Jana Janderová

Ochrana soukromí na internetu – návrh nařízení EU a přijatá doporučení Výboru ministrů Rady Evropy

1. Úvod

S tím, jak na jedné straně přibývá každodenních uživatelů internetu, kteří jej používají pro běžné činnosti (pracovní i soukromá komunikace, bankovní operace, nakupování, vyhledávání informací např. z oblasti medicíny apod.) a na druhé straně poskytovatelů různých internetových služeb, kteří mají díky tomu přístup k mnohdy velmi citlivým údajům, jež mohou zneužít, vyvstává otázka, jak legislativně zabezpečit dostatečnou ochranu soukromí jeho uživatelů. Protože vývoj technologií, které se stávají stále sofistikovanějšími a umožňují v zásadě neomezené uchovávání dat, jejich propojování a další zpracování, je velmi prudký, zdá se, že dosavadní (obecnější) právní úprava je mnohdy nedostačující, nehledě na to, že je roztříštěná. Problémy způsobuje rovněž skutečnost, že právní rámec ochrany práv uživatelů je odlišný stát od státu, nicméně internet ze své povahy musí být nadnárodním prostředkem sdílení informací.

Je zřejmé, že internet má mnoho přínosů a jako nástroj výměny informací a komunikace mezi jednotlivci přispívá k realizaci řady lidských práv a základních svobod, zejména svobody projevu a přístupu k informacím a vzdělání, v případě sociálních sítí pak například svobody sdružovací. Umožňuje jedincům účast na politickém, sociálním a kulturním životě a jako takovýto prostředek pak posiluje občanskou společnost a demokratické právní principy. Na druhé straně pak s sebou přináší pro své uživatele mnohá rizika v souvislosti s údaji, které o sobě při využívání služeb poskytují, a jež jsou shromažďovány a dále zpracovávány, ať už se jedná o osobní údaje, které o sobě přímo zpřístupní na sociálních sítích, nebo o informace o navštívených stránkách, množství stažených dat, adresátech elektronické pošty a jiné komunikace, údaje o platebních kartách, případně údaje o pohybu mobilního telefonu při prohlížení internetových stránek. Z uchovávaných údajů lze dovodit celou řadu mnohdy citlivých údajů o daném uživateli a jeho soukromí, například o jeho smýšlení, zdravotním stavu, sexuální orientaci, kupní síle a způsobu, jakým utrácí. Především pak zkombinování různých údajů a jejich poskytnutí třetím osobám může mít velmi citlivý dopad na soukromý život uživatelů. V případě, že data nejsou dostatečně zabezpečena nebo je-li umožněn jejich prodej, mohou být zneužita k celé řadě účelů počínaje nevyžádaným adresným marketingem a konče například prověřováním

indicií ohledně zdravotního stavu uživatelů ze strany potenciálních zaměstnavatelů v případě, kdy uživatel hledá práci, a v USA se rozmáhajících případech, kdy zdravotní pojišťovny odmítají uživatele pojistit, když ve vyhledavači často zadával klíčová slova vztahující se k závažným chorobám.

Uchovávání údajů ve výše popsaných případech vyplývá z vlastní vůle provozovatelů různých služeb na internetu. Ti takováto data uchovávají a dále zpracovávají, ať už proto, že se snaží vyjít vstříc některým uživatelům (koho by neobtěžovalo stále dokola vyplňovat svou adresu, číslo zákaznické karty a podobné údaje, které mohou po jejich prvním zadání zůstat před-vyplněné v nabídce), případně poznat lépe chování uživatelů, jejich preference a potřeby, aby mohli vylepšit své služby a získat tak konkurenční výhodu oproti ostatním podnikatelům v daném sektoru. V horším případě také protože někteří tato data neoprávněně za úplatu poskytují dále. Specifickou otázkou je pak možnost zneužití údajů v souvislosti s právními předpisy stanovenou povinností poskytovatelů internetového připojení uchovávat jisté provozní a lokalizační údaje pro potřebu vyšetřování trestné činnosti.

Pro účely vyšetřování trestné činnosti jsou totiž poskytovatelé internetového připojení a telefonní operátoři po určitou dobu povinni uchovávat provozní a lokalizační údaje a tyto údaje poskytnout na vyžádání oprávněným orgánům. Provozními údaji jsou v zásadě jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování. Lokalizačními údaji jsou údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele služby elektronických komunikací. Jedná se například IP adresy, množství přenesených dat při datové komunikaci, dále zejména o datum a čas zahájení telefonní komunikace, telefonní čísla volajícího a volaného a délku komunikace. Protože státní orgány mají tendenci nadužívat možnosti vyžádat si tyto údaje, bývá pak sporným bodem, v jakém rozsahu mají být údaje uchovávány, po jakou dobu, jakým způsobem mají být předávány oprávněným orgánům, včetně vymezení těchto orgánů, dodatečného informování osob, jichž se údaje týkají, jejich použití jako důkazních prostředků apod.

Tento příspěvek si však neklade za cíl důkladně se zabývat touto specifickou problematikou uchovávání provozních údajů pro potřeby vyšetřování, protože se tato problematika ve větší míře týká telefonní komunikace než internetu. Bude zmíněna pouze na okraj v souvislosti s nálezem Ústavního soudu Pl. ÚS 24/10 ze dne 22. března 2011, který je však pro účely tohoto příspěvku důležitý z toho důvodu, protože jím Ústavní soud definuje právo na soukromí, tedy prostor, do kterého nemá být zasahováno, a tím limity, kterých by se měl zákonodárce při přijímání nové úpravy řídit. Ochrana soukromí na internetu je totiž doposud v České republice právními předpisy opomíjena, vyjma zmíněné oblasti uchovávání údajů pro potřeby vyšetřování trestné činnosti (přičemž o kvalitě úpravy této oblasti lze pochybovat). Je to zřejmě zapříčiněno tím, že právní úprava musí vždy nutně přicházet až s jistým odstupem v reakci na vznikající problémy, které však nelze ignorovat, což u ochrany soukromí na internetu s rapidně rostoucím množstvím údajů, jež je možno zneužít, platí dvojnásob.

