Iuridicum Remedium, o.s.

Co dělají provideři a telefonní operátoři s našimi daty?

Studie praxe poskytovatelů internetových a telekomunikačních služeb (ISP)

Praha, 20. dubna 2010

Tato studie vznikla v rámci projektu "Reclaim Your Rights in the Digital Age", který je realizován díky finanční podpoře nadace Trust for Civil Society in Central and Eastern Europe.

Abstrakt

V naší studii se zaměřujeme na poskytovatele komunikačních služeb v oblasti internetových technologií. Soustředíme se na ochranu dat zpracovávaných v rámci těchto služeb ve vztahu k existující právní regulaci. Zvláštní důraz klademe na problematiku předávání dat o elektronické komunikaci bezpečnostním orgánům státu.
Oslovujeme vybraný vzorek firem, ptáme se těchto firem, jak postupují v oblasti zkoumané problematiky v praxi. Získané poznatky interpretujeme zpětně ve vztahu k zákonným normám, ze kterých jsme vycházeli.
Na základě výsledků formulujeme doporučení pro zlepšení ochrany údajů zákazníků ve zkoumané oblasti podnikání.

Obsah

1. Předpoklady a motivace výzkumu

S bouřlivým rozvojem internetových technologií, kdy se rychle rozvíjí způsoby mezilidské online komunikace, kdy lidé na síť promítají část svého života, kdy se komunikační technologie začleňují do mnoha různých činností v průběhu běžného dne, vyvíjejí se současně i nástroje společenské potřeby komunikaci sledovat a kontrolovat. Témata kontroly, svobody a bezpečnosti jsou velmi citlivým tématem, býváme svědky vyhraněných názoru a polemik. Současný vývoj musíme sledovat velmi bedlivě, protože právě teď vznikají společenské normy, které budou výrazně ovlivňovat nejen budoucí rámec uplatňování těchto norem dlouho dopředu, ale i případné významy při vyjednávání a společenské diskuzi o nových normách a změnách norem stávajících.

Ačkoli rozvoj nových technologií poskytování služeb neznamená nutně útlum a opouštění starých způsobů komunikace, snažili jsme se zaměřit hlavně na otázky spojené s technologií internetu. Problematice například tradiční telefonie jsme se primárně nevěnovali, ačkoli jsme se jí jistě nepřímo dotýkali, protože může být často třeba v osobě poskytovatele a použité infrastruktury propojena s internetovými technologiemi.

V našem výzkumu se budeme věnovat dílčímu aspektu elektronické komunikace – ochraně soukromí. Používáním komunikačních služeb často předáváme poskytovatelům těchto služeb mnoho informací, které jsou silně vztaženy k našemu soukromí. Právě obrázek současné praxe ochrany *osobně vztažitelných dat*[1] firmami působícími v českém prostředí a vytyčení otázek pro další výzkum v této problematice je jedním ze zamýšlených cílů této práce.

Dalším záměrem je naší studie je sledovat právní rámec spjatý s ochranou *osobních údajů*[2] na jedné straně a na druhé straně s monitoringem elektronické komunikace bezpečnostními orgány státu jako zdrojem informací o společensky nebezpečném jednání. Právní normy chceme konfrontovat s reálnou praxí u dotazovaných provozovatelů služeb elektronické komunikace.

Konečně třetím cílem studie je na základě námi učiněných závěrů navrhovat praktická doporučení pro praxi poskytovatelů služeb elektronických komunikací, a to hlavně z pohledu ochrany citlivých dat o osobě zákazníka. Chceme tak podpořit diskuzi o problematice ochrany osobně vztažitelných dat a zapojovat do této diskuze všechny dotčené strany.

Studie byla zpracována v rámci projektu "Reclaim Your Rights in the Digital Age", který je realizován díky finanční podpoře nadace Trust for Civil Society in Central and Eastern Europe. Zpracoval ji Petr Kučera za podpory pracovníků občanského sdružení Iuridicum Remedium, jmenovité díky hlavně Filipu Pospíšilovi a Janu Vobořilovi. Iuridicum Remedium[3] je nevládní nezisková organizace na ochranu lidských práv typu "watchdog". Zaměřuje se na pokusy o plošné omezování práv občanů legislativní cestou i na konkrétní případy porušování lidských práv. Problematice uchovávání provozních a lokalizačních dat v elektronické komunikaci (známý je pojem z angličtiny *data retention*) se věnuje dlouhodobě v rámci programu Lidská práva a technologie[4]. Vyvíjí proto legislativní aktivity, poskytuje právní pomoc a šíří informace mezi odbornou právnickou, novinářskou i nejširší veřejnost.

---

[1] Ve studii se snažíme pužívat pojem *osobní údaje* ve významu zákona 101/2001 Sb. Pojem *osobně vztažitelná data* používáme v obecném významu pro jakákoli data, která potenciálně mohou obsahovat informace vypovídající o soukromí dotčené osoby; pod tento pojem tedy budou spadat veškerá data, u kterých panuje pochybnost, jsou-li osobními údaji.

[2] Viz poznámka 1.

[3] Webové stránky sdružení: http://www.iure.org

[4] Webové stránky pro program Lidská práva a technologie: http://www.slidilove.cz

1.1. Návaznost na provedené výzkumy

Protože si nejsme vědomi žádného obsahově nebo rozsahově podobného provedeného výzkum v českém prostředí, zaměřili jsme se na výzkumy provedené v zahraničí. Vzhledem k nadnárodnímu charakteru některých komunikačních služeb na internetu jsme se i v zahraničních výzkumech mohli setkat se subjekty působícími na českém trhu.

Jedním z relevantních výzkumů pro naši studii bylo šetření časopisu Wired (Singel 2007a, 2007b), které se týkalo praxe poskytovatelů internetového připojení při správě a zabezpečení osobně vztažitelných dat a při případném komerčním využívání anonymizovaných dat o zákaznících. Některé otázky z tohoto výzkumu jsme adaptovali i do českého prostředí.

Druhým podkladem pro naši studii bylo šetření organizace Privacy International (2007), která uskutečnila obsáhlé šetření u vzorku významných poskytovatelů webových služeb. Výzkum se zaměřoval na všeobecný přístup k osobně vztažitelným datům zákazníků a ochranu takových dat, na úroveň komunikace se zákazníky, na nabízená doporučení zákazníkům pro dobrou ochranu údajů. Výsledkem výzkumu byla jakási forma bodování zkoumaných firem z pohledu jejich všeobecné praxe ve vymezené problematice. Metodologické poznámky v tomto výzkumu nám pomáhaly identifikovat možné zdroje nejasností při vymezení si našich okruhů zájmu i při sestavování dotazníku.

1.2. Teoretické zdroje výzkumu

Význam uchovávání osobních údajů jako nástroje pro uplatňování moci byl významným prvkem motivace pro uskutečnění této studie. V historii technických řešení sledování komunikace dominuje metoda odposlechů; předmět zájmu je na základě podezření sledován, informace zpětně o komunikaci před získáním povolení lze získat jen obtížně. S nástupem digitální elektronické komunikace se objevuje technologická možnost získat důvěrné údaje i zpětně. Je možné uchovávat záznamy o proběhlé komunikaci. Objevuje se koncept povinného uchovávání dat. Data jsou uchovávána o každém, bez nutnosti jakéhokoli podezření na nezákonné jednání. Tím je vlastně popírán princip presumpce nevinny. Tím, že uchovávaná data jsou možným zdrojem moci pro budoucí použití, stávají se nanejvýš citlivým materiálem. Proto se zde zaměříme na praxi zabezpečení uchovávaných osobních údajů i dalších potenciálně citlivých dat. V současnosti probíhá debata o ústavnosti preventivního uchovávání dat v mnoha evropských státech[5]. My se však v této studii na problematiku ústavnosti zákona zaměřovat nebudeme.

Jinou otázkou je vůbec proveditelnost efektivního sledování komunikace i další otázky z technologicko-právní problematiky. Můžeme v tomto směru poukazovat na kontrast rozdílných přístupů v národních měřítcích ve vztahu k nadnárodnímu charakteru internetu, nebo na diverzitu různých komunikačních technik na internetu a jejich různé úrovně zabezpečení. Důležitým hlediskem je též otázka odpovědnosti za uveřejněný obsah, je-li uchováván na serverech třetích stran (viz např. Polčák 2009). V této studii se však nechceme pouštět do polemiky o proveditelnosti internetové kontroly ve společnosti mnoha rozdílných i protichůdných zájmů. Budeme však sledovat, zda se toto téma projevuje v praxi jednotlivých poskytovatelů elektronických komunikačních služeb na internetu.

S předchozím bodem souvisí otázka vymahatelnosti národních zákonů u nadnárodních firem sídlících v zahraničí. Při mezinárodních transakcích po internetu bývá obtížné určit, na jaké národní

[5] V Rumunsku byla směrnice o uchovávání dat označena ústavním soudem za neústavní (EDRi 2009a), v Německu je soudně zpochybněn význam směrnice (EDRi 2009b), V Rakousku nebyla směrnice zatím uvedena do praxe (EDRi 2009c), v Česku je iniciován ústavněprávní přezkum platnosti Zákona o elektronických komunikacích (Iuridicum Remedium 2009).

právní normy se odvolávat (viz např. Čermák 2001, Loebl 2003, Smejkal 2004, Mališ 2008). V našem výzkumu se blíže podíváme, co to znamená pro zákazníky služeb z pohledu bezpečnosti jejich osobně vztažitelných dat.

Dalším zdrojem nejasností pro východiska i závěry výzkumu je nejasnost vymezení pojmu „osobní údaj[6]“ ve vztahu k současným technologiím na internetu. Problém vzniká u údajů, které nejsou navázané na „tvrdé“ osobní údaje (např. jméno, příjmení, adresa, rodné číslo, datum narození apod.), nicméně identitu přesto s velkou přesností určí. Příkladem mohou být údaje do určité míry přenositelné mezi osobami (IP adresa), dále údaje, u kterých není ověřována jejich návaznost na „tvrdé“ osobní údaje, avšak v praxi je návaznost často zřejmá třeba běžným použitím řetězce jméno+příjmení (např. uživatelské jméno, emailová adresa), údaje spojené s historií komunikace konkrétní osoby (opět např. uživatelské jméno, emailová adresa). Na internetu jsou k dispozici nástroje, které dokáží z útržků uveřejněných informací o konkrétní osobě na základě například emailové adresy složit poměrně konsolidovaný obrázek konkrétní osoby[7]. Například v případě IP adresy se vede spor mezi pojetím USA a EU ohledně zařaditelnosti do kolonky osobní údaj[8]. I v případě této nejasnosti bude velmi zajímavé sledovat důsledky v praxi námi zkoumaných poskytovatelů služeb.

2. Metodika nastavení výzkumu

Při snaze ohraničit si naše téma a najít konkrétní východiska pro výzkum jsme si museli odpovědět na otázky vymezení dotazovaných subjektů a hloubky důrazu na jednotlivá témata.

2.1. Poskytovatelé jakých služeb budou předmětem výzkumu?

Výchozím materiálem pro náš výzkum byl zákon o elektronických komunikacích (zákon č. 127/2005 Sb.), kde jsou definovány subjekty, kterých se zákonné úpravy týkají. Při čtení zákona nás upoutala poměrně vágní a obecné vymezení dotyčných subjektů, hlavně z pohledu nových technologií na internetu. Zde je důležité zdůraznit, že jsme vycházeli z našeho čtení zákona a naší interpretace tohoto zákona. Teprve později jsme se konfrontovali s reálnou praxí interpretace tohoto zákona. Jako předmět zákonné úpravy jsou stanoveny osoby „zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací“. Oba pojmy jsou pak ještě dále upřesňovány, ale dle našeho názoru je jasný výklad na základě těchto definic stále obtížný. Zákon dále stanovuje povinnosti při provádění služeb elektronické komunikace, sběru a správě osobních údajů zákazníků (i s odkazem na zákon o ochraně osobních údajů 101/2001 Sb.[9]), sběru a správě provozních a lokalizačních údajů dle § 97[10], povinnosti ve vztahu k monitoringu bezpečnostních služeb (v tomto bodě je doplněn odkazem na prováděcí vyhlášku[11]).

