/46/ES dalším významným evropským milníkem ochrany osobních údajů. Výhodou nařízení je jeho přímá aplikovatelnost v celé EU bez potřeby další implementace do národních právních řádů (oproti směrnici, která musí být dále implementována do jednotlivých právních řádů členských států, což může trvat až několik let od jejího přijetí, a ani po jejím implementování nelze zajistit zcela jednotnou a konsistentní právní úpravu ve všech členských státech).

Evropská komise od Nařízení očekává, že kromě posílení ochrany osobních údajů také usnadní podnikání na společném evropském trhu, sníží náklady podnikatelům na související právní služby a na administrativu. Podnikatelé se tak nebudou muset zabývat 27 právními úpravami jednotlivých členských států, ale pouze jednou úpravou a jednat s jedním úřadem pro ochranu osobních údajů pro celou EU. Viviane Reding tuto koncepci nazývá „*one-stop shop*“, takže podnikatelé budou jednat s úřadem pro ochranu osobních údajů toho členského státu, kde mají sídlo, resp. kde jsou usazeni. Nařízení by tak mělo harmonizovat fragmentovanou evropskou právní úpravu dat.

2.2 Nástin reformy

Návrh Nařízení je založen na článku 16 SFEU[194], který tvoří právní základ pro přijetí pravidel ochrany osobních údajů zavedený Lisabonskou smlouvou[195]. Nařízení vychází z principů a základních pravidel Úmluvy č. 108 a Směrnice 95/46/ES, kterou má nahradit a vytvořit tak jediný soubor pravidel pro ochranu údajů platný v celé EU. Návrh Nařízení v úvodních ustanoveních odůvodňuje nutnost přijetí nové právní úpravy a to ve formě nařízení a dále odkazuje na článek 8 Chartu základních práv EU[196], tj. právo na ochranu osobních údajů.

Předmětem Nařízení se má stát ochrana fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů. Cílem Nařízení má být ochrana základních práv a svobod fyzických osob a především jejich práva na ochranu osobních údajů. Nařízení se má vztahovat jak na zcela nebo částečně automatizované, tak na neautomatizované (tzn. manuální) zpracování osobních údajů. Věcná působnost Nařízení stanoví několik výjimek, na než se Nařízení nebude vztahovat.[197] Mezi tyto výjimky patří „*zpracování osobních údajů prováděné fyzickou osobou, které má výlučně osobní či domácí povahu a které se neprovádí za účelem zisku*". Zde vidíme zajímavou změnu oproti stávající právní úpravě. Nařízení tuto výjimku rozšiřuje o podmínku „*zpracování se neprovádí za účelem zisku*", která se spolu s druhou podmínkou této výjimky uplatní kumulativně. Nařízení tak zúží rozsah aplikovatelnosti této výjimky.

Nařízení se má vztahovat na zpracování osobních údajů v rámci činností provozovny správce nebo zpracovatele v EU. Nařízení by se také mělo vztahovat na zpracování osobních údajů subjektů údajů, které mají bydliště v EU, správcem, který není usazen v EU, pokud zpracování souvisí s nabízením zboží nebo služeb subjektům údajů v EU, nebo sledováním chování subjektu údajů EU. Nařízení by se dále mělo aplikovat na zpracování osobních údajů správcem, který není usazen v EU, ale na místě, kde se vnitrostátní právní předpisy členského státu uplatňují na základě mezinárodního práva veřejného. Oproti Směrnici 95/46/ES by tak Nařízení podstatným způsobem rozšířilo věcnou působnost dnešní právní úpravy ochrany osobních údajů.

---

[194] Smlouva o fungování Evropské unie, Úřední věstník C 83 ze dne 30.03.2010 (do 30.11.2009 pod názvem Smlouva o založení Evropského společenství).
[195] Lisabonská smlouva, Úřední věstník C 306 ze dne 17.12.2007.
[196] Blíže viz kapitola 1.2, str. 7 dole.
[197] Viz čl. 2 odst. 2 Nařízení.

Návrh Nařízení obsahuje, podobně jako Směrnice 95/46/ES, řadu definic souvisejících s ochranou osobních údajů.[198] Návrh Nařízení stávající definice ze Směrnice 95/46/ES nejen přebírá a místy upravuje, ale zároveň přichází s definicemi novými[199]. Klíčový pojem „*osobní údaje*" návrh Nařízení popisuje jako „*veškeré informace o subjektu údajů*". Nadále by tato definice tedy nevyžadovala určitelnost subjektu údajů na základě takové informace, jako je tomu dnes. Návrh Nařízení totiž tuto „*určitelnost*" z dnešní definice osobních údajů převzal do navrhované definice subjektu údajů. Návrh Nařízení také podrobněji definuje „*souhlas subjektu údajů*", kdy by nadále nestačil dnešní svobodný a vědomý souhlasný projev vůle subjektu údajů se zpracováním osobních údajů, ale tento souhlas by musel být také konkrétní, jednoznačný a především výslovný, v čemž tkví zásadní změna oproti dnešní úpravě. Nařízení by také mělo posílit tzv. minimalizaci dat, kdy by data mohla být shromažďována a uchována pouze tehdy, pokud účel zpracování nemohl být naplněn jinými prostředky.

Nařízení by na jedné straně mělo zrušit některé povinnosti správce (např. povinnost oznámit Úřadu zpracování osobních údajů), na druhé straně by mělo správci uložit celou řadu nových povinností (např. povinnost jmenovat zvláštního inspektora ochrany údajů pro podniky zaměstnávající více jak 250 osob). Nařízení by mělo zavést transparentnější zpracování osobních údajů, snadno dostupná pravidla pro jejich zpracování a výkon práv subjektů údajů. Správce by byl povinen poskytnout subjektu údajů všechny informace o zpracování osobních údajů subjektu údajů ve srozumitelné, jasné formě užívající běžného jazyka. Dále jsou kladeny zvláštní požadavky na zpracování osobních údajů dětí mladších 13 let, včetně povinnosti schválení souhlasu rodičem, resp. zákonným zástupcem dítěte. Nařízení by nově zavedlo povinnost správce ohlásit orgánu dozoru, že došlo k narušení bezpečnosti osobních údajů, a to nejpozději do 24 hodin od chvíle, kdy se správce o narušení dozví.

