

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra systémové analýzy

Diplomová práce

2012

Bc. Gerasim Farafonov

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra systémové analýzy

Osobní údaje a problémy personalizace

Vypracoval: Bc. Gerasim Farafonov
Vedoucí práce: Ing. Antonín Rosický, CSc.
Rok vypracování: 2012

Čestné prohlášení:

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V Praze dne 7. prosince 2012

Podpis:

Poděkování:

Na prvním místě chci velmi poděkovat panu Ing. Antonínu Rosickému, CSc. za odborné vedení, velice cenné rady a čas, který mi věnoval. Dále na tomto místě bych rád poděkoval pracovníkům Úřadu pro ochranu osobních údajů v Praze za konzultace a doporučení. V neposlední řadě děkuji své rodině za podporu v průběhu zpracování této diplomové práce.

Abstrakt

Společnost se v současné chvíli nachází uprostřed informační revoluce, a pouze teď si tuto skutečnost začíná uvědomovat. Primární měnou v nové ekonomice jsou uživatelská data a tato nesmírná hodnota je zřejmá pouze společnostem obchodujícím s nimi.

Diplomová práce se věnuje problematice ochrany osobních údajů v kontextu současného vývoje trendu personalizace. Autor vyjmenovává nástroje, pomocí kterých se uskutečňuje online sledování, jejich technickou náplň, porovnává legislativní úpravy České republiky, Ruské federace a Spojených států amerických, vyhodnocuje rozdíly, tendence vývoje, klady a zápory ve vztahu k praxi vytváření profilů a behaviorálního cílení reklamy. Následně autor vyjmenovává další rizika tohoto trendu pro svobodu a soukromí a sestavuje seznam jak obecných doporučení, tak i doporučení pro samotné uživatele pro maximalizaci ochrany soukromí a osobních údajů.

Klíčová slova:

Online sledování, Profilování, Behaviorální cílení, Personalizace, Bublina filtrů, Google, Facebook, Cookies, Osobní údaje, Soukromí.

Abstract

Society is currently finding itself in the middle of an information revolution, and only now begins to realize this fact. The primary currency in the new economy is user data and the enormous value is evident only to companies doing business with them. This thesis is dedicated to the protection of personal data in the context of the currently developing trend of personalization. Author sets out tools that make online tracking possible, compares the legislative regulation of the Czech Republic, the Russian Federation and the United States of America, evaluating the differences, trends, strengths and weaknesses in relation to the practice of creating profiles and behavioural targeting advertising. Subsequently, the author lists the additional risks of this trend for the freedom and privacy, lists general recommendations as well as recommendations for the users themselves to maximize the protection of privacy and personal data.

Keywords:

Online tracking, Profiling, Behavioural targeting, Personalization, Filter bubble, Google, Facebook, Cookies, Personal data, Privacy.

Obsah

Úvod.....	1
1 Vymezení tématu a základní pojmy tykající se osobních údajů a personalizace.....	4
1.1 Cookies.....	4
1.2 HTML cookies	5
1.2.1 Cookies třetích stran.....	6
1.2.2 Flash cookies	7
1.2.3 Ostatní cookies	10
1.3 Alternativa cookies.....	10
1.4 Personalizace	14
1.5 Profilování	14
1.6 Behaviorální marketing	17
2 Specifika vybraných serverů a služeb	19
2.1 Prohlížeče a politika společnosti	19
2.2 Google	20
2.3 Facebook	22
3 Typické přístupy neodpovědného nakládání s osobními údaji	24
4 Typické způsoby zneužívání osobních údajů, včetně porušování jejich ochrany a jejich analýza.....	25
4.1 Definice sledovacích serverů třetích stran.....	25
4.2 Google a DoubleClick	31
4.3 Google Analytics	32
4.4 Facebook	34
4.5 Ostatní servery	41
4.6 Agregátory dat	42
4.7 Bublina Filtrů	45