---

[6] Debatě k pojmu „osobní údaj“ se dlouhodobě věnuje Úřad pro ochranu osobních údajů – například v sekci *Názory úřadu – K problémům z praxe* na http://uoou.cz/uoou.aspx?menu=14&loc=365

[7] Například služba *Pipl – People Search* na http://pipl.com/

[8] Zatímco soudy ve Spojených státech rozhodly, že IP adresa není osobním údajem (Davis 2009), pracovní skupina Evropské komise se vyjádřila že *„... pokud poskytovatel internetových služeb není schopen s naprostou jistotou odlišit, že údaje odpovídají uživatelům, kteří nemohou být identifikováni, bude muset pro jistotu nakládat se všemi informacemi o IP adresách jako s osobními údaji“* (Pracovní skupina pro ochranu údajů zřízená podle článku 29 – WP 148 – 2008).

[9] Zákon o ochraně osobních údajů je dále upravován dalšími předpisy. Více například na webových stránkách Úřadu pro ochranu osobních údajů: http://uoou.cz/uoou.aspx?menu=4&submenu=5

[10] V textu se na § 97 zákona 127/2005 Sb. budeme odkazovat pro zjednodušení pouze jako na „§ 97“

[11] Momentálně je platná vyhláška č. 485/2005 Sb. (o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání) a vyhláška č. 486/2005 Sb. (kterou se stanoví výše a způsob úhrady efektivně vynaložených nákladů na zřízení a zabezpečení rozhraní pro připojení

Protože bylo jedním ze stanovených cílů výzkumu nahlédnout praxi u provozovatelů elektronických komunikačních služeb, zvolili jsme jako předmět výzkumu jak firmy[12] poskytující služby v oblasti zajištění připojení k internetu, tak firmy poskytující služby již přímo na internetu a to především prostřednictvím webového rozhraní (poskytovatelé v oblasti webových služeb).

V průběhu výzkumu se opakovaně vyjevilo, že poskytovatelé webových služeb v praxi z pohledu orgánů státu nespadají pod stejný režim a rutiny jako poskytovatelé připojení k internetu. Poskytovatelům webových služeb se v současnosti stále daří existovat v jakémsi pojmovém i právním vakuu, definice jsou zde rozostřené, vše dále komplikuje fakt, že webové služby nejsou vázané na geografickou lokalitu a příslušnou lokální jurisdikci tak silně, protože se realizují v kyberprostoru (viz např. Čermák 2001). Rozdělení na dvě oblasti poskytovaných služeb – poskytovatelé **připojení k internetu** a poskytovatelé **webových služeb** – nás provází v celém výzkumu.

Nejvýrazněji se absence zakotvení pojmů kolem webových služeb projevuje v případě oznamovací povinnosti „komunikační činnosti" u Českého telekomunikačního úřadu (ČTÚ)[13]. Námi oslovení poskytovatelé webových služeb (viz Tabulka 3 v kapitole 4.1.3) nemají registraci u ČTÚ ani jediný[14].

2.2. Na jaká témata vybraná v rámci stanovených cílů se zaměříme?

Abychom zúžili náš záběr v problematice správy a ochrany osobně vztažitelných dat, soustředili jsme se na základní otázky praxe sběru, uchovávání a zabezpečení osobně vztažitelných dat, dále téma komunikace se zákazníky (například prostřednictvím dokumentu „Politiky správy osobních údajů"). Na druhé straně jsme se zaměřili na praxi při kontaktech firem s orgány veřejné moci.

Co se týče samotných osobně vztažitelných dat, o které jsme se v rámci studie zajímali, snažili jsme se o celkový pohled. Důraz však byl kladen na provozní a lokalizační údaje, neboť jejich uchovávání je stanoveno jako zdroj informací pro bezpečnostní složky dle § 97. Samotný obsah komunikace při přenosu zpráv není nyní předmětem uchovávání ze strany provozovatelů služeb pro účely bezpečnostních orgánů státu; takové údaje mohou bezpečnostní orgány získávat sami metodou odposlechů, tedy ne zpětně.

3. Metodika provedení výzkumu

Při výběru společností, kterých se budeme dotazovat, jsme jednoznačně chtěli obsáhnout nevýznamnější subjekty na českém trhu. Řídili jsme se hlavně údaji o velikosti firmy či velikosti poskytované služby na českém trhu. Vybírali jsme podle odhadovaných počtů uživatelů služeb i

---

koncového telekomunikačního zařízení pro odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby).

[12] Pojem *firma* používáme v tomto textu jako synonymum pojmu *společnost*. Oba pojmy jsou používány zároveň.
[13] Podmínky registrace u Českého telekomunikačního úřadu jsou popsány na http://www.ctu.cz/ctu-informuje/jak-postupovat/podnikani-v-e-komunikacich/oznamovani-podnikani.html
[14] Databáze podnikatelů v elektronických komunikacích je veřejně dostupná na webových stránkách ČTÚ: http://www.ctu.cz/ctu-online/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.html

podle relevance v internetových vyhledávačích[15]. Jsme si vědomi, že seznam kontaktovaných firem nemusí být kompletní, v budoucnu bychom ho rádi dále zpřesňovali.

Při výběru konkrétních kategorií služeb, na které se ve výzkumu zaměříme, byl výběr poměrně přímočarý u služeb připojení k internetu. Naopak webové služby zahrnují pestrou paletu různorodých služeb, ze kterých bylo nutné provést zužující výběr. Snažili jsme se vybrat kategorie webových služeb, které zákazníci využívají nejčastěji. Zároveň jsme se však záměrně vyhnuli kategorii internetových obchodů a internetových bankovních služeb, a to hlavně z obavy neochoty subjektů v tomto oboru odpovídat ve výzkumu.

Vybrali jsme 6 kategorií služeb:

- Oblast 1 - Poskytovatelé služeb **připojení** k internetu
  - poskytovatelé připojení k internetu (bez poskytovatelů mobilního připojení)
  - poskytovatelé mobilního připojení k internetu
- Oblast 2 - Poskytovatelé **webových** služeb
  - poskytovatelé služby webového emailu
  - poskytovatelé služeb internetového vyhledávání
  - poskytovatelé služeb sociální sítě (fórum apod.)
  - poskytovatelé služeb zobrazování reklam

V každé ze šesti identifikovaných kategorií jsme identifikovali 4 – 7 nabízených služeb, na jejichž poskytovatele se obrátíme s dotazy. K tomu jsme se navíc pro srovnání rozhodli obrátit ještě na 2 menší poskytovatele služeb "nemobilního" připojení k internetu. Vzhledem k tomu, že nemapujeme malé poskytovatele připojení k internetu systematicky, rozhodli jsme se jména dvou referenčních malých firem nezveřejnit. Celkem jsme takto identifikovali 32 jednotlivých služeb, jejichž poskytovatelé budou předmětem výzkumu. Zajímavé pak bylo zjištění, že přiřadíme-li k námi vybraným službám jejich provozovatele, dospějeme k počtu 20 firem. Nejvýraznější společnosti na trhu tedy často provozují širší portfolio služeb. Zároveň portfolio služeb však jen zřídka zasahuje do obou námi vymezených oblastí poskytovaných služeb.

Tabulka 1: Služby vybrané pro výzkum, se zařazením k provozující firmě, seskupeno dle kategorií služeb

Kategorie služby v zájmu studie	**Název služby (zkráceně)**	**Název firmy**
připojení k internetu	GTS	GTS Novera
	UPC	UPC Česká republika, a.s.
	Volný	VOLNÝ, a.s.
	O2	Telefónica O2 Czech Republic, a.s.
	České Radiokomunikace	České Radiokomunikace a.s.
mobilní připojení k internetu	Vodafone	Vodafone Czech Republic a.s.
	T Mobile	T-Mobile Czech Republic a.s.
	O2	Telefónica O2 Czech Republic, a.s.
	U:fon	MobilKom, a.s.

[15] Údaje o počtech českých uživatelů služeb, na které se v našem výzkumu zaměřujeme, lze získat jen fragmentované a s nejasnou mírou přesnosti (viz např. Dočekal 2009). Pro účely našeho výzkumu jsme považovali za dostatečné vycházet z pořadí, v jakém se firmy řadí ve výsledcích vyhledávače Google.

reklama na internetu	Sklik	Seznam.cz, a.s.
	Etarget	ETARGET CZ, s.r.o.
	Google Adwords	Google Czech Republic, s.r.o.
	Adfox	Centrum Holdings s.r.o.
sociální síť	Seznamka.cz	TANGER, spol. s r.o.
	Rande.cz	TANGER, spol. s r.o.
	LibimSeTi	Libimseti.cz a.s.
	Facebook	Facebook, Inc.
	Aukro	Aukro s.r.o.
	Lide.cz	Seznam.cz, a.s.
	Spoluzaci.cz	Seznam.cz, a.s.
	Nyx.cz	(fyzická osoba)
internetový vyhledávač	Seznam.cz	Seznam.cz, a.s.
	Atlas.cz	Centrum Holdings s.r.o.
	Google.cz	Google Czech Republic, s.r.o.
	Centrum.cz	Centrum Holdings s.r.o.
	Jyxo.cz	Jyxo, s.r.o.
webový email	Seznam.cz	Seznam.cz, a.s.
	Email.cz	Seznam.cz, a.s.
	Gmail	Google Czech Republic, s.r.o.
	Centrum.cz	Centrum Holdings s.r.o.

Protože jsme se v našem výzkumu zaměřili i na otázky praxe při komunikaci a spolupráci s bezpečnostními složkami, tedy dle našeho odhadu potenciálně citlivě vnímané otázky, rozhodli jsme se rozdělit dotazování firem do dvou fází. Tím jsme chtěli zajistit nižší míru odmítnutí spolupráce hned v počátku výzkumu.

V první fázi byly firmy požádány o vyplnění dotazníku (vzor dotazníku viz Příloha 1), který byl zaměřený na praxi uchovávání a zabezpečení dat a na úroveň informační otevřenosti v komunikaci směrem ke klientům firem. V druhé fázi jsme ty společnosti, které byly ochotny spolupracovat v první fázi výzkumu, požádali o osobní rozhovor, alternativně o písemné zodpovězení otázek. Písemně kladenými otázkami jsme se snažili obsáhnout shodnou problematiku jako při osobním rozhovoru (otázky viz Příloha 2). Jednalo se o otázky k praxi v komunikaci firmy s bezpečnostními složkami, hlavně co se týče předávání provozních a lokalizačních údajů.

Vybraných 20 firem jsme se snažili kontaktovat nejčastěji přes jejich vlastní kanál pro komunikaci s médii (press centrum, public relation). Pokud ve firmě takový komunikační kanál neexistoval, obraceli jsme se na kontakty vedoucích pracovníků, které jsme nalezli na webových stránkách firem. Firmy jsme oslovili emailovou zprávou s podrobným vysvětlením naší žádosti o spolupráci k výzkumu (vzor zprávy viz Příloha 3), dodatečně jsme kontakt urgovali telefonicky s odkazem na předchozí email. V individuálních případech byly použity další opakované emailové urgence.