Nařízení by mělo dále zjednodušit předávání osobních údajů mimo EU vzhledem k tomu, že se bude uplatňovat jednotná právní úprava a postup upravující tuto otázku. Předávání dále bude možné do zemí, které Evropská komise označí jako bezpečné pro předávání, nebo na základě zvláštního povolení. Výhodou je také, že správce by musel

[198] Viz čl. 4 Nařízení.

[199] Nové definice: narušení bezpečnosti osobních údajů, genetické údaje, biometrické údaje, údaje o zdravotním stavu, hlavní provozovna, zástupce, podnik, skupina podniků, závazná podniková pravidla, dítě, orgán dozoru.

jednat pouze s jedním úřadem pro ochranu osobních údajů, kterým by byl úřad v členském státě EU, kde má správce sídlo.

Nařízení by nově zavedlo právo subjektu údajů na přenositelnost údajů, tzn. právo na předávání údajů z jednoho automatizovaného systému zpracování do jiného, aniž by tomu správce mohl zabránit. Předpokladem výkonu tohoto práva je právo subjektu obdržet od správce předmětné údaje ve strukturovaném a běžně používaném elektronickém formátu. Z toho vyplývá, že by Nařízení umožnilo uživatelům získat od poskytovatele služeb sociální sítě všechny informace z osobního účtu uživatele a volně je přenést například na jinou sociální síť. Lze předpokládat, že toto opatření by uvítali zejména ti uživatelé, kteří jsou nespokojeni se službami jejich sociální sítě, ale nechtějí z ní odstranit svůj osobní účet právě kvůli ztrátě dat, která by následovala.

Nařízení by upravilo právo subjektu údajů na opravu nepřesných údajů, které se ho týkají. Významnou změnou by oproti stávající úpravě bylo zakotvení práva být zapomenut a práva na výmaz.[200] Subjekt údajů by měl právo požadovat od správce výmaz osobních údajů subjektu a zdržení se dalšího šíření těchto údajů. Pokud by správce tyto údaje zveřejnil, byl by povinen přijmout (vzhledem k údajům, za něž je odpovědný) veškerá rozumná opatření, včetně opatření technických, aby informoval třetí strany zpracovávající tyto údaje o tom, že se subjekt údajů dožaduje jejich vymazání, včetně všech odkazů na tyto údaje, kopií a replik údajů. Povolil-li správce zveřejnění osobních údajů třetí straně, sám za ně ponese odpovědnost. Správce by byl povinen neprodleně výmaz provést.[201] Zavedení práva být zapomenut bude jistě vítaným opatřením (alespoň ze strany uživatelů sociálních sítí) a doufejme, že opravdu pomůže vypořádat se se současnými riziky ochrany osobních údajů v internetovém prostředí. Zda bude takové opatření úspěšné prokáže až praxe.

Nařízení by dále posílilo výkon práv subjektu údajů. Například by zavedlo lhůty k poskytnutí informací správcem subjektu údajů. Poskytnutí informací by bylo bezplatné. V případě správcova odmítnutí informace poskytnout by byl správce povinen informovat subjekt údajů o možnosti podat stížnost orgánu dozoru a uplatnit soudní opravné prostředky ochrany.

Návrh Nařízení rozšiřuje správcovu odpovědnost za škodu a ukládá členským státům povinnost stanovit pravidla pro ukládání sankcí podle Nařízení včetně zajištění

---

[200] Tzv. right to be forgotten založené na myšlence Viktora Mayer-Schönbergera (viz jeho kniha *Delete – The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009).

[201] Samozřejmě z tohoto pravidla existují určité výjimky (obdobné těm dnešním) – viz čl. 17 odst. 3 a násl. Nařízení.

jejich provádění. Za nejzávažnější porušení ochrany osobních údajů návrh Nařízení navrhuje správci uložit stupňovité pokuty až do výše 2% světového obratu správce. Oproti dnešním relativně velmi nízkým pokutám[202] by nově zaváděná výše pokut pro správce měla být dostatenčným impulsem k tomu, aby správce měl ekonomický zájem na dodržování právní úpravy ochrany osobních údajů. Důležitá by v tomto ohledu byla také vzájemná přeshraniční spolupráce úřadů na ochranu osobních údajů.

Nařízení specifikuje právní prostředky ochrany. Subjekt údajů by kromě stížnosti orgánu dozoru měl možnost domáhat se jednání orgánu dozoru o jeho stížnosti soudním opravným prostředkem. Nově by Nařízení upravilo možnost výběru místní příslušnosti soudu: (i) stát, v němž je žalovaný usazen, nebo (ii) stát, kde má subjekt údajů bydliště. Tato možnost výběru by mimo jiné posílila ochranu práv uživatelů sociálních sítí, kdy by nadále nemuseli řešit soudní spory proti poskytovateli ve státě poskytovatelem určeném (v případě největších poskytovatelů jako např. Facebook, LinkedIn či Google+ ve státě Kalifornie, USA), ale ve státě svého bydliště. Návrh Nařízení dále stanoví společná pravidla pro soudní řízení včetně práv zúčastněných stran.

Nařízení by zřídilo nezávislou Evropskou radu pro ochranu údajů (Rada), kterou by tvořily orgány dozoru z každého členského státu a evropský inspektor ochrany údajů. Rada by nahradila tzv. Pracovní skupinu 29, zřízenou článkem 29 Směrnice 95/46/ES. Evropská komise by měla právo být v Radě zastoupena.

