Svoboda "v síti"

David C. Hájiček

Resume
This thesis focus on the legal aspects of privacy protection in the environment of data networks, especially the Internet. There is the information technology attack defined in the beginning of the document, following by typical attacks known. Those targeting on the privacy are pointed out and divided into the two basic categories: PUSH and PULL, also explained in the document. In the second part, the actual legal consequences in Czech Republic and European Union are discussed. The legal view is described from the administrative law and criminal law perspectives. The second part is divided into the two logical chapters, first summarizing existing laws and highlighting consequential sections and definitions, second explaining how those sections and definitions can be enforced in the practice. As the "European arrest warrant and the surrender procedures between Member states" is one of the European tools helping to enforce (among others) the privacy, the last part brings a brief overview of main principles discussed in that document and describes, how they have been implemented into the Czech legislation. There has been no space to analyze the national legislation in the area of privacy of other important countries (e. g. USA, China) in the thesis, neither to discuss this topic from the international perspective.

Svoboda "v síti"
V souvislosti s rozšiřováním komunikačních technologií se čím dál častěji setkáváme s obavami uživatelů o některé aspekty svých základních práv. Jedná se zejména o obavy o vlastní **soukromí** (v poslední době čím dál častěji rovněž o **vlastnictví**) přičemž v obou případech jde o hodnoty "nejvyšší" – tedy chráněné Listinou základních práv a svobod ČR (dále LZPS)[1] i například Listinou základních práv Evropské unie (dále LZPEU)[2]. Zmiňovaná práva jsou chráněna i dalšími mezinárodními instrumenty – například Evropskou úmluvou o ochraně lidských práv a základních svobod[3] nebo i mezinárodními smlouvami mezinárodního práva veřejného. V práci se zaměřujeme zejména na ochranu soukromí[4]. Cílem práce je definovat typy jednání zasahujících do soukromí uživatelů počítačových sítí a popsat existující českou a evropskou legislativu umožňující obranu proti takovému jednání.

Útoky proti soukromí
V úvodu je vhodné definovat, co je počítačový útok. Lze ho popsat jako související aktivity rozdělené do 5 fází:

- footprinting (fáze sběru informací, mapování a modelování kompletního profilu útočníkova cíle),
- scanning (zjišťování technických specifik v cílových systémech),
- enumeration (nalézání slabin ve zjištěných specifikách),
- využití nalezených slabin k provedení samotného útoku,
- zahlazení stop[5].

Z technického hlediska lze dále rozlišovat na automatizované a manuální útoky. Automatizované jsou ty, kdy je aktivita útočníka patrná převážně v počátcích útoku (příprava software určeného k útoku) a samotný útok potom probíhá bez jeho výrazného zásahu. Automatizované útoky mají zpravidla za úkol zjišťovat a sbírat[6] o uživateli informace (osobní údaje, autentizační data apod.), případně mu zobrazovat vybrané informace (např. reklamy). U automatizovaných útoků proti soukromí uživatele se jen velmi vzácně setkáváme s cílem poškodit rovněž zařízení uživatele nebo využívat jeho zdroje pro potřeby útočníka.

Manuální útoky potom předpokládají zapojení útočníka v průběhu všech fází útoku. Jsou velmi často zahajovány těmi automatizovanými (zejména v prvních třech fázích), případně se setkáváme s jejich kombinacemi. V takových případech je do soukromí uživatele zasahováno z důvodu přípravy jiných útoků (často trestných činů), například proti vlastnictví.

Nejčastějšími druhy útoků jsou[7]:

- Malware ("computer contaminant"; automatizované útoky)
  - virus (škodlivý program schopný se dále šířit, s různými schopnostmi a vlastnostmi),
  - červ (umí se sám šířit – replikovat, může mít různou funkčnost – jako virus),
  - trojský kůň (škodlivý program, zakrývající své skutečné chování jiným účelem),
  - backdoor (tzv. "zadní vrátka" vytvořená programátorem pro pozdější převzetí kontroly nad programem – například přímo v kódu uložené uživatelské jméno a heslo, skryté legálním uživatelům programu),
  - keylogger (program tajně zaznamenávající znaky zadávané uživatelem – například hesla – s cílem zpřístupnit je útočníkovi),
  - spyware (programy odesílající dat bez vědomí uživatele),

1 Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění ústavního zákona č. 162/1998 Sb.

2 Listina základních práv Evropské unie (2007/C 303/01).

3 ve znění protokolů č. 3, 5, 8 a 11, vyhlášena 4. 11. 1950 Radou Evropy v Římě.

4 LZPS v článku 7, odst. 1) stanoví, že "Nedotknutelnost osoby a jejího soukromí je zaručena." Otázku ochrany soukromí dále řeší v článku 10, především odst. 2) a 3); LZPEU potom předmětné téma upravují články 7 a 8.

5 srov. McClure, S., Scambray, J., Kurtz, G. *Hacking Exposed.* 6th Edition. New York: Nakladatelství McGraw Hill, 2009. s. 7-157.