U dat, která jsme získali z dotazníků, je potřeba brát v úvahu, že se zakládají na tom, co daná firma deklaruje. Ne vždy se to nutně musí shodovat se skutečnou praxí. Avšak neklademe si za cíl vyjádření společností vyvracet nebo potvrzovat na základě informací z třetích zdrojů. Proto je při čtení výsledků výzkumu brát toto metodické omezení v potaz.

4. Výsledky výzkumu

4.1. Poznatky získané ve fázi kontaktování firem (před vyplněním dotazníku)

Poměrně příjemným zjištěním pro nás bylo, že firmy přes své kanály pro komunikaci s médii byly většinou ochotny se bavit i o našem výzkumu, i když jsme se na firmy obraceli jako nezisková organizace a ne jako zástupce tisku. Užití kombinace emailové a telefonické komunikace pro navázání kontaktu s firmou se ukázalo být dobrou volbou. Při telefonické urgenci naší žádosti o spolupráci se často ukazovalo, že naše emailová zpráva nezapadla, avšak zástupci firem otáleli s odpovědí. Telefonickou urgencí se pak podařilo podpořit autentičnost a důležitost naší emailové zprávy. Ve výsledku od všech firem, které uváděly na svých webových stránkách kontakt na konkrétní osobu pro komunikaci s médii, se podařilo k našemu výzkumu získat vyjádření.

Tabulka 2: Spolupráce oslovených firem v rámci výzkumu, s údajem o existenci oddělení pro styk s médii

Název firmy	Mají oddělení pro styk s médii	Podařilo se získat vyjádření k výzkumu	Spolupráce na dotazníku	Spolupráce ve druhé fázi výzkumu
GTS Novera	**ano**	**ano**	ne	ne
UPC Česká republika, a.s.	**ano**	**ano**	ne	ne
VOLNÝ, a.s.	**ano**	**ano**	**ano**	**ano**
Telefónica O2 Czech Republic, a.s.	**ano**	**ano**	**ano**	ne
České Radiokomunikace a.s.	**ano**	**ano**	ne	ne
Vodafone Czech Republic a.s.	**ano**	**ano**	**ano**	ne
T-Mobile Czech Republic a.s.	**ano**	**ano**	**ano**	**ano**
MobilKom, a.s.	**ano**	**ano**	**ano**	**ano**
ETARGET CZ, s.r.o.	**ano**	**ano**	**ano**	ne
TANGER, spol. s r.o.	ne	ne	ne	ne
Libimseti.cz a.s.	ne	ne	ne	ne
Facebook, Inc.	**ano**	ne	ne	ne
Aukro s.r.o.	**ano**	**ano**	ne	ne
Seznam.cz, a.s.	**ano**	**ano**	ne	ne
Google Czech Republic, s.r.o.	**ano**	ne	ne	ne
Centrum Holdings s.r.o.	**ano**	**ano**	**ano**	ne
Jyxo, s.r.o.	ne	**ano**	ne	ne
Nyx.cz (název služby, není firmou)	ne	**ano**	**ano**	**ano**
Malý poskytovatel internetu č. 1	ne	**ano**	**ano**	**ano**
Malý poskytovatel internetu č. 2	ne	ne	ne	ne

4.1.1. Firmy, od kterých se nepodařilo získat vyjádření

Ze 20 oslovených společností se nám nepodařilo získat žádné vyjádření od 5 subjektů. Zajímavým poznatkem přitom je, že mezi těmito 5 firmami se nacházejí převážně provozovatelé sociálních sítí (Facebook, LíbímSeTi.cz, Tanger – provozovatel Seznamka.cz a Rande.cz) a nadnárodní firmy (Facebook, Google). Pátým subjektem, od kterého jsme nezískali reakci, byl i jeden z malých poskytovatelů internetového připojení.

Právě provozovatelé sociálních sítí často neuváděli na svých webových stránkách kontakt pro komunikaci s médii. Pokud se nám tedy podařilo provozovatele sociální sítě kontaktovat, bylo to buď přes mateřskou firmu, která má širší záběr podnikatelských aktivit, a tedy i kontakt pro komunikaci s médii (Seznam.cz), nebo díky nadstandardní znalosti kontaktu uvnitř sociální sítě (Nyx.cz). Ani u aukční služby Aukro, která však není typickou sociální sítí díky svému zaměření na obchodování, nebyl v době výzkumu kontakt na člověka zodpovědného za komunikaci s médii uveden (respektive odkaz nebyl funkční). Již nyní je tedy možné konstatovat, že získat vyjádření od

provozovatelů sociálních sítí se nám jeví jako obtížné, pro provozovatele je často charakteristická uzavřenost vůči veřejnosti a médiím. Zajímavým tématem pro další výzkum by mohlo být zjistit, zda jsou provozovatelé sociálních sítí v komunikaci s uživateli uvnitř sítě otevřenější, než navenek.

V případě nadnárodních firem se sídlem v zahraničí mohou být důvody nezískání reakce do našeho výzkumu odlišné. V našem výzkumu se toto týká dvou firem: Google a Facebook. Obě služby mají v českém prostředí významnou uživatelskou základnu, v případě některých služeb mohou překonávat i konkurenční české firmy. Zároveň však uživatelé z Česka představují jen zlomek celkového celosvětového počtu uživatelů. Nadnárodní firmy tak podnikají vlastně v o mnoho vyšším měřítku, počty uživatelů jsou řádově stonásobné[16]. V případě obou zmíněných firem jsme zaznamenali, přítomnost účinných obranných metod proti kontaktování zodpovědné osoby. Na svých webových stránkách se snaží možného tazatele odkázat na existující zdroje informací, návody, licenční ujednání, často kladené otázky apod. Kdo nenajde v nabídce dokumentů odpověď na své dotazy, dostane se až ke kontaktní emailové adrese nebo formuláři. Pro komunikaci s médii mají firmy podobnou strategii. Telefonické spojení v obou případech pro mediální kontakt uvedené nebylo. V případě Googlu jsme získali emailový kontakt na kancelář pobočky v Praze, v případě Facebooku jsme psali anglicky na globální emailový kontakt. V obou případech se nejednalo o emailový kontakt na konkrétní osobu, což dále zvyšuje pocit odcizení při komunikaci s velkou firmou. V případě provozovatele Facebooku jsme obdrželi dokonce automatickou odpověď, která obsahovala sdělení o vytíženosti komunikačního kanálu a o tom, že firma negarantuje odpověď (viz Příloha 4). Odpověď jsme přes opakované dotazy do dnešního dne po více než dvou měsících od žádné z obou firem neobdrželi.

Je důležité zdůraznit, že naše zkušenost s komunikací se zmíněnými nadnárodními firmami nemusí odpovídat zkušenosti běžného uživatele například v případě technických problémů s poskytovanou službou. Domníváme se, že pro zmíněné firmy je charakteristická sofistikovaná práce s informačními a komunikačními kanály, které mohou mít z pohledu firmy různou prioritu pro odpovědi na otázky. Prozkoumání aktuálního stavu a monitoring komunikačních kanálů v největších nadnárodních firmách poskytujících webové komunikační služby je zajímavým tématem pro další výzkum. Tématu se věnuje i výše citovaný výzkum organizace Privacy International (2007).

V případě firmy provozující sociální síť Facebook, která vlastně spadá do obou problematických kategorií (sociální síť a nadnárodní firma) narážíme ještě na další problém, který se týká českých specifik, o která jsme se ve výzkumu zajímali. Firma nemá pobočku v České republice, kontakt na mediálního zástupce společnosti v Česku jsme získali až po skončení výzkumu[17]. V našem výzkumu tak vyvstává otázka, jaký postoj k dodržování českých standardů ochrany osobních údajů vlastně mají firmy, které v České republice nemají pobočku. Domníváme se, že v současné situaci je vymáhání dodržování českých standardů v případě nadnárodních firem bez české pobočky prakticky velmi těžko uskutečnitelné.

4.1.2. Firmy, které poskytly vyjádření k neúčasti ve výzkumu

Z celkového počtu 15 odpovědí od oslovených firem bylo 6 odpovědí ve vztahu k účasti ve výzkumu zamítavých. Vyjádření k důvodu neúčasti ve výzkumu je pro nás však také zajímavým poznatkem:

[16] Například sociální síť Facebook má v Česku něco mezi 1,5 – 2 mil. uživatelů, globálně to je přes 350 mil. uživatelů (Dočekal 2009).

[17] Firma Visibility (http://visibility.cz/), která se však podle informací uvedených na svých webových stránkách soustředí hlavně na oblast poskytování reklamy. Navíc podle posledních informací, které máme k dispozici, tuto roli mediální agentury dnes přebírá firma ARBOinteractive, spol. s r. o. (http://arbointeractive.cz/).

- Firma UPC: Při telefonickém rozhovoru se zástupcem firmy se nám dostalo vyjádření, že vzhledem ke vnitřním směrnicím vlastníka firmy, nadnárodního koncernu Liberty Global Inc., nejsou oprávněni poskytovat údaje o české divizi. Prý je možné získat z ústředí informace o koncernu jako celku, ne však o jeho národních divizích.

- Firma GTS Novera: Při telefonickém rozhovoru se zástupcem firmy se nám dostalo vyjádření, že firma poskytuje služby výlučně firemním klientům a výzkumu se nehodlá zúčastnit.

- Firma Seznam.cz: Vyjádření z emailové zprávy od zástupce firmy: *S ohledem na to, že naše společnost nespadá pod zákon o elektronických komunikacích a osobní údaje zpracovává jen v minimální míře v rámci svých registrací u ÚOOÚ, jsme se rozhodli Vašeho průzkumu nezúčastnit.*

- Další firmy, které se odmítly výzkumu zúčastnit, uvedly jako důvod nedostatek času pro účast ve výzkumu (České Radiokomunikace, Jyxo.cz) nebo vysokou citlivost problematiky (Aukro).

Případ společnosti UPC ukazuje na další rys komunikace s globálními firmami. Monolitická struktura firmy ve vztahu k veřejnosti a médiím umožňuje prakticky zajistit obranu proti nepříjemným dotazům. Získat informace o místní pobočce firmy přes nadnárodní centrum firmy může být i například kvůli jazykovým barierám náročné a možná díky vnitřní politice firmy i nemožné. Jak už bylo zmíněno výše, prozkoumat komunikační kanály nadnárodních firem ve vztahu k národně specifickým zákonným úpravám bude důležitým tématem pro další výzkum. A to i proto, že nadnárodní vlastnictví je v českém prostředí dnes všudypřítomné.

Vyjádření společnosti Seznam.cz nám ukazuje, že situace v oblasti uchovávání provozních a lokalizačních údajů a v oblasti zpracování osobních údajů je velmi nejednoznačná. Vidíme, že firma využívá nejednoznačnosti zákonů o elektronické komunikaci a o ochraně osobních údajů ku svému prospěchu. Domníváme se, že firma Seznam.cz je si vědoma přínosu své interpretace pro snížení nákladů při svém podnikání. Zároveň pravděpodobně svou právní interpretaci zákona má dobře zdůvodněnou a chrání se proti případnému nařčení z porušování zákona. Pro firmy podnikající v oblasti webových služeb to může být inspirací. Pro uživatele služeb firmy Seznam.cz i pro náš výzkum znamená tento poznatek dva důležité momenty:

- Vzhledem k tomu, že firma provozuje například webmail a sociální sítě, nelze se domnívat, že by nepracovala s informacemi osobního charakteru. Svým vyjádřením dává najevo, že je možné, že informace, které uživatelé těchto služeb o sobě uvádějí, nejsou považovány za osobní údaje a tedy nespadají pod přísnější standardy ochrany osobních údajů. Uživatelé služeb firmy by se tedy měli zajímat o standardy ochrany všech svých dat, které firma zpracovává.