2.3 Ohlasy na reformu

Návrh Nařízení připravený Evropskou komisí byl po svém uveřejnění 25. ledna 2012 rozeslán členským státům a vybraným institucím k připomínkování. V současnosti návrh Nařízení čeká na první čtení v Evropském parlamentu. V této kapitole se zaměříme na odezvu, kterou toto Nařízení vyvolalo, a to nejen v politických kruzích.

[202] Blíže viz správněprávní prostředky ochrany v kapitole 1.7.4. ii. Podle ZoOÚ dosahuje nejvyšší pokuta částky 10.000.000,-Kč. Zvážíme-li však obrat obrovských nadnárodních společností (např. Facebook), i tato dnešní maximální výše pokuty se zdá být směšná.

Jarní konference 2012 evropských komisařů pro ochranu osobních údajů[203] návrh Nařízení uvítala s tím, že návrhy adresují nové výzvy pramenící z všudypřítomného shromažďování a užívání osobních údajů v propojeném a globalizovaném světě. Komisaři jsou spokojeni především s (i) pravidly poskytujícími více transparentnosti a větší kontrolu nad zpracováním dat, (ii) se zakotvením principu minimalizace dat, (iii) více možnostmi pro odškodnění subjektů údajů, (iv) posílením pravidel ohledně práva na přístup k datům a práva na námitky, (v) zařazením práv za účelem adresování výzev vyvstávajích z internetového prostředí (zvláštní ochrana dětí, právo být zapomenut a nové právo přenositelnosti dat), (vi) snahou zavést zjednodušená a konzistentní pravidla pro správce dat, (vii) zavedením principu odpovědnosti, (vii) představením mechanismů a nástrojů sloužících jako podněty projevu odpovědnosti jako je záměrné přednastavení ochrany dat, jmenování komisaře pro ochranu dat a povinnosti oznámení, že došlo k narušení bezpečnosti dat, (viii) zavedením tzv. koncepce *one-stop shop* jak pro správce tak pro subjekty údajů a (ix) požadavkem vzájemné spolupráce úřadů pro ochranu osobních údajů, posílení jejich nezávislosti a pravomocí, včetně správních pokut.

Komisaři upozorňují, že je důležité, aby koncepce Nařízení zůstala konzistentní a varují před rizikem oslabení účinnosti aplikace Nařízení prostřednictvím velkého množství výjimek a derogací. Výjimky musí být v souladu s klíčovými aspekty práva na ochranu osobních údajů. Základní pravidla musí být aplikována konzistentně bez ohledu na oblast jejich užití.

Připravovanou reformu vítá také European Social Networks Group (Evropská skupina sociálních sítí, tzv. ESNG). ESNG oceňuje především harmonizaci práva na ochranu osobních údajů v EU jako významný milník na cestě k větší rovnosti soutěže a příležitostí. Zvláštní důležitost ESNG přikládá aplikovatelnosti práva i na poskytovatele sociálních sítí, kteří nejsou z EU, ale poskytují služby sociálních sítí občanům EU. ESNG to považuje za základní prerekvizitu rovné soutěže a náležité ochrany uživatele. ESNG v tomto ohledu připomíná, že právě kvůli nedostatečné místní působnosti současné úpravy získali mimoevropští poskytovatelé služeb sociálních sítí (především ti z USA) soutěžní výhodu na úkor ochrany uživatele.

[203] Viz *Resolution on European data protection reform*. Jarní konference 2012 evropských komisařů pro ochranu dat, Lucemburk, 03.-04.05.2012. Dostupné na: http://www.springconference2012.lu/files/7/3/document_id29.pdf (21.11.2012).

ESNG je proti tomu, aby návrhovaná úprava byla přijata jako nařízení opravňující Evropskou komisi přijímat nelegislativní akty s obecnou působností. Dle ESNG to odporuje článku 290 SFEU[204], podle něhož je taková úprava možné pouze, je-li to nezbytné pro „*některé prvky legislativního aktu, které nejsou podstatné*".

ESNG vidí jako pozitivní krok také nově zaváděné právo subjektu údajů na přenositelnost dat, avšak příslušné ustanovení návrhu Nařízení považuje za vágní a nejednoznačné. Proto ESNG doporučuje, aby bylo toto právo přesně definováno, nebyla umožněna přenositelnost dat mezi jednotlivými správci, ale výlučně ve vztahu správce-subjekt údajů a nebyly povoleny žádné výjimky. Výjimky z tohoto pravidla by dle ESNG znevýhodnily ostatní poskytovatele a narušily základy hospodářské soutěže.

Za vágní považuje ESNG také ustanovení o právu být zapomenut. Podle ESNG je nejasný rozsah tohoto práva. Navíc by jeho technická realizace byla komplikovaná a v rámci příspěvků uživatele v některých fórech a skupinách by mohlo její odstranění vyvolat kontextuální nesrozumitelnost sdělené informace. ESNG kritizuje také vysoké pokuty za porušení práva na ochranu osobních údajů, což nás jistě nepřekvapí vzhledem k tomu, že ESNG reprezentuje právě poskytovatele služeb sociálních sítí, jimž by tyto pokuty mohly být uloženy.

Rozporuplné reakce reforma vyvolala také u členských států EU.[205] Některé státy nesouhlasí s tím, aby byl předložený návrh přijat ve formě nařízení a uvádí, že by postačila směrnice (např. Belgie, UK), zatímco jiné (např. Itálie) formu nařízení silně podporují. Časté výhrady se objevují v souvislosti s tím, že Nařízení příliš spoléhá na delegaci pravomoci Nařízení pozměnit či jinak upravit na Evropskou komisi (např. Belgie, Francie, UK). Pochyby se vyskytly také u práva být zapomenut (např. Francie). Byla položena otázka, zda jsou data opravdu odstraněna nebo jestli je pouze odstraněn přístup k nim.[206] Byla položena otázka, jak právo být zapomenut souvisí se sociálními sítěmi vzhledem k tomu, že Nařízení neupravuje zveřejnění osobních údajů třetími stranami.[207]

---

[204] Smlouva o fungování Evropské unie, Úřední věstník C 83 ze dne 30.03.2010 (do 30.11.2009 pod názvem Smlouva o založení Evropského společenství).