Tento článek je proto zacílen na poskytnutí informací o právním rámci takovéto ochrany rodící se předně v Evropské unii v podobě nařízení, jež se bude díky svému

přímému účinku, vztahovat rovněž na všechny poskytovatele internetových služeb a jejich uživatele v České republice, a dále pak rovněž v podobě dvou doporučení – tedy soft law – v Radě Evropy. Lze jen doufat, že tyto dokumenty poslouží coby podněty de lege ferenda pro českou legislativu, když stávající právní úprava je zcela nedostačující.

2. Návrh nařízení Evropského parlamentu a Rady

Oblast ochrany osobních údajů v rámci Evropské unie je obsažena v primárních předpisech v článku 16 odst. 1 Smlouvy o fungování Evropské unie, jak byl zaveden Lisabonskou smlouvou, který zakládá právo každého na ochranu osobních údajů. Odstavec 2 téhož ustanovení obsahuje zmocnění pro přijímání předpisů v této oblasti. Článek 8 Listiny základních práv Evropské unie prohlašuje ochranu osobních údajů za základní právo. Klíčovým sekundárním předpisem je doposud směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, přičemž dále ji doplňuje pro oblast elektronických komunikací směrnice Evropského parlamentu a Rady 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.[1)] Účelem směrnice 95/46/ES je ochránit osobní údaje a dále umožnit jejich volný pohyb v rámci států EU. Tento účel stále v zásadě plní, avšak s překotným rozvojem technologií a s nárůstem možnosti zneužití údajů, jak bylo popsáno výše, byla stávající úprava stále častěji kritizována. Komise tudíž dospěla k závěru, že je třeba přijmout novou úpravu. Z důvodu roztříštěnosti národních právních úprav jednotlivých členských států EU a právní nejistoty občanů EU, složitosti právních norem upravujících poskytování osobních údajů do třetích zemí mimo EU, kterým se stávající směrnicí nepodařilo předejít, se Komisi jako vhodnější nástroj úpravy než směrnice jeví nařízení, které díky přímému účinku povede k harmonizaci národních právních úprav.

Evropská Komise dne 25. ledna 2012 zveřejnila návrh nařízení COM (2012)11 final o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů).[2)] Cílem navrhovaného nařízení je výrazně zvýšit právní jistotu občanů a správců osobních údajů, snížení administrativní zátěže, konzistentnost právních úprav všech členských států včetně donucovacích

---

[1)] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací – tato směrnice byla změněna Směrnicí Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, a také Směrnicí Evropského parlamentu a rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.

[2)] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [citováno 21. května 2012].

prostředků k ochraně osobních údajů, efektivní možnost výkonu práv souvisejících s ochranou osobních údajů po celém teritoriu EU a účinný dohled nad ochranou osobních údajů a její prosazování. Komise zdůvodňuje nezbytnost jednotné úpravy na úrovni EU (naplnění podmínky plynoucí z principu subsidiarity) tak, že ochrana osobních údajů musí být ve všech členských státech stejná. Rozdílná úprava, a tedy i úroveň ochrany by omezovala přeshraniční předávání údajů mezi státy s rozdílnými standardy úpravy. Stejná úroveň ochrany je rovněž potřebná při předávání dat do třetích zemí. Jednotlivé členské státy nemohou samy omezit stávající problémy, které plynou zejména z roztříštěnosti úprav. Jednotná evropská úprava tedy bude efektivnější.

Z návrhu lze vyčíst, že nařízení má stavět na dosavadní úpravě obsažené ve směrnici Evropského parlamentu a Rady 95/46/ES a dále ji prohlubuje. Ochrana obsažená v návrhu nařízení se vztahuje na všechny fyzické osoby bez ohledu na jejich národnost nebo místo, kde trvale pobývají. Nevztahuje se na ochranu základních práv a svobod a volný pohyb údajů nebo jejich zpracovávání, které spadá mimo unijní právo. Dále se nevztahuje na zpracovávání dat fyzickými osobami pro jejich soukromé potřeby, unijními institucemi[3] ani členskými státy v případech, kdy vykonávají společnou zahraniční a bezpečnostní politiku Evropské unie. Ochrana osobních údajů při jejich zpracování příslušnými orgány pro účely prevence, vyšetřování, odhalování či stíhání trestných činů a výkonu trestů a volný pohyb těchto údajů, se bude řídit zvláštním právním předpisem, jímž bude paralelně s nařízením připravovaná směrnice COM (2012)010 final[4].

Z pohledu tohoto příspěvku jsou podstatná práva, jež budou plynout z nařízení v případě jeho přijetí uživatelům internetu. V článku 11 je zakotvena povinnost správců dat poskytovat transparentní, dostupné a srozumitelné informace. Dále dle článku 12 mají zavést procedury pro uplatnění práv osob, jejichž data jsou zpracovávána, včetně elektronických žádostí, přičemž odpověď bude muset být zaslána ve stanoveném termínu a zamítnutí žádosti bude muset být odůvodněno. V článku 14 je rozvinuta dosavadní povinnost správců dat poskytovat informace, nově o době, po kterou jsou údaje zpracovávány, o možnosti podat stížnost, dále informace o mezinárodním poskytování dat a o zdroji, ze kterého data pocházejí. Zůstávají však výjimky dosud obsažené ve směrnici, informační povinnost nebude dána v případech, kdy uchovávání údajů nebo jejich poskytnutí vyplývá přímo ze zákona. Tato výjimka by se mohla vztahovat například na řízení vedená úřady pro ochranu hospodářské soutěže, finančními úřady a celními správami, nebo úřady s agendou v oblasti výplaty sociálních dávek. V článku 15 je zakotveno právo na přístup k vlastním osobním údajům, přičemž je nově přidáno právo na jejich opravu, jejich výmaz a právo podat stížnost. Dále jsou tato práva rozvedena v článcích 16 a 17 včetně práva na to být zcela zapomenut. Jestliže subjekt zpracovávající osobní údaje tyto poskytl třetím

---

[3] Na tyto se vztahuje směrnice č. 45/2001/ES.

[4] Návrh směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů - podrobnosti dostupné na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:CS:HTML [citováno 21. května 2012].

osobám, zavádí se povinnost, aby tyto informoval o žádosti o výmaz veškerých kopií takovýchto údajů a vazeb na ně. Dále je zde obsaženo právo v určitých případech požadovat omezení zpracovávání osobních údajů. V článku 18 se zavádí právo na „převoditelnost" osobních údajů, tedy aby osoba, o níž se takováto data shromažďují, mohla data převést z jednoho elektronického systému do jiného, aniž by jí v tom mohl správce dat bránit. Přitom daná fyzická osoba může požadovat po správci dat, aby jí data poskytl ve strukturovaném a běžně používaném formátu. Právo protestovat proti zpracovávání dat je obsaženo v článku 19. V případě, že údaje jsou zpracovávány pro marketingové účely, musí být nadto umožněno podat protest bez jakéhokoli poplatku a zároveň v rámci poskytovaných informací musí být každý, jehož data jsou zpracovávána, na toto právo upozorněn.