- Z pohledu zákona o elektronických komunikacích dává firma najevo, že nehodlá o uživatelích sbírat a uchovávat provozní a lokalizační údaje pro účely použití orgány veřejné moci. Z našeho výzkumu však nevyplývá, jak se firma staví v praxi k případným požadavkům ze strany bezpečnostních složek, zda opravdu na vyžádání žádné údaje neposkytuje.

V podobném duchu jako firma Seznam.cz se vyjádřil i provozovatel diskuzního serveru Nyx.cz, který byl však ochoten se přesto výzkumu zúčastnit. Deklaroval, že žádné osobní údaje od uživatelů nevyžaduje a je jen na nich, pokud o sobě nějaké údaje uvedou (např. do kolonky kontakty ve svém osobním profilu).

4.1.3. Registrace firem u Úřadu pro ochranu osobních údajů

V případě všech oslovených firem jsme zjišťovali, zda jsou registrované u Úřadu pro ochranu osobních údajů (ÚOOÚ) pro zpracování osobně vztažitelných dat svých klientů. Dle zákona o ochraně osobních údajů je povinné se u ÚOOÚ registrovat pro každou jednotlivou činnost zpracování osobních údajů[18]. Dále je nutné podotknout, že pro sběr a uchovávání provozních a lokalizačních údajů (a dalších údajů, sbíraných na základě nějaké zákonné povinnosti) dle zákona o ochraně osobních údajů není potřeba registrace u ÚOOÚ.

Formulář pro registraci u ÚOOÚ vyžaduje specifikaci rozsahu zpracovávaných údajů, účel zpracování údajů, stanovení zpracovatele údajů apod[19]. Avšak v praxi se často setkáme s příliš obecnými informacemi, domníváme se, že některé firmy se snaží vyplnit formulář co nejobecněji, aby jim v praxi poskytovala obecná definice pokud možno co největší volnost. Proto jsme byli nuceni pracovat s obecným vyjádřením "zpracování dat klientů", ze kterého není jasné, jaká data v portfoliu služeb firmy jsou konkrétně zpracovávána, ani přesně jaká data jsou firmou považována za osobní údaje. Proto jsme pro potřeby tohoto výzkumu hledali, zda má firma jakoukoli registraci, pro zpracování osobních údajů svých klientů. I tak jsme dospěli k zajímavým poznatkům.

[18] Databáze subjektů registrovaných u ÚOOÚ je volně přístupná na webových stránkách Úřadu: http://uoou.cz/uoou.aspx?menu=29&submenu=30&loc=503

[19] Formulář pro oznámení o zpracování osobních údajů je k dispozici na webových stránkách ÚOOÚ: http://uoou.cz/uoou.aspx?menu=29&submenu=31

Tabulka 3: Firmy oslovené v rámci výzkumu a údaje o registraci v databázích ÚOOÚ, ČTÚ a ARES

	Registrace v databázi		
Název firmy	**ÚOOÚ**	**ČTÚ**	**ARES**[20]
GTS Novera	**ano**	**ano**	**ano**
UPC Česká republika, a.s.	**ano**	**ano**	**ano**
VOLNÝ, a.s.	**ano**	**ano**	**ano**
Telefónica O2 Czech Republic, a.s.	**ano**	**ano**	**ano**
České Radiokomunikace a.s.	**ano**	**ano**	**ano**
Vodafone Czech Republic a.s.	**ano**	**ano**	**ano**
T-Mobile Czech Republic a.s.	**ano**	**ano**	**ano**
MobilKom, a.s.	**ano**	**ano**	**ano**
ETARGET CZ, s.r.o.	ne	ne	**ano**
TANGER, spol. s r.o.	**ano**	ne	**ano**
Libimseti.cz a.s.	**ano**	ne	**ano**
Facebook, Inc.	ne	ne	ne
Aukro s.r.o.	**ano**	ne	**ano**
Seznam.cz, a.s.	**ano**	ne	**ano**
Google Czech Republic, s.r.o.	ne	ne	**ano**
Centrum Holdings s.r.o.	**ano**	ne	**ano**
Jyxo, s.r.o.	ne	ne	**ano**
Nyx.cz (název služby, není firmou)	ne	ne	**ano**
Malý poskytovatel internetu č. 1	ne	**ano**	**ano**
Malý poskytovatel internetu č. 2	ne	ne	**ano**

V oblasti služeb zajištění připojení k internetu jsou u ÚOOÚ registrovány všechny velké firmy z našeho výzkumu. Oslovení dva malí poskytovatelé internetového připojení registraci u ÚOOÚ nemají. To může být z jejich strany pochybení způsobené neznalostí nebo nejednoznačností výkladu zákona.

Zajímavá situace však panuje v oblasti poskytovatelů webových služeb. V případě společnosti Etarget, která je poskytovatelem reklamního systému na webových stránkách, se nejspíše dotýkáme sporné definice osobního údaje v případě údaje IP adresy. Přitom se domníváme, že právě údaje o IP adrese a dalších identifikátorech počítače, kterému se zobrazilo reklamní sdělení, jsou pokladem pro kvantifikaci úspěšnosti jednotlivých webových reklam i pro další zpřesňování reklamního zacílení.

Problém sporné definice a sporného výkladu pojmu osobní údaj je zřetelný z výčtu dalších firem, které nejsou registrovány u ÚOOÚ: Facebook, Google, Jyxo.cz, Nyx.cz. Ti všichni pravděpodobně interpretují údaje, které získávají od uživatelů jako údaje, které nespadají do kategorie osobních údajů. A to včetně IP adresy, emailových adres či uživatelského jména.

Charakteristickým rysem služeb, jejichž poskytovatelé nejsou registrováni u ÚOOÚ, je to, že se z pohledu uživatelů často jedná o služby "zdarma". Služba nabízená zdarma bývá totiž často kompenzována příjmy z poskytování reklam. Odvrácenou stranou služeb poskytovaných "zdarma" je využívání poskytnutých údajů o uživateli k lepšímu zacílení reklamy. Uživatelé by si tedy měli uvědomovat, že žádná služba není úplně zdarma a že často za službu zdarma mohou platit nižší mírou ochrany osobně vztažitelných dat a vyšší mírou využívání těchto dat ke komerčním účelům.

[20] Administrativní registr ekonomických subjektů (ARES) – Databáze registrovaných subjektů je volně přístupná pro vyhledávání na webové adrese http://wwwinfo.mfcr.cz/ares/ares.html

Naopak u poskytovatelů služeb připojení k internetu, což jsou vesměs služby placené, je registrace u ÚOOÚ běžná.

4.2. Poznatky získané na základě odpovědí firem

Vyplněný dotazník z první fáze výzkumu jsme dostali od 7 subjektů, další 2 subjekty se vyjádřily k tématům z dotazníku v dokumentu vlastní formy – tedy nerespektovaly formu dotazníku, nicméně poskytly více či méně hodnotné informace v relacích obsahu dotazníku. Dohromady se tedy vyslovilo 9 společností z 20 oslovených ve výzkumu.

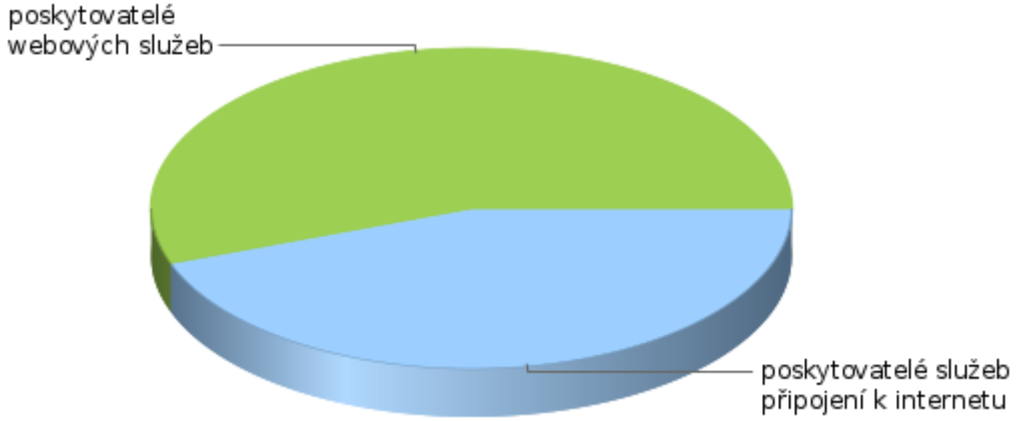
Ve druhé fázi výzkumu se podařilo uskutečnit 1 řízený rozhovor, od 4 firem jsme získali odpovědi k tématům rozhovoru písemně.

4.2.1. První fáze dotazování: Dotazník

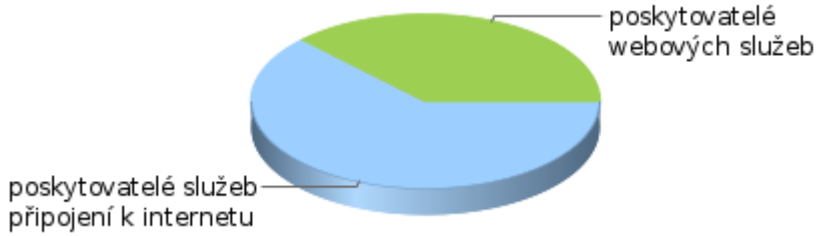
V následující pasáži budeme procházet jednotlivé poznatky z této části výzkumu. Pokusíme se získané údaje interpretovat a případně doplnit doporučením pro lepší praxi uchovávání dat o zákaznících služeb.

Strukturu zaměření služeb společností, které byly ochotny odpovídat na otázky z první části našeho výzkumu ilustruje Obrázek 2.

Obrázek 1: Rozložení oslovených firem dle oblastí podnikání



Obrázek 2: Rozložení firem, které odpověděly v první části výzkumu, dle oblastí podnikání



- Většina firem (7 firem) má vlastní metodiku pro sběr, uchovávání a zabezpečení dat o uživatelích svých služeb, avšak většina firem (6 firem) nedostala k vytvoření metodiky pokyny od státních úřadů.

Vidíme, že firmy většinou mají stanovenu metodiku pro zabezpečení určitých standardů práce s údaji o svých uživatelích. Pro subjekty poskytující veřejně dostupnou službu elektronických komunikací je taková metodika povinná[21]. Pro vytvoření metodiky firmy vesměs nedostaly pokyny od státních orgánů. Jedinou společností, která uvedla, že pokyny od státních orgánů obdržela, byla Telefónica O2.

Doporučení: Firmy by měly zpracovávat metodiku pro sběr, uchovávání a zabezpečení dat o uživatelích svých služeb bez ohledu na to, zda spadají pod definici zákona o elektronických komunikacích. Dají tím svým zákazníkům jasný signál, že jejich data zpracovávají zodpovědně.