[205] Viz *Komentáře členských států EU k Obecnému nařízení o ochraně údajů.* Zn. 9897/2/12 REV 2, 2012/0011 (COD), Rada EU, Brusel, Belgie, 18.07.2012. Dostupné na: http://www.statewatch.org/news/2012/jul/eu-council-dp-reg-ms-positions-9897-rev2-12.pdf (19.11.2012).

[206] Je to velmi dobrá otázka. Domníváme se však, že z příslušného ustanovení je patrné, že autoři návrhu Nařízení zamýšleli odstranit samotná data a nejen přístup k nim. Aby se však do budoucna předešlo podobným diskuzím, bylo by vhodné toto ustanovení blíže specifikovat a vyloučit tak případné nejasnosti.

[207] Zde si dovolíme nesouhlasit. Zveřejnění osobních údajů je jednou z forem zpracování. Zpracovává-li data třetí osoba – stanoví vždy účel a prostředky nakládání s daty, (neuplatní-li se příslušné výjimky) stane se

Znepokojení bylo vyjádřeno ohledně administrativní a finanční zátěže na podnikatele, ať už se jedná o povinnost podnikatele zaměstnávajícího více jak 250 osob mít pověřeného zaměstnance na správu osobních údajů; nebo požadavek oznámení o narušení bezpečnosti ochrany osobních údajů do 24 hodin, kdy se lhůta pro splnění tohoto požadavku zdála být příliš krátká (např. UK, Lichtenštejnsko). Byla vznesena také pozoruhodná otázka ohledně aplikace práva. Nařízení je totiž klasifikováno jako „pouze pro Schengenský prostor", jehož součástí však UK ani Irsko nejsou. Znamenalo by to tedy, že by se na ně Nařízení nevztahovalo.

Česká republika (ČR) vítá návrh Nařízení, které by harmonizovalo právní úpravu ochrany osobních údajů v celé EU. ČR má však výhrady k formě nařízení. ČR se domnívá, že by v nařízení měla pouze nezbytná opatření a podrobnější úprava by měla být přijata prostřednictvím směrnice, kterou by členské státy měly možnost implementovat podle potřeb jejich právních řádů. Česká republika zastává názor, že některá ustanovení návrhu Nařízení je třeba blíže specifikovat, aby tak nedocházelo k nejasnostem při jejich pozdější interpretaci.

American Chamber of Commerce (Americká obchodní komora, tzv. AmCham) schvaluje snahy Evropské komise vytvořit jedno aplikovatelné právo ve všech 27 členských státech.[208] AmCham připomíná, že současné prostředí vytváří právní a obchodní nejistotu. Dále uvádí, že pravomoci dozorových orgánů musí být blíže specifikovány. AmCham požaduje, aby nová úprava byla dostatečně flexibiní a schopna se přizpůsobit potřebám jednotlivých odvětví. Doporučuje přepracovat právo být zapomenut, přenositelnost dat a záměrnou přednastavenou ochranu dat vzhledem k tomu, že v současné podobě jsou tato pravidla příliš normativní. AmCham kritizuje odpovědnost správce za smazání dat i u třetích stran, povinnost informovat subjekt údajů o narušení bezpečnosti dat do 24 hodin a excesivně vysoké pokuty za porušení Nařízení. AmCham má také výhrady k úpravě

správcem nebo zpracovatelem. Jsme toho názoru, že měl-li tento argument směřovat proti uživatelům sociálních sítí uveřejňujících osobní údaje jiných osob, původce tohoto argumentu si neuvědomil, že na tyto uživatele v takovém případě zpravidla pohlížeme jako na správce (samozřejmě neuplatní-li se výjimka zpracování výlučně pro osobní potřebu, která se však v prostředí sociálních sítí aplikuje spíše výjimečně – viz rozhodnutí ESD ve věci *Lindqvist*).

[208] Viz *AmCham EU position on the General Data Protection Regulation.* American Chamber of Commerce to the European Union. 11.07.2012.
Dostupné na: http://www.cnpd.public.lu/fr/actualites/national/2012/07/Fedil-reforme/AmCham_EU_-_Position_Paper_on_Data_Protection_20120711.pdf (24.11.2012).

přeshraničního pohybu dat. AmCham vítá zvláštní pravidla zpracování dat dětí a především jasně danou horní věkovou hranici 13 let pro jejich aplikaci.

Doufejme, že reforma ochrany osobních údajů v EU bude úspěšná a podaří se ji co nejdříve přivést v účinnost. Je však třeba, aby byly zachovány její základní principy a s nimi i konzistentnost reformy. Byla by škoda, kdy kvůli silné lobby nebo partikulárním zájmům jednotlivých činitelů došlo k narušení samotné podstaty reformy. Domníváme se, že nejefektivnější formou přijetí reformy by bylo jednoznačně nařízení. Obáváme se, jaké důsledky by mělo přijetí ve formě „pouhé" směrnice. Nechť je nám předchozí Směrnice 95/46/ES příkladem toho, jak se výsledná právní úprava může rozmělnit, když je implemetována do 27 různých právních řádů různými právními autoritami, kdy každá vnímá pojetí nové úpravy rozdílně. Za vhodné nepovažujeme ani návrh ČR spočívající v kombinaci nařízení a směrnice a to z obdobných důvodů. Je třeba mít také na paměti, že trvá mnohem déle, než se podaří úvést v účinnost směrnici ve všech státech EU než je tomu u nařízení.

Velkým přínosem předloženého návrhu Nařízení je jeho aplikovatelnost také na mimoevropské správce poskytující služby občanům EU. V prostředí sociálních sítí by se tak vyřešil problém s místní působností práva, kdy největší poskytovatelé sídlí na území USA, poskytují služby sociálních sítí evropským uživatelům, avšak smluvně volí americké právo a soudní příslušnost.