6 U útoků na soukromí uživatelů zpravidla hovoříme o převzetí dat, velmi vzácně sebrání (data nejsou totiž ve většině případů pevně vázána na nosič, po útoku tak zpravidla zůstávají ve vlastnictví jejich původce a ten neztrácí možnost s nimi disponovat).

7 Předmětem článku není podat vyčerpávající informace o typech počítačových útoků, jsou uvedeny pouze ty, které jsou významné pro zvolené téma.

    - adware (programy zobrazující nevyžádaná sdělení),
    - robot (crawler, spider; sbírají data procházením sítě a následně je prezentují uživateli/útočníkovi).
- Předstírání identity (automatizované/manuální útoky)
    - pharming (přepsání záznamu v DNS a předstírání cizí identity),
    - phishing (rozesílání e-mailových zpráv vybízejících cíl útoku, aby klikl na odkaz uvedený v těle e-mailu; uživatel tak učiní v domění, že se připojuje k důvěryhodnému systému – například k bankovním službám – a je přesměrován na stránky útočníka),
    - podvržení (například podvržení serverové certifikátu, předstírajíc cizí identitu),
    - sociální sítě (uživatelé o sobě sami a dobrovolně zveřejňují nepřiměřené množství osobních, často citlivých údajů[8]).
- Exploit (využití zranitelnosti v některé ze služeb běžící na cílovém počítači; manuální útoky)
    - system Hacking (ovládnutí cílového počítače útočníkem),
    - cross-Site-Scripting (XSS; využití chyb ve zdrojovém kódu webových stránek hostitele, jehož služby cíl útočníka využívá),
    - noti a Zombie (programy neautorizovaně nainstalované do prostředí cíle útočníka, konzumující systémové prostředky uživatele, využívané v tzv. Botnetech pro různé typy útoků).
- Zachycení/podvržení komunikace (manuální útoky)
    - man-in-the-Middle (neautorizované vstoupení do komunikace mezi dvěma stranami, kdy útočník v komunikaci se stranou A předstírá, že je strana B a naopak),
    - e-mail Hacking (zachytávání a neautorizované čtení e-mailů[9]).
- Spamming (zasílání nevyžádaných sdělení[10]).

Jak je patrné z uvedeného rozdělení, útoky proti soukromí – tedy vlastně i osobnosti – lze dále rozdělit na PULL (kdy se útočník snaží získat informace) a PUSH (kdy útočník naopak některé informace sděluje a tím narušuje soukromí uživatelů), přičemž fatálnější dopady mají (až na výjimky[11]) útoky typu PULL. Na základě takto získaných dat totiž může útočník rozvíjet útoky do dalších oblastí, případně zvyšovat dopady již provedených útoků – motivem je pak pro útočníky především obohacení, či získání jiných výhod (například prostřednictvím vydírání).

Původce automatizovaných útoků – zejména autory malware – nemusí být vždy snadné (či dokonce možné) identifikovat. U manuálních útoků je to s určením útočníka o poznání snazší – často lze totiž (v závislosti na legislativě zemí, přes něž či z nichž útočník svůj útok vede) lokalizovat jejich zdroj. Alespoň na území Evropské unie by potom mělo být možné jít při identifikaci až do úrovně konkrétních fyzických či právnických osob[12]. Proto i právní ochrana před těmito typy útoků je o poznání konkrétnější.

V dalších částech práce je pozornost věnována především PULL útokům, a to zejména těm, při kterých je možné identifikovat útočníka.

Současný stav ochrany soukromí v ČR a EU

Právní úprava ochrany soukromí v ČR a EU

Útočníci se mohou svojí činností dopouštět *správních deliktů* nebo *trestných činů*. Správní delikt je souhrnné označení pro *přestupky* a *jiné správní delikty*. V obou případech se jedná o protiprávní jednání stanovené zákonem (a to i neúmyslné), za které ukládá správní orgán ve správním řízení[13] zákonem stanovenou sankci, rozdíl spočívá v tom, že přestupku se může dopustit pouze fyzická osoba, zatímco jiného správního deliktu právnická osoba, resp. fyzická osoba podnikající.

Trestný čin[14] (u mladistvých pachatelů nazývaný *provinění*) je delikt závažnější než přestupek (správní delikt) a může být spáchán pouze fyzickou osobou. Protiprávní čin je trestným činem, je-li formálně naplněna skutková podstata trestného činu. Trestné činy dělí trestní zákoník dále na zločiny a přečiny, kteréžto rozlišuje sazba trestu odnětí svobody, případně úmysl při jejich spáchání (do 3 let jde o přečin, stejně jako v případně spáchání z nedbalosti).

V případě správního deliktu ani trestného činu směřujícího do oblasti soukromí v prostředí datových sítí nelze příliš předpokládat, že by útočník jednal v rámci nutné obrany či krajní nouze (a tím se vyhnul zodpovědnosti za své konání), avšak nejsou ojedinělé případy, kdy útočník nedosáhl ještě 15 let věku či nemohl rozpoznat nebezpečnost svého jednání díky duševní poruše.