Zásadní je pak právo nebýt podroben opatření založenému na profilování vyplývající z článku 20. Každá fyzická osoba tak má právo nebýt podrobena opatření, které pro ni vyvolává právní důsledky nebo se jí významně dotýká, a které je založeno výhradně na automatizovaném zpracování dat určeného k vyhodnocení určitých osobních stránek dané fyzické osoby nebo k analýze, či předpovědi zejména toho, jak bude daná osoba výkonná v zaměstnání, jaká je její ekonomická situace, kde bydlí, jak pevné má zdraví, jaké jsou její preference, zda je spolehlivá či jak se chová. Takovémuto opatření může být fyzická osoba podrobena pouze, když k němu dochází při zpracování dat v následujících případech. Jestliže fyzická osoba požádala o uzavření smlouvy, případně o její plnění, pak je možné takovéto opatření použít, bylo-li jí vyhověno, případně jestliže byla zavedena vhodná opatření k tomu, aby byly chráněny legitimní zájmy dané osoby, jako je například právo na lidský zásah do automatizovaného zpracování. Dále jej lze použít, umožňují-li to unijní předpisy nebo předpisy členských států, které zároveň obsahují vhodná opatření na ochranu legitimních zájmů fyzických osob. Naposled pak, dala-li k tomu daná fyzická osoba písemný souhlas a opět jsou-li zavedena vhodná opatření. V odstavci 5 tohoto článku je pak zmocněna Komise k tomu, aby přijala prováděcí předpis ohledně kritérií a podmínek týkajících se těchto „vhodných opatření".

Dále je v článku 32 upraveno právo fyzické osoby na informaci o tom, že došlo k zásahu do jejích osobních údajů, jestliže takovýto zásah může pravděpodobně nepříznivě ovlivnit ochranu osobních údajů nebo případně zasáhnout do jejího soukromí. Toto oznámení musí následovat bezprostředně po oznámení učiněném orgánu dohledu a musí obsahovat popis zásahu a alespoň kontaktní údaje na inspektora ochrany údajů, který poskytne bližší informace, a opatření, jež jsou doporučena k tomu, aby se co možná zmírnily následky zásahu do osobních údajů. Oznámení nemusí být dotčené osobě zasláno v případě, kdy osoba zpracovávající její údaje dostatečně prokáže kontrolnímu orgánu, že přijala vhodná technická opatření proti zásahům do osobních údajů a tato opatření uplatnila i v případě osobních údajů, jichž se týkal zásah.

Článek 21 umožňuje Evropské unii a členským státům přijmout právní předpisy, které rozsah výše popsaných práv omezí, a to za předpokladu, že omezení bude nezbytné a přiměřené k tomu, aby v demokratické společnosti zajistilo (i) veřejnou bezpečnost, (ii) prevenci, vyšetřování, odhalování či stíhání trestných činů, (iii) jiné

veřejné zájmy Unie nebo členského státu, zejména důležitý ekonomický nebo finanční zájem, včetně měnových, rozpočtových a daňových záležitostí a ochrany stability a integrity trhu, (iv) prevenci, vyšetřování, odhalování či stíhání porušení etických pravidel u regulovaných povolání, (v) dohled, kontrolu a regulační činnost (rovněž příležitostnou) správního orgánu v případech uvedených výše a (vi) ochranu osoby, jejíž data jsou shromažďována a práv a svobod jiných osob. Přitom takovýto právní předpis musí obsahovat zvláštní ustanovení přinejmenším o cílech, které mají být zpracováním dat dosaženy, a určení konkrétních správců dat.

Nově je v článku 35 zavedena povinnost pro všechny veřejnoprávní subjekty a dále pro velké podniky, u kterých vyžaduje shromažďování a zpracování osobních údajů pravidelný a systematický dohled mít inspektora ochrany údajů. Dále se zakládá nezávislá Evropská rada ochrany údajů, jež se bude skládat z hlav jednotlivých národních orgánů dohledu nad ochranou osobních údajů.

Konečně podstatná je rovněž navrhovaná úprava nápravných opatření. Každý bude mít právo na základě článku 73 podat stížnost k orgánu dohledu. Článek 74 pak zaručuje právo na soudní přezkum rozhodnutí orgánu dohledu ohledně podané stížnosti. Dále je upraveno v článku 75 právo na soudní ochranu cestou žaloby podané proti subjektu zpracovávajícímu osobní údaje, s tím, že žalobce bude mít možnost volby sudiště dle sídla žalovaného nebo místa, kde jsou data shromažďována. V článku 77 je stanovena odpovědnost a právo na náhradu.

Předpokládá se, že nařízení nabude účinnosti dva roky poté, co bude publikováno v Úředním věstníku EU. Zároveň s tím bude zrušena směrnice Evropského parlamentu a Rady 95/46/ES. Díky přímému účinku bude nařízení od tohoto okamžiku závazné i pro Českou republiku.

Postoj české vlády i obou parlamentních komor k návrhu nařízení je však velmi vlažný[5)]. Vytýkají mu zejména nedodržení principu subsidiarity v některých pasážích, zároveň činí spornou vlastní formu úpravy pomocí nařízení, výhrady pak mají k vymezení některých institutů – například definici citlivých údajů, nezávislých dozorových orgánů. Pokud i další země vyjádří podobné námitky, dozná navrhovaný text pravděpodobně ještě úprav.

Narozdíl od tohoto nařízení, které sice velmi pravděpodobně bude jednoho dne (ať už v jakkoli upraveném znění) závazné, avšak prozatím se nachází ve fázi návrhu, mají evropské země již nyní k dispozici v konečné verzi dvě doporučení mezinárodní organizace. Tato doporučení sice nejsou závazná a mají pouze charakter soft law, ale vahou Rady Evropy, jež za nimi stojí, působí jako zdroj, na který by měly členské státy reagovat a jež by minimálně neměl zůstat nepovšimnut bez jakéhokoli zdůvodnění. Lze tedy již nyní velmi dobře čerpat z těchto doporučení pro případnou vlastní vnitrostátní právní úpravu, jež by mohla vyplnit minimálně časový prostor před tím, než nařízení nabude účinnosti.