Předložený návrh Nařízení jistě dozná ještě mnohých změn před jeho finální podobou. Jisté úpravy současného návrhu Nařízení se zdají být nezbytné především vzhledem k potřebě blíže upřesnit některá ustanovení návrhu Nařízení, aby se předešlo případným budoucím interpretačním rozporům. Vítáme zejména podrobnější úpravu likvidace dat, zakotvení práva být zapomenut a právo přenositelnosti údajů, což považujeme oproti dnešnímu nevyhovujícímu stavu ze velmi přínosnou a podstatnou změnu nejen pro uživatele sociálních sítí, ale také pro ostatní uživatele internetu.

Jak vidíme, harmonizace právní úpravy ochrany osobních údajů v EU má před sebou ještě dlouhou cestu k jejímu konečnému schválení. Zdá se, že legislativní proces by mohl trvat ještě dva roky, než bude dokončen. Nesmíme však zapomenout, že bude třeba zahrnout také potřebný čas, než Nařízení vstoupí v účinnost. V případě, že by návrh Nařízení byl nakonec přijat ve formě směrnice, trvalo by ještě déle, než bude

implementována do právních řádů jednotlivých členských států. Bohužel se tak zdá, že půjde-li všechno hladce bez větších komplikací a bude-li návrh schválen ve formě Nařízení, účinné nové právní úpravy se nedočkáme dříve než v roce 2015.

Stručné shrnutí

V této části diplomové práce jsme se podívali na důvody, proč je potřeba reformovat ochranu osobních údajů v EU, nastínili jsme nejdůležitější změny v předloženém návrhu Nařízení a ukázali jsme si, jaké reakce návrh vyvolal. Podle ohlasů na předložený návrh Nařízení lze očekávat, že návrh bude nakonec přijat. Otázkou zůstává, v jaké formě a jaké bude jeho finální znění. Doufejme, že základní koncepce a klíčové změny představené návrhem Nařízení se zachovají a návrh si tak uchová svoji konzistenci. Zda byla reforma úspěšná a poskytla adekvátní řešení stávajících problémů však prokáže až praxe.

ZÁVĚR

Cílem této diplomové práce bylo popsat současnou právní úpravu ochrany osobních údajů na sociálních sítích se zaměřením na likvidaci osobních údajů a poukázat na její případné nedostatky, které se v prostředí sociálních sítí projevují. Dalším záměrem bylo zvážit, zda existují důvody pro přijetí nové právní úpravy, a představit připravenou reformu ochrany osobních údajů Evropské komise a její návrh Nařízení, jenž by mělo harmonizovat ochranu osobních údajů v celé EU.

V první kapitole jsme poukázali na to, že soukromí je v případě sociálních sítí spíše iluzorním pojmem a na příkladech jsme se přesvědčili, jak nebezpečné je tomuto dojmu podlehnout. Připomněli jsme, že nejlepší ochranou našeho soukromí je prevence. To, co o sobě nezveřejníme, nebudeme muset následně složitě odstraňovat. Upozornili jsme také na technicky i právně problematické, mnohdy nemožné, kompletní odstranění jednou zveřejněných osobních údajů nejen ze sociálních sítí, ale také z databází a datových nosičů správce a internetových vyhledávačů.

Zaměřili jsme se také na nerovný právní vztah poskytovatele služeb sociální sítě a uživatele založený na adhezních inominátních smlouvách. Zásadním problémem je v tomto ohledu především místní působnost práva a soudní příslušnost (často v USA), minimum práv uživatele, nesrozumitelné smluvní podmínky, netransparentnost zpracování osobních údajů a neefektivní právní prostředky ochrany uživatele spolu s problematickou vymahatelností práv uživatelů vůči poskytovatelům.

Důkladnou analýzou této problematiky jsme zjistili, že její nedostatky jsou mnohem komplexnějšího rázu, než jsme předpokládali. Došli jsme k závěru, že současná právní úprava není schopna efektivně řešit aktuální právní problémy vznikající v prostředí internetu, resp. sociálních sítí. Je tedy zjevné, že reforma stávající úpravy je nevyhnutelná.

Tyto nedostatky si uvědomuje také Evropská komise, která počátkem letošního roku představila návrh celoevropské reformy ochrany osobních údajů. Návrh, který rozebíráme v kapitole druhé, obsahuje řadu nových, v praxi opravdu potřebných práv, jako je právo přenositelnosti osobních údajů nebo právo být zapomenut. Návrh nejen posiluje práva subjektů údajů a pravomoci úřadů na ochranu osobních údajů, ale také odpovědnost správce. Velkým přínosem návrhu je také úprava místní působnosti práva, kdy by se nově vztahovala evropská právní úprava i na mimoevropské správce, kteří poskytují služby na území EU. Tím by se vyřešil současný problém, kdy se právní vztahy největších správců-

poskytovatelů služeb sociální sítě řídí často americkým právem doporovázeným americkou soudní příslušností, což představuje zásadní překážku vykonatelnosti práva pro evropské uživatele sociálních sítí. Neměli bychom opomenout také navrhované výrazné zvýšení správních pokut za porušení této úpravy, které by oproti dnešním relativně velmi nízkým pokutám měly účinně působit jako silný ekonomický podnět pro důsledné dodržování práva správci.

Návrh Evropské komise považujeme ze velmi přínosný pro řešení nedostatků současné právní úpravy a pevně věříme, že bude v dohledné době nakonec přijat. Doufáme, že podstata výše popsaných změn, které návrh představil, se i přes jejich kritiku a lobbying správců zachová a bude úspěšně uvedena v život. Z našeho pohledu je však návrhu třeba vytknout místy určité nepřesnoti působící interpretační rozpory. Na základě naší analýzy návrhu a jeho důvodové zprávy jsme dospěli k závěru, že některá ustanovení návrhu mohou působit bez předchozího seznámení se s jeho důvodovou zprávou nejednoznačně. Soudíme proto, že návrh příliš spoléhá na svoji důvodovou zprávu. Za vhodnější považujeme využití důvodové zprávy při další specifikaci nejasných ustanovení návrhu.