Následující kapitoly se zaměřují na správněprávní, resp. trestněprávní ochranu proti útokům na soukromí.

8 Definice dle z. č. 101/2000 Sb., o ochraně osobních údajů.

9 V nedávné minulosti bylo toto téma velmi aktuálním, zejména ve vztahu k oprávnění zaměstnavatele číst elektronickou poštu svých zaměstnanců. Odborná veřejnost se shoduje, že obsah obecně všech elektronických zpráv je chráněn na základě článku 13 LZPS. Problematika ochrany elektronické korespondence je upravena rovněž Směrnice č. 2002/58/ES Evropského parlamentu a Rady upravující zpracování osobních údajů a ochrany soukromí v oblasti elektronických komunikací. Obecně je obsah e-mailové komunikace považován za listovní tajemství a měly by se na něj proto vztahovat ustanovení z. č. 29/2000 Sb., O poštovních službách (zejména § 6 odst. 6). Přesto se lze v praxi setkat s případy, kdy zaměstnavatelé elektronickou poštu svých zaměstnanců monitorují, zpravidla na základě dohody obsažené v pracovní smlouvě.

10 Nevyžádaná obchodní sdělení v prostředí ČR zakazuje například z. č. 480/2004 Sb., o některých službách informační společnosti, který je v § 11 označuje za správní delikt.

11 Míněno zejména použití phishingu, kdy prostřednictvím zasílání nevyžádaných e-mailů pod cizí identitou (PUSH) je útok zaměřen na získání osobních údajů.

12 Viz dále – zejména zákon o elektronických komunikacích.

13 Správní řízení je vedeno dle z. č. 500/2004 Sb., správní řád, v případě řízení o přestupcích pak rovněž dle z. č. 200/1990 Sb., o přestupcích.

14 Definovaný v zákoně č. 40/2009 Sb., trestní zákoník.

Správně právní úprava

Vedle v úvodu zmiňovaných základních listin je soukromí v českých podmínkách definováno zákonem o ochraně osobních údajů[15]. Ten se dle ustanovení §3, odst. 3 nevztahuje *na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.* Dříve ÚOOÚ používal pro popsání výjimky také slov „nahodilé" či „nesystémové" zpracování. Zákon tedy upravuje především systematické zpracování osobních údajů. Ochranu před jednorázovými, resp. nesystematickými zásahy do soukromí jednotlivce pak upravují §§ 11–17 občanského zákoníku[16]. Přestože jsou předmětná ustanovení podřazena pod název „Ochrana osobnosti," je možné je aplikovat na diskutované téma – ochranu soukromí. Stejně tak zákon o ochraně osobních údajů lze brát jako nástroj ochrany soukromí, a vlastně i ochrany osobnosti.

Zákon o ochraně osobních údajů rozlišuje dva základní pojmy: *osobní, případně citlivý údaj.* § 4, odst. a) považuje osobní údaj za jakoukoliv informaci *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.* Tato definice je poměrně široká a dává prostor různým interpretacím. Za povšimnutí stojí také na první pohled vágní formulace „určený" a „určitelný." Zcela bez zajímavosti z tohoto pohledu není skutečnost, že § 18, odst. 2) správního řádu[17] má o údajích nutných k identifikaci zcela konkrétní představu: *Údaji umožňujícími identifikaci fyzické osoby se rozumějí jméno, příjmení, datum narození a místo trvalého pobytu, popřípadě jiný údaj podle zvláštního zákona.*

Zákon o ochraně osobních údajů však transponuje směrnici Evropského parlamentu a Rady 95/46/ES (dále Směrnice) a volná definice osobních údajů je se směrnicí v souladu. Oproti taxativnímu vymezení totiž umožňuje nahlížet na osobní údaje v kontextu individuálně řešené situace[18].

Český parlament v §2, odst. 1 zákona o ochraně osobních údajů zřídil, v souladu s požadavkem článku 28 Směrnice, Úřad pro ochranu osobních údajů, jemuž svěřil *kompetence ústředního správního orgánu pro oblast ochrany osobních údajů.* Směrnice sama nezřizuje žádný ústřední kontrolní orgán, pouze pracovní skupinu (články 29 a 30), s funkcí nezávislého poradního orgánu.

Vymoženost ústředního nadřazeného úřadu evropského „kalibru" přichází až s Nařízením Evropského parlamentu a Rady 45/2001/ES které zřizuje Evropského inspektora ochrany osobních údajů[19]. K tomu rovněž zavádí opravné prostředky (možnost podat žalobu k Soudnímu dvoru Evropské unie, možnost stížnosti Evropskému inspektorovi). Nařízení dále řeší zásady pro kvalitu, zásady pro legitimní zpracování, diskutuje zvláštní kategorie osobních údajů, dále se věnuje informování subjektů osobních údajů, jejich právům, výjimkám a omezením, důvěrné povaze a bezpečnosti zpracování a ochranu osobních údajů a soukromí v rámci vnitřních telekomunikačních sítí. Nutno však dodat, že nařízení se zaměřuje na ochranu fyzických osob v souvislosti se zpracováními osobních údajů orgány a institucemi Evropské unie, neupravuje tedy problematiku ochrany soukromí proti výše jmenovaným typům útoků.