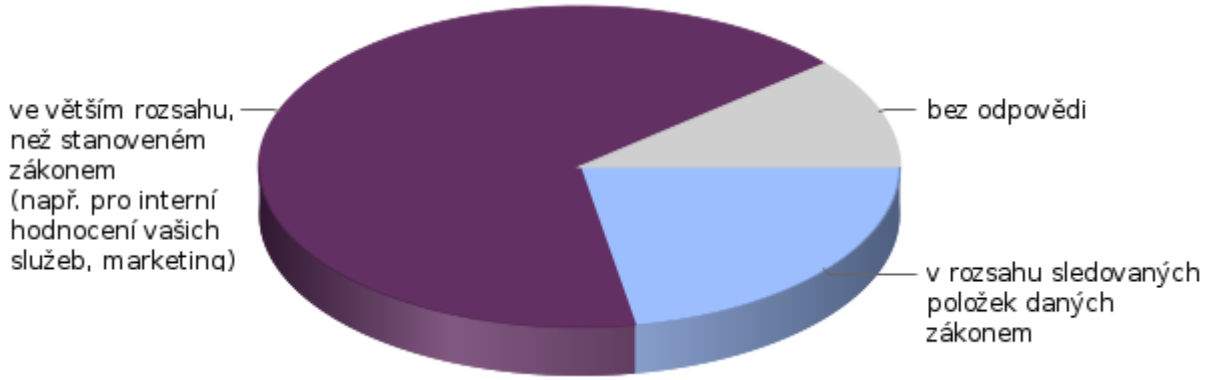
- Většina firem (6 firem) sbírá data o uživatelích ve větším rozsahu, než je stanovený rozsah provozních a lokalizačních dat dle § 97. Dobu uchování dat o uživatelích udává téměř polovina firem delší než 2 roky (4 firmy).

V otázce rozsahu sbíraných dat většina firem uváděla „ve větším rozsahu, než stanoveném zákonem (např. pro interní hodnocení vašich služeb, marketing)“. Z toho nutně plyne, že sběr a vyhodnocování dat o uživatelích přináší firmám významný užitek. To doplňují i odpovědi o době uchovávání dat, která bývá i více než čtyřnásobná oproti maximální době uchovávání u provozních a lokalizačních údajů sbíraných dle § 97[22]. Speciálně společnost Vodafone byla ve svém vyjádření přesnější, když uvádí:

„Doba zpracování údajů je závislá na účelu pro něž jsou data zpracovávána; pro vymáhání pohledávek vzniklých z titulu poskytování služeb elektronických komunikací jsou data zpracovávána i více než 24 měsíců. Provozní a lokalizační data jsou zpracovávána pouze po dobu uloženou zákonem.“

Data o uživatelích tedy mají pro obchodní záměry firmy různou hodnotu, což přímo určuje i rozsah a dobu uchovávání. Jakou hodnotu mají pro firmu provozní a lokalizační data, jež jsou uchovávána na základě § 97? Vyjádření firmy Vodafone nám napovídá, že záleží na důležitosti pro možné vymáhání pohledávek. Bude předmětem dalšího šetření, zda a jaká část dat sbíraných na základě § 97 překrývá i s daty uchovávanými dlouhodoběji.

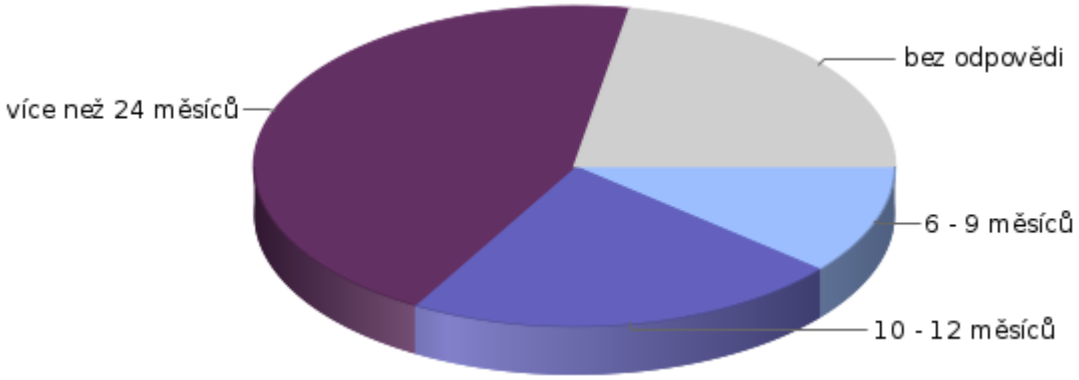
Obrázek 3: Rozsah uchovávaných dat dle odpovědí firem



[21] Povinnost vzniká na základě § 88 odst. c) zákona o elektronických komunikacích 127/2005 Sb.: *Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací podle písmen a) a b) vnitřní technicko-organizační předpis; ochranu údajů a důvěrnost komunikací zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany.*

[22] Zákon 127/2005 Sb. stanoví dobu uchovávání, která *nesmí být kratší než 6 měsíců a delší než 12 měsíců* (§ 97, odst. 3), vyhláška 485/2005 Sb. to dále zpřesňuje a *údaje se uchovají po dobu 6 měsíců* (§ 4, odst. 1).

Obrázek 4: Doba, po kterou jsou data uchovávané dle odpovědí firem



Doporučení: Firmy by měly zvážit alternativu předplacených služeb. Ušetřily by si starost s vymáháním pohledávek za neuhrazené služby a nemusely by pro tyto účely sbírat osobní údaje zákazníků. Omezil by se tak i rozsah údajů sbíraných na základě § 97.

- Většina společností udává nějakou formu ochrany dat o uživatelích proti potenciálnímu zneužití ze strany svých zaměstnanců (7 firem), avšak úroveň ochrany je pravděpodobně různá, protože se firmy neodkazují na standardizované normy (pouze jedna firma se přihlásila k metodickým standardům ISO[23].).

- Necelá polovina firem (4 firmy) nechává prověřovat zabezpečení dat s informacemi o svých uživatelích nezávislým auditem.

Dobrou zprávou je, že data jsou zpravidla nějak chráněna. Odpovědi firem o způsobu ochrany dat jsou však různé, s výjimkou jedné firmy se žádný z respondentů neodkazoval k nějaké formě standardů zabezpečení dat.

Doporučení: Zabezpečení dat o zákaznících firmy by mělo být postaveno na jasně deklarovaných standardech[24], které by měly být pravidelně testovány prostřednictvím auditu. Výsledky auditu by měly být publikovány. Taková transparentnost bezpečnostní politiky firmy dává dobrý signál zákazníkům, že si firma svěřených dat opravdu váží.

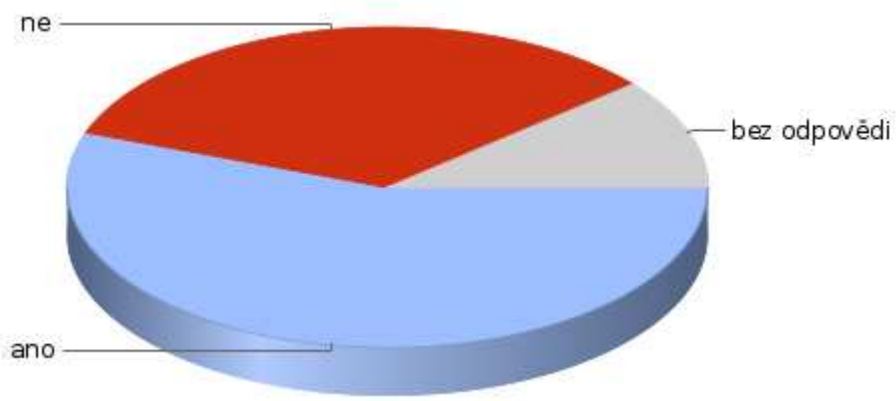
- Přes polovinu dotazovaných firem (5 firem) deklaruje, že své zákazníky informuje o rozsahu a zabezpečení uchovávaných dat

- Více než polovina dotazovaných firem má vypracovaný dokument politiky správy osobních údajů (5 firem), avšak některé z těchto firem udávají, že tento dokument mají v neveřejné podobě (2 firmy)

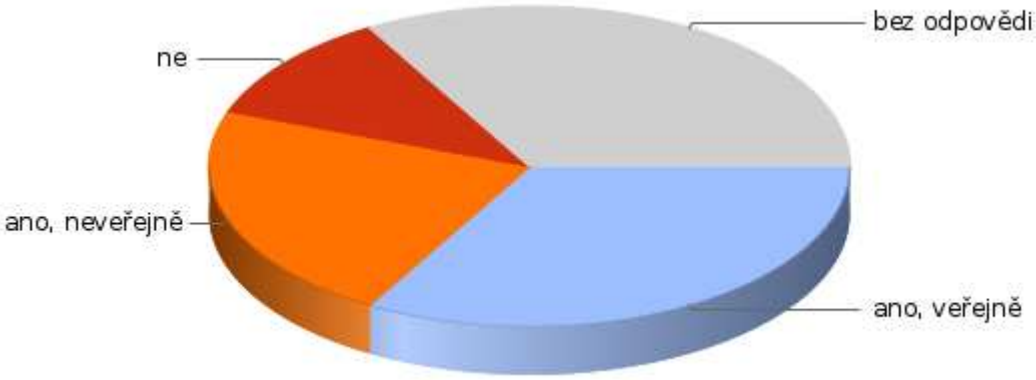
Obrázek 5: Rozložení odpovědí dotazovaných firem na otázku „Informujete uživatele vašich služeb o rozsahu a zabezpečení uchovávaných dat?“

[23] Dle vyjádření firmy: *Společnost Vodafone Czech Republic a.s. jakožto člen skupiny Vodafone Group má pro práci s daty uživatelů nastavena opatření v rozsahu tzv. Minimum security Requirements, které odráží požadavky ISO/IEC 27001 a ISO/IEC 27002 (dříve ISO/IEC 17799).*

[24] Kromě šířeji formulovaných standardů ISO může být příkladem garanta dodržování standardů politiky správy osobních údajů například organizace eTrust, která standardy tohoto typu stanovuje a kontroluje jejich dodržování u těch, kdo se ke standardům přihlásí - viz http://www.etrust.org/



Obrázek 6: Rozložení odpovědí dotazovaných firem na otázku „Uveďte prosím odkaz na „Privacy Policy" (politiku správy osobních údajů) vaší firmy, máte-li“



Je patrné, že kvalita informování zákazníků se liší napříč firmami. Dvě podobné otázky[25] pro nás překvapivě nutně neznamenaly shodné odpovědi. Například firma Centrum Holdings uvedla, že své zákazníky neinformuje o rozsahu a zabezpečení uchovávaných dat, avšak uvedla odkaz na svou politiku správy osobních údajů. Oproti tomu firma Etarget deklaruje, že své zákazníky informuje o rozsahu a zabezpečení uchovávaných dat, nicméně odkaz na politiku správy osobních údajů nebyl uveden. Překvapením pro nás bylo uvedení neveřejné politiky správy osobních údajů (firmy Volný a Vodafone).

Setkali jsme se také s jevem, kdy je dokument o politice ochrany osobních údajů součástí smluvních podmínek, které jsou však formulovány jako ochrana firmy. Zákazník se tudíž dozví, na co všechno nemá právo, co vše mu není garantováno a na jaké jmenovité položky právo má. Obecně kvalitnější dokumenty politiky ochrany osobních údajů mají velké firmy poskytující připojení k internetu a velcí zahraniční poskytovatelé služeb. Naopak u malých firem se můžeme setkávat s dodržováním nepsané praxe, skutečná správa osobně vztažitelných dat zákazníka může být i více pečlivá než u velkých firem – nebo může být i velmi nezodpovědná. Srovnání reálné praxe firem v poskytování služeb v souvislosti s psanými a nepsanými pravidly by však přesahovalo zaměření tohoto výzkumu.