[5)] Blíže viz. usnesení výboru pro evropské záležitosti Poslanecké sněmovny č. 212 ze dne 5. dubna 2012: http://www.psp.cz/temp/tswf/00088594.pdf [citováno dne 18.6.2012], usnesení výboru pro záležitosti Evropské unie Senátu č. 264 ze dne 2.5.2012 : http://www.senat.cz/xqw/xervlet/pssenat/original/64515/54444/53111 [citováno dne 18.6.2012].

3. Dvě doporučení Výboru ministrů Rady Evropy vztahující se k ochraně soukromí v souvislosti s používáním služeb internetových vyhledavačů a sociálních sítí

V rámci Rady Evropy byla v nedávné době přijata dvě doporučení členským státům, jak zlepšit ochranu soukromí uživatelů internetu. Doporučení sice jsou tzv. soft-law, což znamená, že nejsou pro členské státy Rady Evropy formálně právně závazná, mají však závaznost politickou, a tudíž se dá očekávat, že by se jimi měl v nejbližší době český zákonodárce inspirovat a převést je do českého právního řádu.

Tedy konkrétně, dne 4. dubna 2012 přijal Výbor ministrů Rady Evropy na 1139. zasedání delegátů ministrů dvě doporučení členským státům vztahující se k ochraně soukromí a dalších lidských práv na internetu - Doporučení CM/Rec(2012)3 o ochraně lidských práv v souvislosti s používáním internetových vyhledavačů a Doporučení CM/Rec(2012)4 o ochraně lidských práv v souvislosti s používáním služeb sociálních sítí.

3.1 Vyhledavače

V prvém z doporučení – CM/Rec (2012)3 – Výbor ministrů konstatuje, že vyhledavače hrají rozhodující úlohu coby místa prvního kontaktu na internetu při výkonu práva vyhledávat informace, fakta a myšlenky a další obsah včetně zábavy. Takovýto přístup k informacím je rozhodující pro to, aby si každý mohl učinit vlastní názor a mohl se účastnit politického, kulturního a ekonomického dění. Existuje však jistá obava, že uživatelé využívají pouze omezený počet dominantních vyhledavačů. To může vyvolávat otázky ohledně přístupu k různorodým zdrojům informací, především vzhledem k tomu, že vyhledávání informací a jejich řazení není vyčerpávající ani neutrální, takže některé zdroje mohou být neoprávněně favorizovány. Přitom většina vyhledavačů poskytuje velmi málo informací, případně pouze obecné informace, o tom, jaká kritéria používají při vyhodnocování vyhledaného výsledku coby „nejlepší" odpovědi na zadaný dotaz. Na jedné straně je třeba uznat, že plné zveřejnění vyhledávacích algoritmů není možné, protože jsou předmětem soutěže jednotlivých podnikatelských subjektů a dále protože by to mohlo vést ke zvýšené zranitelnosti služeb vyhledávačů například formou zmanipulování vyhledávání. Na druhé straně by však státy měly podporovat provozovatele vyhledavačů v tom, aby zvýšili transparentnost alespoň obecných kritérií a procesů výběru výsledků a stanovování jejich pořadí (měli by zveřejňovat informace o nasměrování a ovlivnění vyhledávání, tedy zda jsou výsledky zobrazovány například podle zjevné zeměpisné polohy uživatele nebo jeho dřívějších vyhledávání). Dále by provozovatelé vyhledávačů měli rozlišovat mezi výsledky vyhledávání a jakoukoli formou komerčních sdělení, ať už reklam, sponzorovaných výstupů nebo jejich vlastních nabídek.

Vyhledavače zpracovávají velké množství osobních údajů ohledně toho, jak a co uživatelé vyhledávají, ať už jde o tzv. cookies, IP adresy, či historie vyhledávání jednotlivých uživatelů. Historie vyhledávání každého uživatele v sobě obsahuje údaje, ze kterých se dají zjistit zájmy dané osoby, její myšlenky, úmysly a vztahy. Přitom mohou

být odtajněny i citlivé údaje chráněné článkem 6 Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (CETS No. 108), jakými jsou rasový původ, politické přesvědčení, víra, data vztahující se ke zdravotnímu stavu, sexuálnímu životu nebo ohledně trestního stíhání. Zpracování osobních údajů vyhledavači získává novou dimenzi z důvodu velkého rozšíření audiovizuálních dat a vzrůstající popularitě mobilního přístupu k internetu. Specializované vyhledavače umožňují uživatelům vyhledávat informace o konkrétních osobách a místech, kde se pohybují. Dále díky stále přesnějším technologiím rozpoznávání obličejů existují velké obavy ze zneužití fotografií umístěných na internet jednotlivými uživateli, jestliže jsou tyto zahrnuty do výsledků běžného vyhledávání. Kombinací různých informací o určité osobě mohou vyhledavače vytvořit obraz osoby, který nemusí odpovídat skutečnosti nebo tomu, jaký by daná osoba sama o sobě chtěla poskytovat. Kombinace shromážděných údajů tak vytváří pro danou osobu mnohem větší rizika, než kdyby údaje vztahující se k jejímu chování na internetu zůstaly oddělené.

Členské státy by proto měly přimět provozovatele internetových vyhledavačů, aby zvýšili transparentnost způsobu, jakým jsou poskytovány informace, zejména aby informovali o kritériích, podle kterých jsou výsledky vyhledávání vybírány, je jim přiřazena důležitost a jak jsou případně odstraňovány. Dále, aby přehodnotili způsob, jakým je přiřazována důležitost informacím, které byť jsou publikovány ve veřejném prostoru internetu, nejsou zamýšleny k hromadnému šíření. Obsah těchto informací by se měl ve výsledcích vyhledávání objevovat dostatečně vzadu, přičemž by například mohly být nastaveny různé úrovně dostupnosti informací podle toho, zda jejich autor zamýšlel jejich sdělení širším vrstvám, nebo naopak jen omezenému okruhu lidí. Výchozí nastavení by měla být koncipována s ohledem na tento cíl. Měli by také zvýšit transparentnost shromažďování osobních údajů a legitimních důvodů, pro které jsou zpracovávány. Uživatelům by měli umožnit jednoduchý přístup k jejich osobním údajům, které o nich zpracovávají, a v případě potřeby i jejich úpravu nebo vymazání. Měly by se vyvinout nástroje sloužící k minimalizaci shromažďování a zpracovávání osobních údajů, včetně prosazení omezení doby, po kterou jsou data uchovávána, adekvátního způsobu jejich nevratné anonymizace a rovněž tak nástrojů pro jejich vymazání.