Závěrem bychom chtěli konstatovat, že dle našeho názoru byly vymezené cíle této diplomové práce úspěšně naplněny. Potěšilo by nás, kdyby předkládaná diplomová práce našla své čtenáře a inspirovala je k dalšímu studiu sociálních sítí, nebo jim alespoň umožnila vnímat problematiku sociálních sítí v novém světle.

SEZNAM ZKRATEK

AmCham .....
American Chamber of Commerce (Americká obchodní komora)

ESNG .....
European Social Networks Group (Evropská skupina sociálních sítí)

LZPS nebo **Listina** .....
Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů

Obecné nařízení o ochraně údajů nebo **Nařízení** .....
Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem takových údajů (Obecného nařízení o ochraně údajů) ze dne 25. ledna 2012

ObčZ .....
Občanský zákoník, zákon č. 40/1964 Sb., ve znění pozdějších předpisů

Nový ObčZ .....
Občanský zákoník, zákon č. 89/2012 Sb.

Směrnice 95/46/ES .....
Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Směrnice 2000/31/ES .....
Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých právních apektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu

Směrnice 2002/58/ES .....
Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronických komunikací

Směrnice 2006/24/ES .....
Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

SNS .....
Sociální síť (z angl. originálu: „*social networking site*“)

Úmluva č. 108 .....
Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108. Přijata Radou Evropy ve francouzském Štrasburku dne 28. ledna 1981. Platila od 1. října 1985, přičemž pro ČR vstoupila v platnost až od 1. listopadu 2001, kdy byla publikována pod č. 115/2001 Sb.m.s.

Úřad .....
Úřad pro ochranu osobních údajů, zřízený zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů

ZoOÚ .....
Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, ze dne 4. dubna 2000

BIBLIOGRAFIE

Použitá literatura

1. BARTÍK, Václav; JANEČKOVÁ, Eva: *Zákon o ochraně osobních údajů s komentářem*. 1. vydání. ANAG, Olomouc 2010
2. BARTÍK, Václav; JANEČKOVÁ, Eva: *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8. 2012*. 1. vydání. ANAG, Olomouc 2012
3. BOYD, Danah M.; ELLISON, Nicole B.: *Social Network Sites: Definition, History, and Scholarship*. Journal of Computer-Mediated Communication, Vol. 13, No. 1, 2007 Dostupné na: http://www.danah.org/papers/JCMCIntro.pdf (01.11.2012)
4. DE MIGUEL ASENSIO, Pedro Alberto: *Social Networking Sites: An Overview of Applicable Law Issues*. Annali italiani del diritto d´autore, della cultura e dello spettacolo (AIDA), Vol. XX, 2011. Dostupné na: http://eprints.ucm.es/13376/1/pdemiguelasensio-AIDA2011.pdf (12.11.2012)
5. EDWARDS, Lilian; BROWN, Ian: *Data Control and Social Networking: Irreconcilable Ideas?* In Matwyshyn, Andrea: *Harboring Data: Information Security, Law and the Corporation*. Stanford University Press, 2009 Dostupné na: http://ssrn.com/abstract=1148732 (08.11.2012)
6. EDWARDS, Lilian; WAELDE, Charlotte: *Law and the Internet*. 4th edition. Hart Publishing, 2009
7. GARRIE, Daniel: *Data Protection: The Challenges Facing Social Networking.* (31.05.2010). Brigham International Law and Management Review, Vol. 6, pp. 127-152. Dostupné na: http://ssrn.com/abstract=1618403 (11.11.2012)
8. GOLDMAN, Eric: *Social Networking Sites and the Law*. Květen 2007 Dostupné na: http://www.ericgoldman.org/Resources/socialnetworkingsitesandthelaw.pdf (12.11.2012)
9. GREEN, Richard Lane: *Facebook: Líbí se Vám?* Respekt, edice Fenomén, *Svět technologických novinek*, ve spolupráci s The Economist, vydavatelství Economia, 21.05.2012
10. GUARDA, Paolo: *Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks.* Ciberspazio e diritto, pp. 65-92, December 2008 Dostupné na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517449 (12.11.2012)
11. HOPPER, Jessica: *Digital Afterlife: What happens to your online accounts when you die?* Rock Center, 01.06.2012. Dostupné na: http://rockcenter.nbcnews.com/_news/2012/06/01/11995859-digital-afterlife-what-happens-to-your-online-accounts-when-you-die? (21.12.2012)
12. CHVÁTAL, Dalibor Z.: *Profesní sebevražda na sociálních sítích aneb jak Air Bank vyhodila mluvčího.* Server Lupa.cz, 04.07.2012. Dostupné na:

http://www.lupa.cz/clanky/profesni-sebevrazda-na-socialnich-sitich-aneb-jak-air-bank-vyhodila-mluvciho/ (21.11.2012)
13. JACOBSSON PUREWAL, Sarah: *Erase Yourself From the Web*. PCWorld, 30.03.2011. Dostupné na: http://www.pcworld.com/article/223682/erase_your_web_presence.html (21.11.2011)
14. KAVANOVÁ, Lucie*: Ukradli mi moje já*. Respekt, ročník XXIII., č. 33, 11.08.2012
15. KLESLA, Jan: *Internetové tržiště v praxi: Jeden milion facebookových adres stojí pět dolarů*. Server Ihned.cz, 29.10.2012. Dostupné na: http://byznys.ihned.cz/zpravodajstvi-svet/c1-58184820-internetove-trziste-v-praxi-jeden-milion-facebookovych-adres-stoji-pet-dolaru (22.11.2012)
16. KNAPPOVÁ, Marta; ŠVESTKA, Jiří; DVOŘÁK, Jan a kol.: *Občanské právo hmotné 1*. 4. vydání. ASPI, 2005 (Díl I., hlava XIII.)
17. KUČEROVÁ, Alena a kol.: *Zákon o ochraně osobních údajů: komentář*. 1. vydání. C.H. Beck, Praha 2003, 2012
18. MATĚJČEK, Petr: *Šokující fakta o Facebooku a našich osobních údajích*. Server CeskaPozice.cz, 11.02.2012. Dostupné na: http://www.ceskapozice.cz/zahranici/evropa/sokujici-fakta-o-facebooku-nasich-osobnich-udajich (21.11.2012)
19. MATES, Pavel; JANEČKOVÁ, Eva; BARTÍK, Václav: *Ochrana osobních údajů*. Leges, Praha 2012
20. MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav: *Osobní údaje a jejich ochrana*. 2. vydání. ASPI-Wolters Kluwer, Praha 2008
21. MAYER-SCHÖNBERGER, Viktor: *Delete – The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009
22. OTEVŘEL, Petr: *Sociální sítě z pohledu firmy: Co můžete a co ne?* Právní rádce č. 10/2012, Economia 2012
23. ROSEN, Joffrey: *The Web Means the End of Forgetting*. The New York Times, 21. července 2010. Dostupné na: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all (12.11.2012)
24. SOLOVE, Daniel J.: *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*. San Diego Law Review, Vol. 44, 2007. GWU Law School Public Law Research Paper No. 289
Dostupné na: http://ssrn.com/abstract=998565 (12.11.2012)
25. SOLOVE, Daniel J.: *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2007
Dostupné na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1019177 (12.11.2012)
26. ŠIMÍČEK, Vojtěch: *Právo na soukromí*. MUNI Press, Brno 2011
27. ŠVESTKA, Jiří a kol.: *Občanský zákoník I. § 1 – 459. Komentář*. 2. vydání. C.H. Beck, Praha 2009
28. VISCOUNTY, Perry; ARCHIE, Jennifer; ALEMI, Farnaz; ALLEN, Jenny:

Social Networking and the Law (Virtual Social Communities Are Creating Real Legal Issues). Business Law Today, Vol. 18, No. 4, březen/duben 2009
Dostupné na:
http://apps.americanbar.org/buslaw/blt/2009-03-04/viscounty.shtml (12.11.2012)

29. WERNER, Lukáš: *Kvůli Facebooku se propouští. Už i v Česku.* Server Týden.cz, 20.07.2012. Dostupné na: http://www.tyden.cz/rubriky/domaci/kvuli-facebooku-se-propousti-uz-i-v-cesku_129484.html (21.11.2012)
30. WONG, Rebecca: *Social Networking: A Conceptual Analysis of a Data Controller* (30.12.2009).
Communications Law, Vol. 14, No. 5, pp. 142-149, 2009
Dostupné na: http://ssrn.com/abstract=1529738 (02.11.2012)
31. WONG, Rebecca: *Social Networking: Anybody is a Data Controller* (21.09.2008).
Dostupné na: http://ssrn.com/abstract=1271668 nebo
http://dx.doi.org/10.2139/ssrn.1271668 (10.11.2012)
32. ZEMAN, Jiří; MEISNER, Martin: *Základy softwarového práva*. ASPI, 2011

Další zdroje

1. *AmCham EU position on the General Data Protection Regulation*. American Chamber of Commerce to the European Union. 11.07.2012. Dostupné na: http://www.cnpd.public.lu/fr/actualites/national/2012/07/Fedil-reforme/AmCham_EU_-_Position_Paper_on_Data_Protection_20120711.pdf (24.11.2012)
2. *Delete – The Virtue of Forgetting in the Digital Age*. Přednáška Viktora Mayer-Schönbergera z 08.08.2012, Old Theatre, Old Building, The London School of Economics and Political Science. Dostupné na: http://www2.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLectures AndEvents/player.aspx?id=1109 (11.11.2012)
3. *Draft Resolution on Privacy Protection in Social Network Services*. Spolkový komisař pro ochranu dat a svobodu informací, 30. mezinárodní konference komisařů o ochraně dat a soukromí, 17. října 2008, Štrasburk, Francie. Dostupné na: http://www.privacyconference2011.org/htmls/adoptedResolutions/2008_Strasbourg/2020_E5.pdf (11.11.2012)
4. *European Social Networks Position Paper Regarding The Proposed EU Data Protection Regulation*. European Social Networks Group. zn. 120416. Dostupné na: http://esng.eu/wp-content/uploads/2012/08/120416_EUROPEAN-SOCIAL-NETWORKS-POSITION-PAPER.pdf (18.11.2012)
5. *Komentáře členských států EU k Obecnému nařízení o ochraně údajů*. Zn. 9897/2/12 REV 2, 2012/0011 (COD), Rada EU, Brusel, Belgie, 18.07.2012. Dostupné na: http://www.statewatch.org/news/2012/jul/eu-council-dp-reg-ms-positions-9897-rev2-12.pdf (19.11.2012)
6. *Ochrana údajů: Evropané podle nového průzkumu sdílejí údaje na internetu, mají však obavy o soukromí*. Tisková zpráva Evropské Komise, Brusel, Belgie 16.06.2011, ref. zn. IP/11/742. Dostupné na:

http://europa.eu/rapid/press-release_IP-11-742_cs.htm (20.11.2012)
7. *Opinion 5/2009 on online social networking*. Pracovní skupina pro ochranu údajů zřízená podle článku 29, zn. 01189/09/EN, WP 163, 12.06.2009. Dostupné na: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (06.11.2012)
8. *Privacy in the Workplace - Data Protection in Social Networks*. Přednáška Andrease Wiebe na Mezinárodní konferenci v Pecsi, 2.-3. dubna 2012. Dostupné na: http://pawproject.eu/en/sites/default/files/page/15_wiebe_dpsn.pdf (10.11.2012)
9. *Resolution on European data protection reform*. Jarní konference 2012 evropských komisařů pro ochranu dat, Lucemburk, 03.-04.05.2012. Dostupné na: http://www.springconference2012.lu/files/7/3/document_id29.pdf (21.11.2012)
10. *Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union*. Zpráva publikována v červnu 2011. Dostupné na: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (22.11.2012).
11. *The importance of strong data protection rules for growth and competitiveness*. Přednáška Viviane Reding z 01.03.2012, Shaw Library, Old Building, The London School of Economics and Political Science. Dostupné na: http://www2.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLectures AndEvents/player.aspx?id=1379 (21.11.2012)