Stále sílící fenomén užívání komunikačních sítí, zejména potom Internetu, dává vzniknout debatám na národních, evropských i mezinárodních úrovních. Ochraně osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích věnuje pozornost Směrnice Evropského parlamentu a Rady 2002/58/ES. Podle ní má poskytovatel takových veřejně dostupných služeb má povinnost zajistit jejich bezpečnost, členské státy potom musí garantovat uživatelům služeb důvěrnost sdělení. Směrnice dále upravuje použití provozních a lokalizačních údajů, možné omezení identifikace volajícího, podrobné vyúčtování služeb či tvorbu, údržbu a poskytování účastnických seznamů. Zajímavým bodem je ustanovení článku 13, který ustavuje, že automatizovaně zasílaná obchodní sdělení (potenciální útok typu PUSH) je možné takto zasílat pouze s předchozím souhlasem adresáta. V ČR jsou zmiňované požadavky transponovány do praxe zákonem o službách informační společnosti[20]. Orgánem dohlížejícím na dodržování zákazu nevyžádaných obchodních sdělení byl určen ÚOOÚ.

Za zmínku stojí skutečnost, že zatímco Směrnice 2002/58/ES připouští možnost, aby *členské státy mohly přijmout legislativní opatření, kterými omezí rozsah práv a povinností* důvěrného charakteru sdělení ochrany provozních údajů[21], *pokud toto omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému*, Směrnice 2006/24/ES[22] takovéto jednání přímo vyžaduje. Povinnost uchovávat určitý typ údajů o komunikaci jednotlivých stran (uživatelů veřejně dostupných služeb informační společnosti) zakotvuje ve svém v článku 3 a prohlašuje ji za závaznou pro poskytovatele veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

Uchovávané údaje[23], tedy zejména identifikace uživatele (jméno a adresa obou komunikujících stran) a jeho označení v síti, datum a čas sestavení a přerušení spojení (přihlášení a odhlášení ke službě), typ použité služby a jednoznačné označení koncového (přípojného) bodu účastníka, mají být dle ustanovení článku 4 poskytovány pouze příslušným vnitrostátním orgánům

15 zákon č. 101/2000 Sb., o ochraně osobních údajů.

16 zákon č. 40/1964 Sb., občanský zákoník.

17 zákon č. 50/2004 Sb., správní řád.

18 Směrnice 95/46/ES v článku 2, písm. a) přesto uvádí příklady osobních údajů.

19 Viz stránky Evropské komise, European Union, 1995-2012, dostupné z <http://ec.europa.eu/dataprotectionofficer/>.

20 Srov. y. č. 480/2004 Sb., o některých službách informační společnosti.

21 Srov. Článek 13 Směrnice Evropského parlamentu a Rady 2002/58/ES.

22 Směrnice Evropského parlamentu a Rady 2006/58/ES.

23 Srov. Směrnice Evropského parlamentu a Rady 2006/24/ES, článek 5 (směrnice známá také jako data retention).

v souladu s požadavky nezbytnosti a přiměřenosti. Ty mají mít na vyžádání 6 měsíců až 2 roky. Článek 5 dále explicitně stanoví, že *nesmí být uchovávány údaje odhalující obsah sdělení*.

Česká republika transponovala povinnosti vyplývající ze směrnice zákonem o elektronických komunikacích[24] a prováděcí vyhláškou[25]. Několik málo let nato však byla na popud skupiny poslanců vedených M. Bendou nálezem Ústavního soudu ČR[26] ustanovení § 97, odst. 3 a 4, včetně prováděcí vyhlášky, zrušena. To však neznamená, že směrnice o data retention nebude do českých podmínek transponována – můžeme jen doufat, že druhý pokus se již legislativcům povede lépe[27].

Trestněprávní úprava

Trestným činům v oblasti ochrany soukromí (dále pak i osobnosti a listovního tajemství) se věnuje trestní zákoník[28] v části druhé, Hlavě II, Dílu 2. Ten v odst. 1 § 180 stanovuje trestní hranici odnětí svobody až 3 roky či zákaz činnosti tomu, kdo *neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné* ***v souvislosti s výkonem veřejné moci****, poruší státem uloženou nebo uznanou povinnost mlčenlivosti* o osobních údajích a způsobí mu tak vážnou újmu. V odst. 2 stanovuje trestní sazbu v rozmezí 1 roku až 5 let (případně peněžitý trest či zákaz činnosti), pokud tak učiní jako člen organizované skupiny, použije prostředky hromadné komunikace, způsobí značnou škodu nebo tak učiní v úmyslu získat značný prospěch. Trestem odnětí svobody na 3 roky až 8 let pak může být potrestán ten, kdo uvedeným jednáním způsobí škodu velkého rozsahu či získá prospěch velkého rozsahu.