Členské státy by měly zakotvit vhodné prostředky právní ochrany zajišťující uživateli v situaci, kdy k jeho osobním údajům mají přístup jak veřejnoprávní tak soukromoprávní subjekty, možnost v plné míře požívat práv jež mu plynou z Úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluva"). Státy by měly přimět provozovatele internetových vyhledávačů, aby vyřazovali výsledky vyhledávání pouze v souladu s článkem 10 odst. 2 Úmluvy. Uživatel by v takovém případě měl být informován o původu žádosti o vyřazení údajů, přičemž musí být chráněno právo na soukromí a ochranu osobních údajů. Měla by být podporována všeobecná znalost fungování vyhledavačů, zejména procesů výběru výsledků vyhledávání, jejich řazení dle důležitosti a důsledků, jež může mít použití vyhledávačů na uživatelovo právo na soukromí a ochranu osobních údajů. Státy by také měly zvážit možnost nabídnout uživatelům výběr z různých vyhledavačů, zejména s ohledem na to, aby výsledky vyhledávání byly založeny na kritériích veřejných hodnot. Měly by podpořit trans-

parentní mechanismy samoregulace a ko-regulace vyhledavačů, zejména s přihlédnutím k přístupu k informacím, jež jsou prohlášeny soudem nebo jiným k tomu příslušným orgánem za nezákonné, přičemž se musí vždy zachovávat standardy Rady Evropy ohledně svobody vyjadřování a práva na spravedlivý proces.

Na základě doporučení by pak členské státy by měly přijmout tato následující opatření:

- zajistit, aby shromažďování osobních údajů provozovateli vyhledávačů bylo minimální. Žádné uživatelské IP adresy by neměly být ukládány, jestliže to není nezbytné pro sledování legitimního účelu a jestliže stejné výsledky mohou být dosaženy pomocí použití vzorků, namátkového průzkumu nebo anonymizací osobních údajů. Rovněž by měly být podporovány inovativní přístupy zavádějící anonymní vyhledávání,
- zajistit, aby lhůty, po které jsou údaje uchovávány, nebyly delší, než je nezbytně nutné pro legitimní a výslovně stanovené účely zpracování dat. Provozovatelé vyhledavačů by měli být schopni dostatečně zdůvodnit nutnost shromažďování dat a jejich uchovávání,
- zajistit, aby provozovatelé vyhledávačů přijali co nejvhodnější bezpečnostní opatření, aby předešli protiprávnímu přístupu třetích osob k osobním údajům, a dále vhodné mechanismy ohlašování takovýchto neoprávněných přístupů. Opatření by měla zahrnovat „end-to-end" šifrování[6] komunikace mezi uživatelem a provozovatelem vyhledavače,
- zajistit, aby uživatelé byli o zpracovávání jejich dat informováni, s tím, že by jim provozovatelé vyhledavačů měli od počátku sdělovat veškeré zamýšlené účely užití jejich údajů a zdůraznit, že primárním důvodem jejich zpracování je poskytnout lepší výsledky při vyhledávání. Zároveň by měli informovat uživatele, jestliže dojde ke zneužití jejich údajů,
- zajistit, aby k vzájemné souvztažnosti údajů pocházejících z různých služeb/platforem patřících totožnému provozovateli vyhledavače docházelo pouze za předpokladu, že k tomu uživatel dal výslovný a jednoznačný souhlas,
- podpořit provozovatele vyhledavačů v tom, aby rozvinuli nástroje, které umožní uživatelům přístup k jejich vlastním osobním údajům, které byly shromážděny v průběhu používání vyhledavače, a to včetně jakéhokoli profilu vytvořeného například pro přímé marketingové účely, a dále jim umožní, aby tyto údaje mohli upravovat nebo vymazat,
- zajistit, aby žádosti státních orgánů prosazujících výkon spravedlnosti o poskytnutí osobních údajů směřované provozovatelům vyhledavačů byly založeny na odpovídajících právních a soudních postupech a aby byly zakotveny transparentní mechanismy jejich vzájemné spolupráce. Tento požadavek zahrnuje především to,

---

[6] End-to-end šifrování (E2EE) šifruje nešifrovaná (červená) data u zdroje se znalostí určeného příjemce, což umožňuje šifrovaným (černým) datům cestovat bezpečně přes zranitelné kanály (např. veřejné sítě) k jejich příjemci, kde mohou být dešifrována (za předpokladu, že cíl sdílí potřebné klíčové proměnné a algoritmy) Citováno z wikipedie: http://en.wikipedia.org/wiki/End-to-end_encryption [citováno 21. května 2012].

aby existovaly silné právní záruky proti zneužití osobních údajů a byly dodržovány požadavky na spravedlivý proces, a to ještě před tím, než budou osobní údaje a údaje o vyhledávání poskytnuty orgánům státní moci nebo soukromým osobám.

3.2 Sociální sítě

Ve druhém z doporučení – CM/Rec (2012)4 – Výbor ministrů Rady Evropy připomíná, že sociální sítě jsou důležitým nástrojem komunikace mezi jednotlivci, mezi skupinami a rovněž tak slouží pro hromadnou komunikaci. Mají velký potenciál pro lidská práva, zejména svobody vyjadřovací, shromažďovací a práva na výměnu názorů a myšlenek. Na druhé straně mohou ohrozit právo na lidskou důstojnost a právo na soukromí, neboť mohou poskytovat prostor pro diskriminační jednání. Nedostatek právní úpravy a pojistek proti zneužití může vést k vyloučení některých uživatelů, nedostatečné ochraně dětí a mladistvých proti nebezpečnému jednání nebo některým informacím, nerespektování práv druhých, nedostatku ochrany soukromí ve výchozím nastavení, nedostatku informací o důvodech, pro které se shromažďují a zpracovávají osobní údaje.