5	Technická a právní ochrana osobních údajů, porovnání situace v ČR, v Ruské federaci a v USA	48
5.1	Česká republika	48
5.1.1	Evropa	51
5.1.2	Vymezení pojmů souvisejících se zákonem o OOÚ.....	52
5.2	Ruská federace	57
5.3	Spojené státy americké	60
5.4	U. S. – EU Safe Harbor	62
6	Porovnání situace ve výše uvedených zemích, jejich vyhodnocení a doporučení pro zlepšení situace v ČR	64
6.1	Porovnání a vyhodnocení	64
6.2	Informační etika a soukromí.....	68
6.3	Obecná doporučení.....	70
6.4	Doporučení pro uživatele	74
	Závěr	78
	Seznam použité literatury.....	81
	Literatura	81
	Internetové zdroje.....	82
	Seznam obrázků	85
	Seznam tabulek	85

Úvod

Existenční problematika člověka je jeho základní problematikou. Existence člověka má řadu forem, řadu projevů, je k ní možno přistupovat z různých významových hledisek. Jednou z forem existence je chování člověka.

Člověk jako jedinec žije ve stavu nekončící informační potřeby, musí neustále být ve stavu rovnováhy se svým existenčním prostředím jednoduše proto, aby přežil, aby jeho chování bylo v souladu s externími podmínkami.

Tím chce autor jednoduše naznačit to, že lidská činnost závisí na výměně informací, že jednotlivci jsou součástí společnosti, ve které existují, a až na extrémní výjimky nejsou schopné fungovat bez interakce s vnějším prostředím. Frekvence životních změn společnosti, ve které žijeme, nabývá na dynamičnosti. Výrazným prvkem změn je vývoj stále sofistikovanějších technologií. Jednou stranou vývoje by měl být pokrok lidstva a kvalitativní přínos pro život jedince. Druhou stranou novodobých technologií jsou invazivní prvky, které mohou negativním způsobem ovlivňovat každodenní život. Moderní technologie nám umožňují shromažďovat, vyhodnocovat, přenášet a zpracovávat dosud nevídané množství dat. Lidé dnes mají přístup k informacím, které dříve k dispozici nebyly. Úměrně tomu se zvyšuje i riziko průniku do soukromí jednotlivce a dalších nechtěných důsledků. Oblasti, která se z tohoto pohledu jeví vysoce rizikovou, je ochrana osobních údajů a soukromí. Skutečnosti, které byly před několika lety námětem literatury science-fiction, se dnes díky novodobým technologiím stávají realitou a často i reálnou hrozbou ¹.

Ochrana osobních údajů a údaje samotné jsou stále se rozvíjející a diskutovanou oblastí práva. S těmito pojmy se setkáváme v každodenním životě například při jednání s úřady či bankami, když předkládáme průkaz totožnosti nebo potvrzujeme-li svým podpisem, že souhlasíme se zpracováním osobních údajů. Na druhé straně ale nejsou ojedinělé případy, kdy dochází k neoprávněnému zpracování nebo zveřejnění osobních údajů.

V názvu této práce stojí slovo personalizace, které je v kontextu myšleno jako hrozba pro soukromí kvůli neoprávněnému zacházení s osobními údaji. Ihned v úvodu chci zdůraznit několik skutečností. V česky psané literatuře slovo personalizace pojímá pouze trend ve vývoji webových stránek, kdy personalizace vyjadřuje možnost

¹ *Ochrana osobních údajů: vybrané otázky: příručka pro podnikatele*. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011, 50 s. ISBN 978-80-210-5572-8.

přizpůsobit webovou stránku svým potřebám. V tomto pohledu důležitým elementem je aktivní vztah uživatele a jeho informovanost. V anglických odborných člancích je slovo personalizace v poslední době, a to zdaleka ne tak často, užíváno pro automatizované tvoření obsahu webu pro každého jednotlivého uživatele, a to na základě vytvořeného pro něj profilu. Tady autor má na mysli dvě podoby – filtrování výsledků vyhledávání a reklamy na webu, které jsou určeny pro konkrétního uživatele. V tomto pohledu důležitým elementem je neaktivní vztah uživatele a jeho naprostá neinformovanost.