§ 182 trestního zákoníku dále stanovuje tresty za narušení důvěrnosti datové komunikace či jiný způsob neoprávněného získávání dat ve výši až 2 let či zákaz činnosti. Odstavce 5 a 6 stanovují tresty pro zaměstnance provozovatelů datových a komunikačních služeb.

Tresty za spáchání trestného činu v rámci organizované skupiny, ze zavrženíhodné pohnutky, způsobení značné škody či za účelem získání značného prospěchu samozřejmě trestní hranici zvyšují. A to i v případě porušení tajemství dokumentů uchovávaných v soukromí (§ 183), kde základní sazba je 1 rok až 3 roky.

Prosazování ochrany soukromí v ČR a EU

Prosazování správněprávní úpravy

Správněprávní ochrana, tedy řízení ve správním soudnictví, se opírá primárně o soudní řád správní[29] a o správní větev obecného soudnictví. Oběť útoku proti soukromí má možnost (už jen při podezření na porušení svých práv v oblasti ochrany osobních údajů) obrátit se na příslušný správní orgán určený k projednání přestupku či jiného správního deliktu v prvním stupni (ÚOOÚ). Ten z úřední povinnosti projednává přestupky či jiné správní delikty, přičemž správní řízení orgán zahajuje, jakmile nastanou a jsou mu známy skutečnosti, které zahájení řízení odůvodňují (to znamená, že krom podaného podnětu či stížnosti může orgán kontrolní činností porušení zákona zjistit rovněž sám). Po projednání přestupku či jiného správního deliktu vydá rozhodnutí[30], proti kterému je přípustný rozklad k odvolacímu orgánu (předsedovi ÚOOÚ) podaný účastníkem řízení[31].

Dnem účinnosti zákona o ochraně osobních údajů pozbyly české soudy pravomoci rozhodovat v otázkách ochrany osobních údajů (dle zákona o ochraně osobních údajů), což ovšem neznamená, že uživatel nemá možnost u soudu požadovat přezkoumání správního rozhodnutí dozorového orgánu pro ochranu osobních údajů.

Opravný prostředek k tomu určený je žaloba podaná proti rozhodnutí ÚOOÚ ke krajskému soudu. V dalším stupni v rámci soudní moci České republiky je možné proti rozhodnutí krajského soudu podat kasační stížnost k projednání nejvyššímu správnímu soudu.

Jedná-li se o narušení soukromí některým orgánem či institucí zřízenou Smlouvami o založení Evropských společenství nebo na jejich základě, má uživatel možnost (jak bylo uvedeno výše), podat stížnost Evropskému inspektoru ochrany údajů. Proti jeho rozhodnutím *lze podat žalobu k Soudnímu dvoru Evropské unie*[32].

Prosazování trestně úpravy

Trestní řízení[33], v rámci kterého jsou projednávány (mimo jiné) trestné činy proti soukromí, zahajují orgány činné v trestním řízení – přesněji řečeno policejní orgány – na základě trestního oznámení (nebo dozví-li se o pravděpodobném spáchání trestného činu jiným způsobem). Trestní oznámení je možné učinit přímo některému z útvarů Policie ČR nebo státnímu zastupitelství. Po zahájení trestního řízení se orgány činné v trestním

24 Srov. z. č. 127/2005 Sb., o elektronických komunikacích.

25 Vyhláška Ministerstva informatiky a Ministerstva vnitra č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

26 Spisová značka Pl. ÚS 24/10; mezi hlavní argumenty patřilo neúměrné zasahování do soukromí osob (článek 10, odst. 3 a článek 13 LZPS), nejasná specifikace orgánů oprávněných vyžadovat lokalizační a provozní údaje, chybějící jednoznačný účel, za jakým jsou lokalizační a provozní údaje oprávněným orgánům poskytovány a absence bezpečnostních opatření, které má poskytovatel služeb aplikovat za účelem ochrany (zajištění dostupnosti, důvěrnosti a integrity) provozních a lokalizačních údajů.

27 Za zmínku rovněž stojí skutečnost, že sběr obrovského objemu dat, kterými plošně sbírané provozní a lokalizační údaje jsou, a jejich uchovávání (v našich podmínkách po dobu 6–12 měsíců) budou znamenat značnou finanční zátěž pro poskytovatele veřejně dostupných služeb elektronických komunikací, která ve finále dopadne na samotné uživatele, v tomto případu na ty, jejichž soukromí bude „narušováno." Či ještě hůře na daňové poplatníky, přičemž efektivita zaváděného opatření je v našem prostředí diskutabilní (jako příklad uveďme argument Ústavního soudu, opírající se o tvrzení J. Herczega v Bulletinu advokacie č. 5/2010 na straně 29, že za období leden–říjen 2009 byla žádost o poskytnutí provozních a lokalizačních údajů učiněna 121 839 krát, zatímco počet objasněných případů z celkových 343 799 trestných činů zjištěných na našem území za toto období dosáhla čísla 131 560 – jak vyplývá ze zprávy Komise EU – „The Evaluation of Directive 2006/24/ES and National Measures to Combat criminal Misuse and Anonzmous Use of Electronic Data.").