Doporučení: Politika ochrany osobních údajů má zákazníkovi srozumitelně ukázat, že firma si jeho osobních údajů váží a spravuje je zodpovědně. Text by měl odrážet reálné dotazy a problémy zákazníků, měl by být průběžně doplňován. Firmy by v otázce správy osobně vztažitelných dat

[25] Do dotazníku jsme zařadili dvě podobně znějící otázky na téma komunikace se zákazníky. Otázka č. 8: *Informujete uživatele vašich služeb o rozsahu a zabezpečení uchovávaných dat?* a otázka č. 13: *Uveďte prosím odkaz na „Privacy Policy" (politiku správy osobních údajů) vaší firmy, máte-li.*

zákazníků měly být pokud možno transparentní. Otevřenost firmy signalizuje, že i před skutečnými problémy se firma neuzavírá, ale je ochotna je řešit.

- Části dotazovaných firem (3 firmy) byly státem uhrazeny náklady na vybudování infrastruktury pro sběr a bezpečné uchovávání provozních a lokalizačních údajů

Zde je zajímavé, že ve všech případech se jednalo o poskytovatele telefonní služeb – Telefonica O2, T-Mobile a MobilKom (provozovatel mobilního operátora značky U:fon). Ačkoli na uhrazení takových nákladů mají firmy právo ze zákona, žádná další firma neuvedla, že by této možnosti využila. Domníváme se (mimo jiné i na základě článku Kučera 2009), že v praxi jsou firmy, které uplatňují úhradu nákladů, nejčastějším terčem dotazů státních bezpečnostních orgánů. Zároveň celý proces zpracování, zabezpečení a předávání provozních a lokalizačních údajů dle § 97 je poměrně složitý a pro malé firmy může být příliš náročné ho celý zvládnout (příklad ze zahraničí viz Grant 2009).

Doporučení: Pokud je firma terčem častých žádostí ze strany bezpečnostních orgánů státu o poskytnutí provozních a lokalizačních údajů zákazníků, měla by zvážit nechat si výdaje uhradit. Pokud jsou ve firmě dotazy státních bezpečnostních orgánů výjimečné, je pravděpodobné, že by se po zavedení procedury úhrady nákladů na poskytnutí informace mohla četnost dotazů i kontrol zvýšit.

- Dvě dotazované firmy uvedly, že poskytují anonymizovaná data o svých zákaznících v rámci obchodní spolupráce třetím stranám

Tímto jsme v našem výzkumu získali potvrzení, že dochází ke komerčnímu poskytování anonymizovaných dat třetím stranám v Česku. Prověření, jakými metodami je anonymizace prováděna a zda nelze z anonymizovaných dat zpětně rekonstruovat identitu uživatele bude předmětem dalšího zkoumání.

Doporučení: Pokud firma provádí anonymizaci dat, měla by zajistit, aby osobní údaje nebylo možno z anonymizovaných dat zpětně zrekonstruovat (viz doporučení Pracovní skupiny pro ochranu údajů zřízené podle článku 29 (WP 148) 2008). Tím spíše, pokud jsou anonymizovaná data poskytována dále třetím stranám.

- Polovina dotazovaných firem uvedla, že poskytuje svým zákazníkům nějakou formu šifrování internetového připojení – většinou se to omezuje však pouze na šifrované posílání přihlašovacích údajů

- Žádná z dotazovaných firem neuvedla, že by svým zákazníkům poskytovala možnost identifikace pomocí služby třetí strany (např. OpenID, Facebook Connect)

Dotazované firmy a možná obecně firmy v Česku nevěnují metodám zlepšení ochrany soukromí[26] přílišnou pozornost. Je pravděpodobné, že je to způsobeno i tím, že to nepožadují v dostatečné míře samotní uživatelé.

Doporučení: Firmy by měly pokud možno nabízet použití metod a technologií pro lepší ochranu soukromí alespoň jako možnou alternativu. Měly by uživatele informovat o metodách zabezpečení jejich údajů pomocí běžně dostupných nástrojů šifrování a anonymizace.

Z porovnání získaných dat dále vyplynulo, že firmy, které jsou registrovány u ÚOOÚ pro nakládání s osobními údaji, prověřují s větší pravděpodobností své zabezpečení pravidelným auditem. Zároveň jsou to s větší pravděpodobností firmy, které dostaly uhrazeno od státu vybudování

[26] Privacy enhancing technologies (angl.) – používá se zkratka PET

infrastruktury ke sběru a bezpečnému uchovávání provozních a lokalizačních údajů. Domníváme se, že tyto výsledky opět reflektují existující hranice mezi poskytovateli připojení k internetu a mezi poskytovateli webových služeb, na kterou jsme již poukazovali v úvodu studie. Zároveň však praxi běžnou u poskytovatelů připojení k internetu selektivně přebírají i někteří poskytovatelé webových služeb, čímž se hranice mezi oběma oblastmi poskytovaných služeb naopak stírá.

4.2.2. Druhá fáze dotazování: Rozhovor a emailové dotazy

Ve druhé části výzkumu jsme se obraceli na firmy, které byly ochotny odpovídat na naše otázky v první části výzkumu. Původně jsme ve druhé části výzkumu počítali pouze s osobními rozhovory se zástupci zúčastněných firem. Kvůli kapacitním i časovým limitům jsme uskutečnili pouze jeden pilotní rozhovor (se zástupcem firmy T-Mobile), komunikace s dalšími firmami probíhala písemně. Takto jsme získali vyjádření od 4 firem. Písemné otázky byly zacílené na témata vytipovaná na základě pilotního rozhovoru. Rozhovory a debaty se zástupci zúčastněných firem bychom rádi uskutečnili v dalších fázích výzkumu.

Konkrétně jsme se ve druhé části výzkumu zaměřovali na informace o praxi komunikace s bezpečnostními složkami v rámci předávání údajů uchovávaných firmami na základě § 97: na četnost a formu kontaktu se zástupci bezpečnostních orgánů státu, na kontrolu oprávněnosti požadavků na předání údajů (seznam firem, které odpovídaly ve druhé části výzkumu viz Tabulka 2 v kapitole 4.1).

Z odpovědí se podařilo zjistit následující poznatky:

- Všichni dotazovaní mají zkušenost s kontaktem s bezpečnostními složkami.
- Četnost kontaktu s bezpečnostními orgány státu je různá – u největších firem se vyplatí přidělit pracovníka na tuto agendu, o malých firem se jedná spíše o výjímečnou záležitost.
- Žádná dotazovaná firma neuvedla, že by měla s bezpečnostními složkami ustanovený dálkový přístup[27].
- Kontakt s bezpečnostními složkami při předávání údajů je převážně písemný – papírovou i elektronickou formou.

Vzhledem k tomu, že pro získání provozních a lokalizačních údajů o uskutečněné komunikaci potřebuje pracovník bezpečnostního orgánu státu oprávnění[28], je elektronický kontakt pro předání takového oprávnění nedostatečný, není-li autentifikován například formou elektronického podpisu. Například dotazovaný zástupce firmy T-Mobile uvedl, že elektronický kontakt probíhá až na základě předání příslušného pověření papírovou formou. U firem, které jsme dotazovali písemně, se nám nepodařilo konkrétní praxi prokazování oprávnění k předání údajů prověřit tak detailně.

- Všichni dotazovaní uvedli, že předávají údaje až na základě platného pověření ze strany bezpečnostní složky. Systematičtější přístup vykázaly spíše velké společnosti. U malých firem, kde je kontakt s bezpečnostními složkami výjimečný, nebývá stanovena jasná metodika pro předávání údajů.

[27] Specifikace dálkového přístupu státních bezpečnostních orgánů k uchovávaným provozním a lokalizačním údajům je součástí vyhlášky 485/2005 Sb.

[28] Policie žádá *„způsobem, který umožní policii uchovávat identifikační údaje o útvaru policie nebo o policistovi, který o poskytnutí informací žádal, a o účelu, k němuž bylo o poskytnutí informací žádáno, nejméně po dobu 5 let.“* (zákon 273/2008 Sb. § 66 odst. 4), což ukazuje na nutnost vnitřní dokumentace žádosti policií. Z toho vyvozujeme nutnost prokazovat se oprávněním, nicméně interpretace způsobu prověření se žádajícím bezpečnostním orgánem státu není dle našeho názoru z pohledu dotčených firem jednoznačná a v praxi se může projevovat různě.

- Dva respondenti výslovně uvedli (Volný a T-Mobile), že neúplné žádosti o předání údajů odmítají.

Domníváme se, že malé firmy obecně vykazují nižší míru informovanosti o problematice předávání údajů. Domněnka se zakládá i na výsledcích z dotazníku, které ukazují, že malé firmy si nenechávají hradit náklady na uchovávání a předávání provozních a lokalizačních údajů dle § 97.

- Žádosti o předání provozních a lokalizačních údajů chodí nejčastěji od policie.

Doporučení: Malé firmy by si měly být vědomi svých povinností a práv v oblasti předávání provozních a lokalizačních údajů. Zvláštní důraz by měl být kladen na dostatečné ověření oprávnění pro předání údajů a na dokumentaci každého takového zaznamenaného případu[29].

5. Shrnutí výsledků výzkumu

V naší studii jsme na základě seznámení se s právními předpisy (zákon o elektronických komunikacích a zákon na ochranu osobních údajů) provedli výzkum a analýzu praxe zpracování, zabezpečení a předávání osobních údajů (s důrazem na provozní a lokalizační údaje dle § 97) u vybraných poskytovatelů služeb připojení k internetu a vybraných poskytovatelů webových služeb. Výsledný obrázek jsme se snažili zpětně konfrontovat s právními předpisy, ze kterých jsme vycházeli.

Podařilo se nám identifikovat několik problematických momentů, které jsou z pohledu ochrany osobně vztažitelných dat důležité.

Potvrdil se nám teoretický předpoklad **nejednoznačnosti právních norem**. Zaznamenali jsme zpoždění vývoje právních norem za vývojem komunikačních technologií. Na základě zpoždění vývoje právních norem jsme dospěli k významnému rozdělení námi zkoumaného vzorku firem na dvě výrazně odlišné oblasti, které jsme nazvali poskytovatelé služeb připojení k internetu a poskytovatelé webových služeb. Výrazným jevem v oblasti poskytovatelů webových služeb je fakt, že se firmy podnikající v tomto odvětví často necítí být provozovateli služeb elektronických komunikací. Zároveň data zákazníků v této oblasti podnikání často nebývají považovány za osobní údaje. V prvním případě to má za následek absenci procesů uchovávání provozních a lokalizačních údajů pro potřeby stanovené dle § 97, na druhé straně to s sebou nese i skutečnost, že data zákazníků nepodléhají zákonné ochraně vyhrazené osobním údajům. Ještě složitější situace je u webových služeb poskytovaných **zahraničními firmami**, kde zákonné normy nejen zaostávají za technologickým vývojem, ale zůstávají často v zajetí pohledu definovaném národní státy, i když realita v této oblasti je globální. Navíc se zde setkáváme s koncepčními neshodami na definici pojmu osobní údaje ze strany Spojených států a EU (viz závěry Pracovní skupiny pro ochranu údajů zřízené podle článku 29 (WP 148) 2008).

Velmi výrazným jevem, který souvisí s již zmíněným zpožděním zaváděním zákonů oproti technologickému vývoji, je vydělení skupiny firem poskytujících služby připojení k internetu. Tyto firmy mají obecně delší tradici v podnikání, často dříve podnikaly v telefonních službách. Pro tyto firmy jsou také současné zákony poměrně srozumitelné a domníváme se, že jsou psány s ohledem na tyto „tradiční“ firmy. Poskytovatelé služeb připojení k internetu byli zároveň celkově výrazně ochotnější se zúčastnit naší studie. Naopak jsme zaznamenali neochotu účastnit se naší studie ze strany některých poskytovatelů webových služeb. Některé poskytovatele webových služeb se nám v rámci našeho výzkumu nepodařilo zkontaktovat, zvláště to platí u velkých nadnárodních firem.