Sociální sítě produkují velké množství osobních údajů, včetně údajů o profilu uživatele a použití internetu. Uveřejnění osobních údajů na profilu uživatele může vést k tomu, že k nim budou mít přístup třetí osoby včetně například zaměstnavatelů, pojišťoven, orgánů činných v trestním řízení a bezpečnostních agentur. Sociální sítě by měly omezit shromažďování osobních údajů pouze na ty, které jsou nezbytně nutné pro smluvený účel a po dobu co možná nejkratší. Měly by si také vyžádat informovaný souhlas uživatelů, pokud chtějí sdílet jejich údaje se dalšími osobami nebo pro jiné účely než ty, které jsou nezbytné pro dosažení účelů specifikovaných v okamžiku, kdy byla data shromážděna. V případě, kdy umožňují třetím osobám přístup k osobním údajům uživatele, měly by sociální sítě zajistit přístup k údajům v několika úrovních, které umožní uživatelům vyjádřit výslovný souhlas s přístupy k různým osobním údajům.

Přitom jestliže nadto profily uživatelů uvádějí vyhledávače ve výsledcích vyhledávání, existuje teoreticky neomezený přístup k informacím, nebo jejich částem, uvedeným na takovýchto profilech. Uživatelé by tedy měli vědět, zda informace uvedené na jejich profilu budou mít soukromý nebo veřejný charakter, a měli by si být vědomi důsledků, které vyplývají z toho, že se rozhodnou určitou informaci publikovat coby veřejně dostupnou. Především děti, a mezi nimi zejména náctiletí, a případně další kategorie zranitelných uživatelů potřebují vést k tomu, aby byly schopné samy spravovat své profily a porozumět tomu, jaký dopad má zveřejnění informací, aby se mohly ochránit před nebezpečími, která hrozí jim a dalším osobám.

Provozovatelé sociálních sítí by proto měli zavést z pohledu uživatelů nejvhodnější postupy. Mezi tyto patří: takové výchozí nastavení chránící soukromí uživatelů a omezující přístup pouze pro osoby, které uživatel sám označí; vhodné zabezpečení, informovaný souhlas uživatelů před tím, než budou jejich osobní údaje šířeny nebo sdíleny s jinými skupinami lidí nebo se společnostmi a před jejich použitím jakýmkoli jiným novým způsobem.

Dále by měla být zpřísněná ochrana citlivých údajů. Zejména použití techniky rozeznávání obličejů by nemělo být ve výchozím nastavení a mělo by být zvláště chráněno. Osobní údaje by měly být chráněny před jejich zneužitím třetími osobami, mezi jinými pomocí nástrojů šifrování komunikace „end to end". V případě, kdy k takovému zneužití přesto dojde, měli by provozovatelé sociálních sítí o tom uživatele informovat, aby tito mohli přijmout preventivní opatření, jako například změnit heslo a bedlivě sledovat své finanční transakce (jestliže provozovatelé sociálních sítí mají přístup k bankovním informacím případně informacím o platební kartě).

Třetí osoby, které nejsou uživateli příslušné sociální sítě, mohou být rovněž dotčeny, ať už tím, že údaje o nich zveřejní uživatelé sítě, nebo tím, že k těmto datům má přístup provozovatel sociální sítě. Tyto osoby by měly mít možnost chránit své údaje, aniž by se musely stát uživatelem sociální sítě. Provozovatelé sociálních sítí by se měli zdržet zpracovávání takovýchto osobních údajů a uživatelé by měli být informováni o tom, že při zveřejnění údajů o třetích osobách mají povinnost dbát jejich práv.

Uživatelé by měli dostat jasnou informaci o tom, jakým právním řádem se řídí jejich vztah k provozovateli sociální sítě a který soud bude příslušný k řešení případného sporu. Taková ustanovení obsažená v obchodních podmínkách, ve kterých je zvolen právní řád či příslušnost soudu dle toho, co je pro provozovatele výhodné, by měla být považována za neplatná, jestliže neexistuje rozumná vazba k příslušnému soudu a zvolenému právnímu řádu. V případě, že v určitém státě je významný počet uživatelů, měl by být přednostně uplatněn právní řád tohoto státu a soud volen dle jejich bydliště. Nad rámec běžných prostředků právní ochrany by měla být zavedena zvláštní procedura, kde by na základě stížnosti nebo žaloby bylo přezkoumáno protiprávní jednání uživatelů, zejména krádež identity.

Na základě doporučení by pak členské státy měly přijmout zejména tato následující opatření:

- zajistit, aby výchozí nastavení limitovalo přístup třetích osob k profilu uživatele pouze na osoby (kontakty) zvolené uživatelem. Zároveň by provozovatelé sociálních sítí měli informovat uživatele o dopadech otevřeného (z pohledu geografického i časového) přístupu k jejich profilům a umožnění veřejného přístupu k jimi publikovaným informacím a shromažďování údajů třetími osobami. Dále by uživatelům měli poskytnout dostatečné prostředky k tomu, aby mohli uplatnit právo omezit přístup k jejich údajům, včetně práva odstranit údaje z archivů a vyrovnávací paměti vyhledavače (tzv. cache),
- zajistit, aby provozovatelé sociálních sítí umožnili uživatelům spravovat své údaje, což znamená, že by uživatelé měli být informováni o tom, že před tím, než zveřejní osobní data třetích osob – včetně audio a video záznamů, potřebují jejich souhlas v případech, kdy přístup k profilu je širší než pro předem zvolený omezený počet osob – kontaktů. Dále musí být informováni o tom, jak zcela vymazat svůj profil a na sociálních sítích jimi uložená data a jak použít pseudonym. Uživatelé musí mít vždy právo odvolat souhlas se zpracováním svých osobních údajů. Dříve než zruší svůj účet, měli by mít právo jednoduše, v použitelném formátu a zcela zdarma přesunout data, která uložili, k jiné službě nebo na jiný nosič dat. Při zrušení účtu

by pak veškerá jimi uložená data a údaje o těchto uživatelích měla být definitivně vymazána z paměťových médií sociální sítě,

- respektovat vůli uživatele nezveřejnit svou totožnost a garantovat právo používat pseudonym. Přitom v případech, kdy sociální síť vyžaduje při registraci zadání totožnosti uživatele, mělo by být na uživateli, zda ji hodlá zveřejnit. To však nic nemění na právu orgánů činných v trestním řízení získat v nezbytných případech k totožnosti uživatele přístup za předpokladu, že budou dodržena jeho základní práva.