28 Srov. z. č. 40/2009 Sb., trestní zákoník.

29 Srov. z. č. 150/2002 Sb., soudní řád správní.

30 V rozhodnutí mohou být uloženy tyto sankce: napomenutí, pokuta, zákaz činnosti, propadnutí věci; v případě ochrany osobních údajů zákon umožňuje pouze uložit pokutu, a to v krajních případech až do výše 10.000.000 Kč.

31 Účastníkem řízení je pouze osoba podezřelá z porušení zákona, nikoliv oběť útoku; ta má možnost vůči útočníkovi uplatňovat právo na náhradu škody nemajetkové újmy podle hmotněprávních předpisů v adhezním řízení: zákon č. 40/1964 Sb., občanský zákoník, zákon č. 513/1991 Sb., obchodní zákoník.

32 Srov. článek č. 32, odst. 3 Směrnice 2001/45/ES.

33 Trestní řízení je vedeno dle zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

řízení věnují sběru důkazního materiálu a zjišťování důležitých okolností. Nasvědčují-li tyto podklady, že byl trestný čin spáchán, je orgánem činným v trestním řízení zahájeno trestní stíhání, následně podán návrh státnímu zástupci na podání žaloby k okresnímu či krajskému soudu.

Vzhledem k charakteru sítí, zejména potom Internetu, není v některých případech zcela jednoduché uvedený postup aplikovat. Často totiž nastávají situace, kdy útočník vede útok na oběť v jiném státě, v jiném kontinentě či využívá zařízení umístěné v jiném státě, než ve kterém se nachází on sám i oběť. V oblasti moci výkonné se Rada Evropské unie snaží na tento fakt reagovat (alespoň na území Evropské unie) rámcovým rozhodnutím o evropském zatýkacím rozkazu[34]. To umožňuje „příslušnému orgánu[35]“ vyžadujícího státu vystavit evropský zatýkací rozkaz vyplněním předepsaného formuláře a požádat tak o vydání osoby z jiného členského státu Evropské unie pro účely výkonu trestu odnětí svobody či trestního stíhání. Následně jej zašle příslušnému orgánu[36] (justičnímu, nikoliv výkonnému) vykonávajícímu členskému státu, který by měl o vydání ve lhůtě 60 dnů rozhodnout.

Evropský zatýkací rozkaz v některých případech prolamuje nutnost ověření oboustranné trestnosti činu. A to v případě je-li možné trestný čin, pro který byl zatykač vydán, ve vystavujícím státě potrestat trestem odnětí svobody s horní hranicí minimálně 3 let, jde-li (mezi jinými) o počítačovou trestnou činnost[37]. Porušení zákona o ochraně osobních údajů sám zákon klasifikuje jako přestupky či správní delikty, samotné jeho porušení tedy trestným činem není. Oporu je tak nutné hledat v trestním zákoníku, který v ustanovení § 230 odst. 1 stanovuje výši maximálního trestu pro toho, kdo *překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části*, na 1 rok odnětí svobody. Odst. 2 téhož § potom zvyšuje hranici na 2 léta pro případy získání přístupu k počítačovým systémům nebo nosičům dat při neoprávněném užití dat, neoprávněném narušení jejich integrity, jejich padělání či vložení. To samo o sobě stačí pouze na uplatnění odst. 1 článku 2 Rozhodnutí o evropském zatykači (tedy oboustranná trestnost je nadále vyžadována), nicméně o vydání je již možné požádat, je-li čin oboustranně trestný.

Aby bylo možné vyhnout se ověření oboustranné trestnosti činu, bylo by nutné prokázat úmysl pachatele způsobit škodu nebo újmu, či získat neoprávněný prospěch a/nebo úmysl neoprávněně omezit funkčnost počítačového systému (ustanovení § 230, odst. 3 stanovuje v těchto případech trest ve výši 6 měsíců až 3 léta). Druhou možností je prokázat členství v organizované skupině při spáchání činu, způsobení značné škody, vážné poruchy v činnosti orgánu veřejné moci, získání značného prospěchu či způsobení vážné poruchy v činnosti právnické nebo fyzické osoby, která je podnikatelem (na tyto případy pamatuje § 230, odst. 4 sazbou odnětí svobody na 1 rok až 5 let). Třetí možnost je potom prokázání, že byla způsobena škoda velkého rozsahu nebo že pachatel získal prospěch velkého rozsahu (dle ustanovení § 230, odst. 5 je možné takový čin potrestat odnětím svobody na tři léta až osm let).