[29] Povinnost vést evidenci o žádostech o předání provozních a lokalizačních údajů ukládá firmám § 97, odst. 10 zákona 127/2005 Sb. o elektronických komunikacích.

Webové služby poskytované zahraniční firmou se fakticky, pokud firma fyzicky nepodniká v ČR, nemusí podřizovat všem zákonům ČR (tj. nepodléhají stejné kontrole jako české firmy). Zákonné normy zůstávají často v zajetí pohledu definovaném národními státy, i když realita v této oblasti je globálního charakteru.

V průběhu studie se dále ukazuje, že důležitost osobních údajů pro firmu se podstatně liší v závislosti na tom, zda firmy poskytují placené služby, nebo služby „zdarma“ hrazené z příjmů z reklamy. V prvním případě pro firmy má uchovávání a ověřování osobních údajů význam hlavně ve vztahu k vymáhání pohledávek za případné neuhrazené služby. V případě služeb hrazených z příjmů z reklamy není pro firmy tolik důležitá identifikace zákazníka na základě osobních údajů, ale rozlišitelnost zákazníka pro získávání údajů pro cílenější a tedy účinnější reklamu (Lenssen 2010).

Z dotazování firem se dozvídáme informace o konkrétní praxi při práci s daty zákazníků poskytovaných služeb. Základním poznatkem je skutečnost, že práce s daty zákazníků je ve firmách různá, nicméně data podléhají většinou nějaké formě ochrany. Zarážející je častá netransparentnost bezpečnostních opatření a auditů těchto opatření. Rozsah a doba uchovávání údajů o používání služby zákazníkem je v případě dotazovaných firem většinou větší, než je stanoveno zákonnými požadavky v případě uchovávání provozních a lokalizačních údajů dle § 97 (127/2005 Sb.). Vyvozujeme z našich poznatků, že ochrana osobních údajů není velmi často dostatečná a není dostatečně kontrolována ani zevnitř firem, ani zvenku.

Míra komunikace se zákazníky je velmi různá: Některé firmy zákazníky neinformují o opatřeních ochrany jejich dat vůbec. Často chybí veřejně deklarované zásady ochrany dat zákazníků (např. formou politiky správy osobních údajů).

Firmy většinou poskytují jen velmi omezené metody pro zlepšení ochrany soukromí – šifrování přenosu mezi webovým prohlížečem a svými servery nabízejí některé firmy alespoň pro přenos přihlašovacích údajů. Pouze v případě jednoho z malých poskytovatelů služeb připojení k internetu jsme se setkali s přístupem, který nabádá uživatele k používání vlastních metod šifrování a anonymizace komunikace, jako efektivní cestu, jak omezit možnosti odposlechu komunikace. S autentizací pomocí nástrojů poskytovaných třetí stranou jsme se u respondentů dotazníkového výzkumu nesetkali.

Zejména velké firmy z oblasti služeb připojení k internetu mají celý proces zpracování, zabezpečení, předávání a případné anonymizace dat technologicky zvládnutý a rutinní. Výsledně jsou právě velké firmy z této oblasti podnikání nejčastěji kontaktovány bezpečnostními složkami. Tyto kontakty jsou dle vyjádření dotazovaných firem korektní, firmy mají pro tuto agendu často speciálně vyčleněného pracovníka. U žádné oslovené firmy jsme se nesetkali se zavedeným dálkovým přístupem státních bezpečnostních orgánů k provozním a lokalizačním údajům o zákaznících.

Malé firmy v oblasti poskytování služeb připojení k internetu mají na jedné straně ztíženou pozici tím, že celá procedura zpracování, zabezpečení a předávání údajů je poměrně komplexní. Domníváme se, že pro velmi malé firmy (například do 10 zaměstnanců) může být zvládnutí celé procedury velmi náročné. Na druhé straně jsme se nesetkali se zaplavováním malých firem dotazy ze strany bezpečnostních složek.

5.1. Doporučení: Shrnutí

Tabulka 4: Pět doporučení pro poskytovatele služeb

1.	Ujasnit si, zda firma spadá pod zákon o elektronických komunikacích (týká se webových služeb)
2.	Omezit objem uchovávaných osobně vztažitelných dat např. nabídkou anonymní varianty služby
3.	Důsledně chránit všechna data o zákaznících, důsledně anonymizovat data, která jsou používaná třetími stranami
4.	Informovat zákazníky otevřeně a kvalitně o zabezpečení jejich dat
5.	Informovat zákazníky o nástrojích pro lepší ochranu soukromí

Firma by si měla ujasnit, **zda spadá pod zákon o elektronických komunikacích**, § 97, a zda se ji tedy týká směrnice o uchovávání dat provozních a lokalizačních dat pro potřeby bezpečnostních orgánů státu. Na jedné straně zde máme poskytovatele připojení k internetu, kteří se dle našeho výzkumu cítí být předmětem zákona o elektronických komunikacích. Na druhé straně zde máme poskytovatele webových komunikačních služeb, kde situace není zdaleka tak jednoznačná. Některé firmy se cítí být zákonem vázány, jiné naopak deklarují, že pod zákon o elektronických komunikacích nespadají a příslušná data tedy neuchovávají (např. Seznam.cz). Vzhledem k tomu, že se najdou i velké firmy v oblasti webových služeb, které deklarují, že nespadají do působnosti zákona o elektronických komunikacích, a tedy ani pod povinnost na základě § 97, je možné z tohoto příkladu vycházet v praxi.

Spadá-li firma pod zákon o elektronických komunikacích, lze **omezit objem uchovávaných osobně vztažitelných dat** o zákaznících **anonymizací poskytované služby**. Příkladem může být model anonymních předplacených SIM karet. Na tomto příkladu je patrné, že sběr osobních údajů je pro firmy zásadní hlavně v oblasti vymáhání pohledávek a v oblasti uzavírání dlouhodobějších smluv. Pokud si firma nechá za své služby zaplatit předem a rezignuje-li na uzavírání dlouhodobé smlouvy se zákazníkem (nebo najde jiný obchodní model), sběr osobních údajů o zákazníkovi nemusí být pro poskytování služeb nutný. Podle znění zákona o elektronické komunikaci § 97 je dotčená firma povinna „uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací“. Zmiňované provozní a lokalizační údaje tedy nemusejí nutně znamenat svázání s osobními údaji.

Firma by si měla ujasnit, zda data, která o svých zákaznících uchovává, jsou osobními údaji. Vzhledem k tomu, že existují druhy údajů, které nejsou jednoznačně osobními údaji z důvodů zmiňovaných v kapitolách 1.2 a 4.1.2, může dotčená firma zvážit, zda opravdu pracuje s osobními údaji. Mnoho firem, které poskytují své služby zdarma, tedy nepotřebují sbírat osobní údaje pro účely fakturace, identifikují své zákazníky často na základě uživatelského jména. V našem výzkumu se často setkáváme se skutečností, kdy firmy údaje typu uživatelské jméno nepovažují za osobní údaj a tedy se necítí být vázány zákonem o ochraně osobních údajů. To může mít pro uživatele nepříjemné důsledky, protože i prakticky velmi osobní informace (např. přehled emailových kontaktů) nespadají pod ochranu stanovenou zákonem o ochraně osobních údajů. Praktickým doporučením pro firmu by měla tedy být **ochrana všech dat o zákaznících**, nejen explicitně osobních údajů. Případně by firma dnes nadstandardní míru ochrany osobně vztažitelných dat (například nepoužívání údajů k cílené reklamě) mohla zpoplatnit.

Ochrana osobně vztažitelných dat zákazníků se stává velmi citlivým tématem hlavně pro samotné zákazníky[30]. V současné době se průběžně zvyšuje povědomí zákazníků o problematice ochrany osobně vztažitelných dat. Zákonné úpravy věnující se této problematice vznikají za běhu a postupně se přizpůsobují technologické praxi. S velkou pravděpodobností se můžeme domnívat, že

[30] Zvyšování zájmu zákazníků na ochraně jejich osobně vztažitelných dat soudíme z faktu, že technologický rozvoj pomalu prostupuje společnost, pokročilé nástroje online komunikace používá stále více lidí. Tím se také zvyšuje povědomí o možných hrozbách pro ochranu soukromí. Například v online rozhovoru serveru Ekonom (Křešnička 2009), který je zaměřen na problematiku sociálních sítí, je vidět velký zájem tazatelů právě o otázky ochrany soukromí.

zákony budou zpřesňovány tak, aby se co nejvíce blížily skutečným problémům, se kterými se setkáváme v praxi. Zpřísnění vymezení pojmu osobních údajů povede k situaci, kdy do oblasti přísné ochrany dat budou spadat i data, která tam dnes nespadají. Pro firmy to bude znamenat další zvyšování nákladů na zabezpečení a zároveň i větší riziko úniku citlivých dat. Z tohoto pohledu považujeme za důležité zvážit, zda sběr osobně vztažitelných dat je pro podnikání firmy nutností, nebo zda lze uvažovat o minimalizaci objemu sbíraných dat.

Vyšší zájem zákazníků služeb o problematiku ochrany dat bude pravděpodobně v budoucnu znamenat, že míra ochrany osobně vztažitelných dat se zařadí mezi důležité ukazatele kvality nabízených služeb v konkurenčním prostředí. Proto doporučujeme **zákazníky kvalitně informovat o celé problematice zabezpečení jejich dat**. V našem výzkumu se ukazuje, že mnoho firem v českém prostředí je poměrně dosti komunikačně uzavřených a o svých službách informují své zákazníky jen v míře dle jejich názoru nezbytně nutné. Otevřenost v komunikaci může být dle našeho názoru důležitý moment pro budování vztahu k zákazníkovi. Proto doporučujeme vypracovat pro zákazníky vstřícné informační prostředí, které uspokojí jejich dotazy. Zákazník by měl mít možnost veřejně žádat i obdržet odpověď[31]. V tomto ohledu by se české firmy mohly nechat inspirovat od zahraničních firem, a to i z toho důvodu, že zahraniční firmy stále častěji vstupují do konkurence v českém prostředí.

Dalším krokem k vyšší ochraně soukromí by ze strany firem mělo být **zvyšování povědomí o nástrojích pro lepší ochranu soukromí**: Firmy mohou sami takové nástroje nabízet především pro zvýšení ochrany přenosu zpráv přes nezabezpečené části sítě (internet), dále mohou poskytnou zákazníkům informace o možných dalších metodách ochrany (šifrování, anonymizace).

Věříme, že pokračující veřejná diskuze o sledované problematice se zapojením všech zúčastněných stran, se stane platformou pro hledání vyváženého přístupu k uplatňování práva na soukromí i bezpečnostních zájmů orgánů veřejné moci.

[31] Pokud se inspirujeme u velkých zahraničních firem v našem výzkumu, můžeme jmenovat komponenty prostředí vstřícného k zákazníkovi: 1. Zveřejněné často kladené dotazy doplněné podrobnou dokumentací. 2. Deklarované zásady, doplněné mechanismem kontroly uplatňování těchto zásad. 3. Kontaktní místa – pestrá nabídka způsobů, jak se zeptat – od telefonní hotline po účast v sociálních sítích; skutečně odpovídat na dotazy. 4. Další komunikační kanály pro nestandartní případy (ombudsman apod.).

6. Přílohy

6.1. Příloha 1: Dotazník k první části výzkumu

Praxe poskytovatelu verejných internetových služeb pri správe

Strana 1

Otázky v tomto dotazníku jsou zaměřeny na praxi vaší firmy v zacházení s osobními daty vašich zákazníků. Tímto výzkumem chceme přispět k vytváření dobré praxe poskytovatelů veřejných internetových služeb, a to hlavně při práci s osobními údaji zákazníků. Proto jsme oslovili vybrané velké společnosti, které poskytují internetové služby pro občany. Hledáme řešení, jak vyhovět zákonným povinnostem vaší firmy s co nejnižšími náklady při zachování maximální efektivity. Jedním z výstupů výzkumu by měla být metodická doporučení, která uveřejníme a budou k dispozici zdarma.