Použité právní předpisy

1. České právní předpisy

- Ústava České republiky, zákon č. 1/1993 Sb. ., ve znění pozdějších předpisů
- Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů
- Občanský zákoník, zákon č. 40/1964 Sb., ve znění pozdějších předpisů
- Občanský zákoník, zákon č. 89/2012 Sb.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů
- Soudní řád správní, zákon č. 150/2002 Sb., ve znění pozdějších předpisů
- Správní řád, zákon č. 500/2004 Sb, ve znění pozdějších předpisů
- Trestní zákoník, zákon č. 40/2009 Sb., ve znění pozdějších předpisů

2. Předpisy a smlouvy EU

- Smlouva o fungování Evropské unie, Úřední věstník C 83 ze dne 30.03.2010 (do 30.11.2009 pod názvem Smlouva o založení Evropského společenství)
- Lisabonská smlouva, Úřední věstník C 306 ze dne 17.12.2007
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

- ❖ Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých právních apektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu
- ❖ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronických komunikací
- ❖ Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES
- ❖ Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem takových údajů (Obecného nařízení o ochraně údajů) ze dne 25. ledna 2012

3. Mezinárodní smlouvy

- ❖ Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108. Přijata Radou Evropy ve francouzském Štrasburku dne 28. ledna 1981. Platila od 1. října 1985, přičemž pro ČR vstoupila v platnost až od 1. listopadu 2001, kdy byla publikována pod č. 115/2001 Sb.m.s.

RESUMÉ

Tato diplomová práce se zabývá ochranou osobních údajů subjektů údajů, tj. fyzických osob, k nimž se tyto údaje vztahují, na sociálních sítích vzhledem k možnostem likvidace osobních údajů, tj. jejich trvalého smazání, jak z fyzického nosiče, databáze správce, resp. zpracovatele, tak z internetového prostředí. Cílem této práce je zhodnotit současnou právní úpravu, poukázat na její nedostatky a představit návrh nařízení Evropské komise, jenž by měl tyto nedostatky vyřešit.

První kapitola této práce se zaměřuje na právo na soukromí, vývoj ochrany osobních údajů, základní principy jejich ochrany, nezbytnou terminologii ochrany osobních údajů, pojem a vývoj sociálních sítí a otázku soukromí na sociálních sítích. Na tento základ navazuje rozsáhlejší kapitolou právního rámce ochrany, jež představuje jádro této diplomové práce. Kapitolu právní rámec ochrany tvoří problematika teritoriality a aplikovatelnosti práva, právní vztah poskytovatele služby sociální sítě a uživatele a především likvidace dat a právní prostředky ochrany.

Druhá kapitola se soustředí na přípravu nové právní úpravy na úrovni EU, která má harmonizovat právní úpravy ochrany osobních údajů všech členských států EU a odstranit nedostatky dnešní zastaralé právní úpravy. Tato kapitola analyzuje návrh nového Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem takových údajů (představený 25.01.2012), který je součástí této reformy. Kapitola pojednává o důvodech pro přijetí nové úpravy, nastiňuje obsah předloženého návrhu nařízení a reakce, které tento návrh vyvolal.

Závěrem je konstatováno, že stávající právní úprava ochrany osobních údajů na sociálních sítí není schopna efektivně řešit aktuální právní problémy vznikající v prostředí sociálních sítí a její reforma je nevyhnutelná. Návrh nařízení Evropské komise je tak v tomto ohledu nejen vítaným, ale také nezbytným prostředkem řešení stávajícího neuspokojivého stavu.

SUMMARY

This diploma thesis deals with personal data protection of data subjects, i.e. natural persons to whom the data refer, in social networks in relation to possibilities of personal data liquidation, i.e. their permanent deletion both from physical data carrier and controller´s database, or processor, and from the Internet. The aim of this thesis is to evaluate current law, to show its imperfections, and to present European Commission´s regulation proposal that should solve these imperfections.

The first chapter of this thesis focuses on privacy law, development of personal data protection, basic legal principles of their protection, necessary terminology of personal data protection, conception and development of social networks, and question of privacy in social networks. This foundation is followed by an extensive chapter on legal framework of protection which comprises the core of this diploma thesis. The chapter legal framework of protection is formed by problems of territoriality and applicable law, legal relationship of social network service provider and user, and predominantly by data liquidation and legal means of protection.

The second chapter concentrates on preparation of new law on the EU level, which should harmonise personal data protection laws in all EU member states, and is to eliminate imperfections of the present old-fashioned law. This chapter analysis the new proposal for the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (presented on 25.01.2012), which presents one part of the reform. The chapter discusses reasons for acceptance of the new law, outlines content of the suggested regulation proposal, and reactions invoked by the proposal.

It comes to conclusion that the present personal data protection law in social networks fails to effectively handle current legal problems arising out of social networks environment, and as such, the reform is inevitable. In this regard, the European Commission regulation proposal is therefore not only a welcomed, but also an essential tool for solution of the present dissatisfactory situation.

Název diplomové práce v českém/anglickém jazyce
Name of the diploma thesis in Czech/English language

Ochrana dat na sociálních sítích /
Data Protection in Social Networks

Klíčová slova/ *Keywords*

- Ochrana dat / *Data protection*
- Sociálně sít(ě) / *Social network(s)*
- Sociální média / *Social media*