Ve všech případech je třeba, aby byl pachatel již za trestný čin odsouzen (zde postačuje, aby byl odsouzen alespoň na 4 měsíce, není-li prolomena zásada oboustranné trestnosti), nebo aby proti němu bylo zahájeno trestní stíhání, a musí být dodržena zásada vzájemnosti. Současně musí být pachatel za trestný čin podle právního řádu ČR v době spáchání trestně odpovědný.

Aby bylo možné pachatele předat z ČR, nesmí být občanem ČR, ani mu nebyla v ČR poskytnuta mezinárodní ochrana (ledaže by s předáním souhlasil). Trestný čin pak dále v našem případě[38]

- nesmí být v ČR promlčen nebo amnestován,
- nesmí spočívat v porušení daňových, celních a devizových předpisů, či jiných finančních práv státu (není-li zaručena vzájemnost),
- nesmí být v ČR (či v některém z cizích států) již rozhodován či rozhodnut,
- nesmí být možné za něj uložit v žádajícím státě trest smrti a nesmí existovat důvodná obava, že trestní řízení by *neodpovídalo zásadám článků 3 a 6 Úmluvy o ochraně lidských práv a základních svobod*, případně že by uložený trest nebyl vykonán v souladu s nimi,
- nesmí existovat důvodná obava, že pachatel *by v dožadujícím státě byl vystavena pronásledování z důvodu svého původu, rasy, náboženství, příslušnosti k určité národnostní nebo jiné skupině, státního občanství nebo pro své politické názory,*
- nesmí pachatele vystavit *vzhledem k jeho věku a osobním poměrům zřejmě nepřiměřenému postihu.*

Každé trestní řízení je ukončováno vydáním rozsudku. Proti tomuto prvoinstančnímu rozhodnutí[39] je přípustné odvolání (o němž je rozhodováno krajským či vrchním souden). To může podat obžalovaný, státní zástupce, oběť či zúčastněná osoba. Konečně proti rozhodnutí krajského nebo vrchního soudu je možné podat dovolání k soudu Nejvyššímu.

V případě vyčerpání veškerých opravných prostředků jak v případě rozhodnutí o trestném činu tak i o správním deliktu je následně možné napadnout rozhodnutí u ústavního soudu ústavní stížností – té však musí předcházet porušení základních práv a svobod, a musí být namířena proti orgánům veřejné moci. Ústavní soud rozhodne vydáním nálezu.

34 Srov. rámcové rozhodnutí Rady Evropské unie č. 2002/584/JHA z 13. 6. 2002 o evropském zatýkacím rozkazu a o předávání mezi členskými státy Evropské unie; v ČR implementované do české legislativy zákonem č. 539/2004, kterým byl změněn trestní řád.

35 V našem prostředí je to Ministerstvo spravedlnosti na žádost soudu, v přípravném řízení soudce rozhoduje o vydání zatykače na návrh státního zástupce.

36 V našem prostředí je krajské státní zastupitelství příslušné místu, kde se zdržuje osoba, na niž byl zatykač vydán, rozhodnutí potom přísluší krajskému soudu.

37 Článek 2, odst. 2 Rámcového rozhodnutí Rady Evropské unie č. 2002/584/JHA.

38 § 393 trestního řádu.

39 Za spáchání trestného činu jsou zpravidla ukládány tresty odnětí svobody. Je-li horní hranice trestní sazby 5 let a více, případně je-li trestný čin spáchán z nedbalosti, jedná se o *přečin*, jinak je protiprávní čin označován jako *zločin*).

Proti nálezu neexistuje opravný prostředek. Jedinou cestou, jak se pokusit nález zvrátit, je podání žaloby proti ČR k Soudnímu dvoru Evropské unie.

Závěr

Jak je patrné z výše uvedených informací, otázka ochrany soukromí jedince v počítačové síti, zejména potom Internetu, je legislativně v naší zemi i v Evropské unii do značné míry upravena i prosazována. Složitější je už mezinárodní situace, které nebylo možné se v této práci s ohledem na požadovaný rozsah věnovat. Bohužel, ani dobrá legislativa však neochrání uživatele před nimi samotnými. V hysterii, která vypukla kolem sociálních sítí, uživatelé o sobě zadávají v nebezpečné míře osobní, často citlivé údaje. Nebo tak činí pod vidinou slev či výher v internetových obchodech. To vše, aniž by si uvědomovali, že tím dobrovolně narušují své soukromí, s omezeným množstvím následné kontroly. Jakmile se jednou objeví data na Internetu, je nesnadné, ne-li nemožné, je odstranit. Osobní údaje uživatelé často sdělují, aniž by věděli, jakému správci je vlastně svěřují do rukou, na jakou dobu a za jakým účelem.

Otázkou tedy je, do jaké míry by měla být v dnešním světě ochrana osobních údajů právně upravena a prosazována. Zda není legislativa zneužitelná kontrolními orgány či „oběťmi" proti „útočníkům." V době, kdy se uživatel datové sítě dobrovolně a někdy zcela zbytečně dělí o své soukromí bez jakékoliv kontroly, nutíme zpracovatele osobních údajů, kteří je řádně zpracovávají k aplikaci často nesmyslných a neúměrně nákladných opatření pod hrozbou sankce.