Odkazujeme-li se na platné zákony, jedná se zejména o Zákon o elektronických komunikacích (zákon č. 127/2005 Sb.), Zákon o ochraně osobních údajů (zákon č. 101/2001 Sb.) a příslušné vyhlášky (zejména vyhláška č. 485/2005 Sb. a č. 486/2005 Sb.).

Jedná se celkem o 14 otázek, jejich vyplnění by vám nemělo zabrat více než 20 minut. Budeme rádi, odpovíte-li na všechny otázky, ale není to podmínkou. Své odpovědi můžete volně upravovat až do odeslání dotazníku.

V případě dotazů a připomínek k výzkumu nás neváhejte kontaktovat na emailové adrese kucera@iure.org

1. Prosím uveďte název vaší firmy

2. Máte ve vaší firmě ustanovenou interní metodiku pro sběr, uchovávání a zabezpečení dat o uživatelích vašich služeb?

- ◯ Ano
- ◯ Ne

3. Dostala vaše firma od státních orgánů pokyny pro sběr, uchovávání a zabezpečení dat o uživatelích vašich služeb?

- ◯ Ano
- ◯ Ne
- ◯ Jiná odpověď (prosím upřesněte)

4. Data o uživatelích vašich služeb uchováváte

- ◯ v rozsahu sledovaných položek daných zákonem.
- ◯ ve větším rozsahu, než stanoveném zákonem (např. pro interní hodnocení vašich služeb, marketing)

5. Jak dlouho data o uživatelích vašich služeb uchováváte?

- ◯ 6 - 9 měsíců
- ◯ 10 - 12 měsíců
- ◯ 13 - 24 měsíců
- ◯ více než 24 měsíců

Praxe poskytovatelu verejných internetových služeb pri správe

6. Jakými opatřeními omezujete přístup zaměstnanců vaší firmy k uchovávaným datům o uživatelích vašich služeb? (Prosím stručně popište.)

7. Prověřujete zabezpečení uchovávaných dat o uživatelích vašich služeb nezávislým auditem?

- ◯ Ano, prověřili jsme jednorázovým auditem.
- ◯ Ano, prověřujeme pravidelnými audity.
- ◯ Ne, ještě jsme auditem neprověřili.

8. Informujete uživatele vašich služeb o rozsahu a zabezpečení uchovávaných dat?

- ◯ Ne
- ◯ Ano - uveďte prosím, kde lze tyto informace nalézt

9. Byly vám uhrazeny náklady na vybudování infrastruktury pro bezpečné uchovávání dat o uživatelích vašich služeb, jak stanoví zákon?

- ◯ Ano, úplně
- ◯ Ano, částečně
- ◯ Ne

Strana 3

10. Poskytujete v rámci obchodní spolupráce třetím stranám anonymizovaná data o chování uživatelů vašich služeb?

- ◯ Ano
- ◯ Ne

Praxe poskytovatelu verejných internetových služeb pri správe

11. Poskytujete uživatelům vašich služeb šifrované připojení (https apod.)

- ◯ Ano, vždy
- ◯ Ano, vždy (uživatel si musí šifrované připojení sám zapnout)
- ◯ Ano, pouze pro přihlašovací údaje
- ◯ Ano, pouze pro přihlašovací údaje, (uživatel si musí šifrované připojení sám zapnout)
- ◯ Ne
- ◯ Jiná varianta (prosím upřesněte)

12. Poskytujete uživatelům vašich služeb možnost identifikace pomocí služby třetí strany (OpenID, Facebook Connect, apod.)?

- ◯ Ano
- ◯ Ne
- ◯ Jiná odpověď (prosím upřesněte)

13. Uveďte prosím odkaz na „Privacy Policy" (politiku správy osobních dat) vaší firmy, máte-li:

14. Pokud autorům tohoto šetření chcete něco vzkázat, můžete tak učinit zde

6.2. Příloha 2: Otázky ke druhé fázi výzkumu

1. Byla vaše firma v poslední době kontaktována policií, zpravodajskou službou nebo jiným státním orgánem ve věci přístupu k datům o aktivitě uživatelů vašich služeb?

2. Jakým způsobem se přístup k datům realizoval (např. vyžádání si výpisu o komunikaci, přímý dálkový přístup k datům apod.)?

3. Jak často se podobné kontaktování děje (prosím odhadněte)?

4. Předložily vám dané orgány dokument (rozhodnutí soudu či státního zástupce), který by je opravňoval k přístupu k datům o uživatelích?

6.3. Příloha 3: Oslovení firem – emailová zpráva

Předmět: Iuridicum Remedium: Výzkum a hledání dobré praxe Vaší společnosti

Vážení,

jménem občanského sdružení Iuridicum Remedium (http://www.iure.org) chceme Vaši firmu požádat o účast ve výzkumu "Praxe poskytovatelů veřejných internetových služeb při správě osobních dat zákazníků".

Chceme tímto výzkumem přispět k vytváření dobré praxe poskytovatelů veřejných internetových služeb, a to hlavně při práci s osobními údaji zákazníků. Proto jsme oslovili vybrané velké společnosti, které poskytují internetové služby pro občany. Hledáme řešení, jak vyhovět zákonným povinnostem Vaší firmy s co nejnižšími náklady při zachování maximální efektivity.

Jedním z výstupů výzkumu by měla být metodická doporučení, která uveřejníme a budou Vám k dispozici zdarma.

Výzkum jsme se snažili navrhnout tak, aby Vás pokud možno co nejméně časově zatížil. Rádi bychom Vás pozvali k vyplnění online dotazníku (odkaz naleznete níže). Vyplnění dotazníku by Vám nemělo zabrat více než 20 minut.

Dotazník: [odkaz na formulář dotazníku]

Veškerá komunikace přenášená přes internet je šifrována - vážíme si údajů, které nám poskytnete.

Po vyplnění dotazníku bychom Vás rádi požádali o schůzku se zástupcem Vaší firmy, obeznámeným s praxí uchovávání údajů o elektronické komunikaci. Na schůzce bychom se rádi pokusili doplnit náměty, které se do dotazníku nevešly a vyjasnit nejasné nebo sporné otázky. Schůzka by neměla zabrat více než 30 minut.

Své případné dotazy prosím pište na email kucera@iure.org

S pozdravem

6.4. Příloha 4: Automatická reakce ze serveru Facebook (adresa press@facebook.com)

Hello,

Due to a high volume of requests, we are unable to respond to everyone immediately. We understand that you may be on deadline and will do our best to respond as quickly as possible. We also encourage you to visit our Press Page (www.facebook.com/press.php), where you will find general information such as the latest statistics.

If you are not a member of the press, please refer to the below resources and direct your inquiry appropriately:

* Help Center (http://www.facebook.com/help.php): If you are a user experiencing a problem with the site, or writing in with a suggestion

* marketing@facebook.com: If you would like to obtain permission to use Facebook's trademarks and/or copyrights for commercial and promotional purposes

* http://www.facebook.com/facebook#/press/request.php: If you have a speaking request

* http://www.facebook.com/advertising: If you are interested in advertising on the site

* http://www.facebook.com/sponsorship: If you would like to request Facebook's sponsorship of an event

Thanks,

The Facebook Corporate Communications Team

7. Zdroje

ČERMÁK, J. (2001): Vztah principu teritoriality a polohy serveru při určení rozhodného autorského práva na Internetu. Itprávo.cz, http://www.itpravo.cz/index.shtml?x=47573 (18. 1. 2010)
DAVIS, W. (2009): Court: IP Addresses Are Not 'Personally Identifiable' Information. Media Post NEWS, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=109242 (18. 1. 2010)
DOČEKAL, D. (2009): Česko v sociálních sítích. Lupa.cz, http://www.lupa.cz/clanky/cesko-v-socialnich-sitich/ (18. 1. 2010)
EDRI (2009a): Germany: Data Retention Is Disproportionate. EDRi-Gram, č. 7.6, http://www.edri.org/edri-gram/number7.6/data-retention-court-case-germany (18. 1. 2010)
EDRI (2009b): Romania: Data Retention Law Declared Unconstitutional. EDRi-Gram, č. 7.20, http://www.edri.org/edrigram/number7.20/romania-data-retention-law-unconstitutional (18. 1. 2010)
EDRI (2009c): Austria: BIM Delivers Draft Act On Implementing Data Retention Directive. EDRi-Gram, č. 7.23, http://www.edri.org/edrigram/number7.23/austria-data-retention-law (18. 1. 2010)
GRANT, I. (2009): Some ISPs more equal than others in data retention implementation. Computer Weekly, http://www.computerweekly.com/Articles/2009/04/08/235577/some-isps-more-equal-than-others-in-data-retention-implementation.htm (18. 1. 2010)
IURIDICUM REMEDIUM (2009): IuRe vyzývá poslance: zastavte slídění v soukromé komunikaci všech občanů. http://www.slidilove.cz/node/2189 (18. 1. 2010)
KŘEŠNIČKA, J. (2009): Ptali jste se na sociální sítě (online rozhovor s Janem Hornou). Ekonom.iHNed.cz, http://ekonom.ihned.cz/c1-38649220-ptali-jste-se-na-socialni-site (18. 1. 2010)
KUČERA, M. (2009): Velký bratr za 150 milionů korun. Týdeník EURO, č. 49/2009, http://www.euro.cz/detail.jsp?id=19883 (18. 1. 2010)
LENSSEN, P. (2010): German Spiegel on Google Goggles' Face Recognition and More. Google Blogoscoped, http://blogoscoped.com/archive/2010-01-10-n86.html (18. 1. 2010)
LOEBL, Z. (2003): Rozhodné právo a soudní pravomoc u obchodních transakcí prostřednictvím Internetu, I. E-PRÁVO.CZ, http://www.epravo.cz/top/clanky/rozhodne-pravo-a-soudni-pravomoc-u-obchodnich-transakci-prostrednictvim-internetu-i-20678.html (18. 1. 2010)
MALIŠ, P. (2008): Rozhodné právo sporů z internetových transakcí. Lawyer.cz, http://www.pravoit.cz/article/rozhodne-pravo-sporu-z-internetovych-transakci (18. 1. 2010)
POLČÁK, R. (2009): Odpovědnost poskytovatelů služeb informační společnosti. Právní rozhledy, č. 23/2009, s. 837-843
PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29 (WP 148) (2008): Stanovisko 1/2008 k otázkám ochrany údajů v souvislosti s vyhledávači. http://uoou.cz/files/wp148_cs.pdf (18. 1. 2010)
PRIVACY INTERNATIONAL (2007): A Race to the Bottom - Privacy Ranking of Internet Service Companies. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961 (18. 1. 2010)
SINGEL, R. (2007a): ISPs Questioned About Selling Your Surfing Habits. Wired, http://www.wired.com/threatlevel/2007/03/isps_questioned/ (18. 1. 2010)
SINGEL, R. (2007b): ISP Data Retention: Early Results In. Wired, http://www.wired.com/threatlevel/2007/03/isp_data_retent/ (18. 1. 2010)
SMEJKAL, V. (2004): Normativní systémy a Internet. http://www.znalci.cz/files/PDF/Kyberprostor_2004.pdf (18. 1. 2010)
WHITTEN, A. (2008): Are IP addresses personal?. Google Public Policy Blog, http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (18. 1. 2010)