4. Česká právní úprava a nález Ústavního soudu Pl. ÚS 24/10 ze dne 22. března 2011

Stávající česká právní úprava vztahující se k výše popsané oblasti je poměrně strohá a při nakládání s osobními údaji je třeba vyjít z obecné úpravy obsažené v zákoně č. 101/2000 Sb., o ochraně osobních údajů. Zde však nemohou být postižena specifika internetu a hrozících zásahů do soukromí souvisejících s jeho používáním. Provozování služeb na internetu je regulováno zákonem č. 127/2005 Sb., o elektronických komunikacích, který se okrajově dotýká rovněž ochrany osobních údajů. Jak již bylo v úvodu naznačeno, tento zákon obsahoval kontroverzní právní úpravu povinnosti telefonních operátorů a poskytovatelů internetového připojení uchovávat provozní a lokalizační údaje o veškeré telefonní, faxové, SMS a e-mailové komunikaci, návštěvách webových stránek a využívání některých dalších internetových služeb a povinnosti tyto údaje poskytovat oprávněným orgánům. V souvislosti s ústavní stížností podanou skupinou poslanců, jíž tuto úpravu napadli, se zabýval otázkou ochrany soukromí na internetu (a v případě používání telefonních sítí) Ústavní soud. Nálezem Pl. ÚS 24/10 ze dne 22. března 2011, publikovaném ve Sbírce zákonů pod číslem 94/2011 Sb., zrušil ustanovení § 97 odst. 3 a 4 zák. č. 127/2005 Sb., o elektronických komunikacích, a prováděcí právní předpis - vyhlášku č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

V nálezu Ústavní soud posuzoval ústavnost uchovávání technických údajů z důvodu jejich předávání oprávněným orgánům pro potřeby vyšetřování trestné činnosti. Byť se tedy jednalo zejména o ochranu soukromí vůči státním orgánům ve specifické situaci trestního vyšetřování, z širší perspektivy ochrany soukromí na internetu a případné budoucí právní úpravy je podstatné, že Ústavní soud zhodnotil zejména aspekty práva na soukromí a možnosti jeho omezení. Nejprve se v nálezu konstatuje, že koncept ochrany soukromí je nejčastěji spojován se západní kulturou, a to konkrétně anglo-americkou představou zasazenou do politické filosofie liberalismu. Požadavek na respekt soukromí a jeho ochranu se objevuje až s rozvojem technických a technologických možností, které zvyšují i svobodu ohrožující potenciál státu, a proto právo na soukromí není ještě v ústavách ze 40. a 50. let minulého století explicitně zmiňováno. Rovněž tak v Listině je ochrana soukromí[7)] rozložena na různých

[7)] Přičemž právo na soukromí Ústavní soud definuje již v nálezu sp. zn. II. ÚS 2048/09 ze dne 2. 11. 2009 tak, že kromě tradičního chápání prostorového spočívajícího v ochraně obydlí

místech – např. čl. 7 odst. 1, čl. 10, 12 a 13 Listiny, přičemž aspekt ochrany soukromí spočívající v právu na informační sebeurčení lze vyčíst z čl. 10 odst. 3 Listiny. Ústavní soud dospívá k závěru, že v Listině uvedený výčet toho, co lze podřadit pod právo na soukromí, není všeobjímající a konečný a dále, že je nezbytné respektovat účel dynamicky se vyvíjejícího práva na soukromí a uvažovat o něm v jeho celistvosti. Proto i právo na informační sebeurčení spadá mezi základní lidská práva a svobody. Přitom zásah do základního práva z důvodu prevence a ochrany před trestnou činností je možný pouze skrz imperativní zákonnou úpravu, která naplňuje tři základní kritéria proporcionality (v širším smyslu), tj. způsobilosti naplnění účelu, dále pak potřebnosti a přiměřenosti. Ve zkoumaném případě pak rozsah uchovávaných technických dat, doba jejich uchovávání a jejich nadužívání, tj. (ne)vymezení spektra oprávněných orgánů a (ne)vymezení účelu, tedy předávání i v případech, kdy se nejedná o zvlášť závažné trestné činy a kdy účelu lze dosáhnout i jinak, vedly k tomu, že Ústavní soud příslušná zákonná ustanovení včetně prováděcího předpisu zrušil.

Z širšího pohledu ochrany soukromí a uchovávání údajů provozovateli internetových služeb je velmi zajímavé vyjádření Ústavního soudu ve formě obiter dicta[8]: „V neposlední řadě považuje Ústavní soud za nutné vyjádřit pochybnosti i nad tím, zda je vůbec žádoucí, aby soukromé osoby (poskytovatelé služeb v oblasti internetu a telefonní a mobilní komunikace, zejm. mobilní operátoři a obchodní společnosti zajišťující připojení k internetu) byly nadány oprávněním uchovávat veškeré údaje o jimi poskytované komunikaci i o zákaznících, jimž jsou jejich služby poskytovány (tzn. údaje jdoucí i nad rozsah údajů, jež jsou dle napadené právní úpravy povinny uchovávat), a volně s nimi za účelem vymáhání pohledávek, rozvoje obchodní činnosti a marketingu disponovaly. Tato skutečnost se Ústavnímu soudu jeví jako nežádoucí zejména z toho důvodu, že v zákoně o elektronických komunikacích ani v jiných právních předpisech není toto oprávnění a jeho účel blíže a podrobněji regulován, nejsou striktně vymezena práva a povinnosti, rozsah uchovávaných údajů, doba a způsob uchovávání, stejně jako nejsou blíže konkretizovány požadavky na jejich zabezpečení a kontrolní mechanismy." Tolik nepřímá výzva zákonodárci k přijetí potřebné úpravy.

5. Závěr

Možnosti zneužití osobních údajů na internetu jsou velmi široké a právní úprava jejich ochrany za překotným vývojem technologií stále zaostává. Přitom si uživatelé často ani možnost zneužití svých dat neuvědomují. Uživatelé mohou být při použití online služby spojeni s on-line identifikátory, jež produkují jejich zařízení, aplikace,

---

a autonomní existenci veřejnou mocí nerušených sociálních vztahů: „ ... zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný v čl. 10 odst. 3 Listiny."