Přehled aktuální judikatury

Eva Fialová, Matěj Myška, Jaromír Šavelka

Soud	Soudní dvůr Evropské unie
Sp. zn.	C-604/10
Datum	1. 3. 2011
Fáze řízení	předběžná otázka
Dostupnost	http://curia.europa.eu/

Rozhodnutím ve věci Football Dataco a další proti Yahoo UK ! a další přidal Soudní dvůr další díl do své série "databázových rozsudků" z let 2002 a 2004 (Fixtures Marketing (C-46/02; C-338/02 and C-444/02 a British Horseracing Board[1]. Hlavní roli v tomto případu opět hrály rozpisy utkání anglických a skotských fotbalových ligových soutěží, vytvořených podle určitého typu pravidel (tzv. "zlatá pravidla"), k nimž si společnost Football Dataco nárokovala jak právo pořizovatele databáze sui generis, tak práva autorská. Toto tvrzení zpochybňovaly společnosti Yahoo UK ! a tvrdily, že jsou oprávněny předmětné rozpisy používat, aniž by měly povinnost za to Football Dataco poskytovat jakékoli protiplnění. Výše citované předchozí rozsudky již poměrně jasně vymezily podmínky, co je databáze a za jakých podmínek přináleží jejímu pořizovateli zvláštní právo (zejména tedy, že právo sui generis chrání strukturu databáze, nikoliv její obsah a že náklady na pořízení údajů nelze považovat za podstatnou investici do tvorby databáze). Nejasnosti ale vyvstaly ohledně interpretace konceptu originality při tvorbě databáze, kterážto je rozhodující pro možnost chránit databázi autorským právem. Court of Appeal (England & Wales) (Civil Division) tak řízení přerušil a dotázal se Soudního dvora, jak chápat výraz *"databáze, které způsobem výběru nebo uspořádáním obsahu představují vlastní duševní výtvor autora"* (čl. čl. 3 odst. 1 směrnice 96/9). Soudní dvůr ve svém rozsudku definoval kritérium originality[2] jako splněné, v případě, že její *"autor prostřednictvím výběru nebo uspořádání údajů, které databáze obsahuje, vyjádří své tvůrčí schopnosti originálním způsobem prostřednictvím rozhodnutí učiněných na základě své tvůrčí svobody a může tak databázi vtisknout „osobitý charakter"*" (bod 38 rozsudku). Naopak aplikace "zlatých pravidel", byť sebevíce náročná, nedostačuje k tomu, aby bylo kritérium originality splněno. Tyto dopředu dané technické úvahy, pravidla a omezení neponechávají dle Soudu žádný prostor pro tvůrčí svobodu, která jediná je předpokladem originality databáze. Duševní úsilí a dovednosti vynaložené na vytvoření údajů, přidání podstatného významu údajům či značné pracovní úsilí a dovednosti nejsou relevantní pro určení způsobilosti databáze pro ochranu autorským právem (bod 46 rozsudku). Soudní dvůr tak poskytl předkládajícímu soudu návod, podle kterého má ověřit, zda byly originality v tomto případě naplněny. Praktickým důsledkem tohoto rozhodnutí je ale zamezení hypertrofie autorskoprávní ochrany databází.[3]

Soud	Soud prvního stupně v Haagu
Sp. zn.	BV0549
Datum	11.1. 2012
Dostupnost	http://zoeken.rechtspraak.nl

Kolektivní správce BREIN zažaloval poskytovatele služeb elektronických komunikací Ziggo, b.v. a XS4ALL, b.v. Počtem svých uživatelů se Ziggo a XS4ALL řadí mezi největší poskytovatele těchto služeb v Nizozemí. BREIN ve své žalobě požadoval, aby výše zmínění poskytovatelé svým uživatelů zablokovali přístup na internetové stránky The Private Bay, jenž umožňoval nabízet torrenty obsahující díla chráněná autorským právem způsobem peer-to-peer (P2P).

Podle soudu porušuje 90% až 95% torrentů dostupných z The Pirate Bay autorské právo a práva související s právem autorským. Blokace IP adresy The Pirate Bay neomezuje podle soudu svobodu slova ani právo přijímat informace podle čl. 10 Evropské úmluvy o lidských právech a základních svobodách. Druhý odstavec toho

1 K těmto rozsudkům vizte i komenář Zuzany Adamové v č. 3 Revue pro právo a technologie. ADAMOVÁ, Zuzana. Rozpisy futbalových zápasov, konských dostihov a iných databáz a ich právna ochrana. *Revue pro právo a technologie*. 2011, roč. 2, č. 3. S.

2 S odkazem na svoji další relevantní judikaturu (Infopaq International, C-5/08, Bezpečnostní softwarová asociace, C-393/09; Football Association Premier League a další, C-403/08 a C-429/08; Painer, C-145/10)

3 Stejným názore uzavřela výše uvedený článek i Adamová.