[8] Bod 57 nálezu Pl. ÚS 24/10 ze dne 22. března 2011.

nástroje a protokoly, jako je například internetový protokol adresy nebo cookie identifikátory. Tyto identifikátory mohou zanechat stopy, které v kombinaci s jedinečnými identifikátory a jinými informacemi obdrženými servery mohou být použity k vytvoření profilů osob a k jejich identifikaci. Zneužití takovýchto profilů není dostatečně právně regulováno. Je možné kvitovat, že z pohledu nadměrného shromažďování takovýchto dat pro účely jejich předávání orgánům činným v trestním řízení se vypořádal v loňském roce Ústavní soud. Nicméně stále zbývá velmi široký prostor pro pozitivní normotvorbu, což mimo jiné obiter dictum Ústavní soud naznačil.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)[9], byl sice po vydání nálezu Ústavního soudu novelizován zákonem č. 468/2011 Sb., účinným ke dni 1. 1. 2012. Avšak zákonodárce se pokusil upravit zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací v zásadě pouze v § 88. Toto ustanovení upravuje povinnost podnikatele poskytujícího službu elektronických komunikací informovat Úřad pro ochranu osobních údajů o porušení ochrany osobních údajů o tom, jaká opatření přijal, případně hodlá přijmout. V případě, že by takové porušení bylo způsobilé zvlášť závažným způsobem ovlivnit soukromí fyzické osoby, nebo jestliže neprovede opatření, kterými je stav porušení napraven, pak je povinen o porušení ochrany informovat i tuto osobu. Zároveň byly rozšířeny kompetence Úřadu pro ochranu osobních údajů. Tato úprava však není dostačující a ani nedosahuje úrovně informačních povinností stanovených v článku 32 návrhu nařízení EU, jak bylo popsáno výše.

V současnosti je ve fázi návrhu novely zákona č. 127/2005 Sb.[10], projednávána v Poslanecké sněmovně úprava, která v zásadě vrací zákon do původního znění před zrušením předmětných ustanovení citovaným nálezem Ústavního soudu. Do jisté míry zpřísňuje podmínky, za jakých se provozní a lokalizační údaje uchovávají a definuje okruh orgánů, jež mohou jejich poskytnutí požadovat. Kromě toho, že je pro uchovávání dat jasně stanovena lhůta 6 měsíců, po jejímž uplynutí musí povinné subjekty nevyžádaná data zlikvidovat, však de facto mnoho nového takto připravená novela v případě přijetí nepřinese. Okruh oprávněných orgánů a důvody, kdy mohou poskytnutí dat požadovat (blíže definované v souběžně navrhované úpravě ustanovení § 88a trestního řádu), jsou stanoveny velmi široce, v zásadě tedy nepřinášejí oproti předchozímu stavu žádné omezení. Nadto ustanovení ukládající povinnost zajistit

---

[9] Z pohledu ochrany osobních údajů, obsahuje zák. č. 127/2005 Sb. následující ustanovení: oprávnění Českého telekomunikačního úřadu stanovit všeobecným oprávněním konkrétní podmínky ochrany osobních údajů a soukromí [§ 10 odst. 1 písm. f)]; osobní údaje v telefonních seznamech nebo databázích, podle nichž se poskytují informace o telefonních číslech účastníků, právo odmítnout uveřejnění těchto údajů (§ 41 a § 95); identifikace zlomyslných nebo obtěžujících volání (§ 67); ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací (§ 87 až § 97); zneužití elektronické adresy odesílatele (§ 93); zákaz nabídky zboží a služeb, zákaz poskytovat údaje, které nejsou obsaženy ve veřejném seznamu (§ 96); odposlech a záznam zpráv (§ 97); správní delikty (§ 118 až § 121).

[10] Dne 14. června 2012 byl v Poslanecké sněmovně návrh zákona projednán coby sněmovní tisk 615/0 ve druhém čtení.

ochranu údajů s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany, je vágní. Konečně, novela se rozhodně žádným způsobem nevypořádává s daty o uživatelích, jež provozovatelé služeb na internetu uchovávají a zpracovávají o vlastní vůli a tuto oblast tedy zcela zanedbává.

Lze tedy shrnout, že vzhledem k závažnosti možných důsledků zásahů do soukromí se nejeví stávající česká právní úprava dostatečnou. Na poli Evropské unie i Rady Evropy, ať už jde o právně nezávazná doporučení, nebo nařízení, které je doposud ve fázi návrhu, se rodí minimálně dostatek podnětů pro novou právní úpravu a lze tedy jen věřit, že se ji podaří připravit co nejdříve.

Shrnutí:

Prudký vývoj internetu a technologií umožňujících neomezené uchovávání dat, jejich propojování a další zpracování, činí dosavadní právní úpravu ochrany soukromí nedostatečnou. Ústavní soud v nálezu Pl. ÚS 24/10 zrušil ustanovení zákona č. 127/2005 Sb. o elektronických komunikacích upravující velmi širokou povinnost provozovatelů shromažďovat technická data a tato předávat orgánům činným v trestním řízení. Zároveň s tím blíže definoval právo na soukromí. Na pozitivní normotvorbu v oblasti ochrany soukromí na internetu v České republice však stále čekáme. Na úrovni EU pak roztříštěnost národních úprav ochrany dat členských států vedla Komisi k přípravě návrhu nařízení, jež rozšiřuje práva fyzických osob, jejichž osobní údaje jsou shromažďovány. Dále Výbor ministrů Rady Evropy přijal dvě doporučení ohledně ochrany soukromí při používání vyhledavačů a služeb sociálních sítí. Pro českého zákonodárce tak existuje z pohledu de lege ferenda dostatek nápadů.

Privacy on the Internet Protection - draft EU Regulation and the Adopted Recommendations of the Council of Europe Comittee of Ministers – summary:

The rapid development of Internet and technology allowing for unlimited data storage, their interconnection, and further processing, renders the existing legislation on privacy inadequate. The Constitutional Court judgment Pl. U.S. 24/10 abolished the provisions of Act No. 127/2005 Coll. Electronic Communications regulating a wide duty of collecting technical data and delivering those to the police, prosecution and criminal courts. The Constitutional Court also further defined the right to privacy. However, the positive law-making in the field of Internet privacy is still awaited in the Czech Republic. On the EU level, the fragmentation of national data protection arrangements of Member States has led the Commission to preparation of a proposal for regulation which extends the rights of the individuals whose personal data are collected. Furthermore, the Council of Europe Committee of Ministers has adopted two recommendations concerning the protection of privacy when using search engines and social networking services. Therefore, there is enough in terms of legal ideas to build on for the Czech legislator.