Pokud si uživatel myslí, že se mu nikdy nezobrazovala reklama cílena na základě jeho chování online, pak pravděpodobně si nedává pozor. Podle neoficiálního průzkumu, více než 90% reklamních kampaní v roce 2011 zahrnovalo sledování jakéhokoliv druhu. Reklamní byznys miluje online sledování stejně tak, jak obránci soukromí ho nenávidí. Pro vytvoření přesnějšího a objektivnějšího celkového obrázku ve vztazích základních pojmů, které se budou objevovat napříč touto prací, je nutné zmínit jakýsi logický řetěz pojmů. Nejprve se pomoci různých nástrojů sleduje každý (a to doslova) pohyb kteréhokoliv uživatele na webu, na základě získaných dat se uživateli přiřadí parametry – jeho vlastnosti a vytvoří se profil. Tyto uživateli přiřazené parametry se můžou týkat jak osobních tak i citlivých údajů a definují jeho patřičnost k obecnější skupině profilů, které jsou užívány jak soukromými společnostmi pro generování zisku, tak i vládami.

Marketingové společnosti využívají profily pro cílenou reklamu. Reklama je tedy cílená na základě chování uživatele na webu. Vyhledávači ukazují personalizované (jiné) výsledky na stejný dotaz různým uživatelům. Sociální sítě rozhodují za samotné uživatele, které příspěvky kamarádů ukazovat a které ne. To vše vyúsťuje do personalizace.

Sledování každého pohybu uživatele online je porušováním soukromí. To je jako být sledován neviditelným stopařem – jedinci si nejsou vědomí této skutečnosti, uživatelé neví kdo je sleduje, a jak jsou jejich informace užívána. Uživatelé nejsou dotazováni pro jejich souhlas a nemají žádnou smysluplnou kontrolu nad sběrem a použitím jejich informací, které často vykonávají třetí strany, se kterým nemají žádné vztahy.

Příkladem společnosti třetích stran jsou Omniture, DoubleClick, AdBrite – tyto weby mohou spojit online aktivitu napříč webem s offline daty, vytvořit detailní profily a nabízet reklamy založené na chování uživatelů. Se stoupající měrou užívání internetu

pro zdraví, finance a jiné služby, se reklamním společností dostávají k dispozici velmi osobní údaje.

Dalším důvodem ke zvýšeným obavám před behaviorálním sledováním je hrozba nepřiměřeného sběru dat vládou, která často dostává privátní informace o občanech od soukromých společností. Omezením komerčního sledování našich online aktivit rovněž může pomoci k ochraně před touto hrozbou.

V první kapitole této práce autor vymezuje téma a vysvětluje základní pojmy týkající se personalizace a ochrany osobních údajů, vyjmenovává technologické způsoby pro sběr osobních údajů a online sledování.

V kapitole druhé se autor snaží zachytit stav ekonomického systému společností působících na webu, jejich služby a metody generování a objemy zisku.

Ve třetí a čtvrté kapitole autor popisuje jak přístupy neodpovědného nakládání s osobními údaji, tak i typické způsoby zneužívání osobních údajů. Autor definuje různé druhy webů, hodnotí je a vymezuje hrozby a dopady na uživatele.

Kapitola pátá se zabývá technickou a právní ochranou osobních údajů, porovnáním situace v České republice, v Ruské federaci a ve Spojených státech amerických. Taktéž jsou v páté kapitole zmíněné navrhované změny v právních úpravách jednotlivých zemí ve vztahu k ochraně osobních údajů.

Poslední kapitola porovnává situaci ve výše uvedených zemích, jejich vyhodnocení a doporučení pro zlepšení situace v ČR. Uživatelská touha ke kontrole sledovacích dat (a jiných dat třetích stran uložených na počítačích uživatelů) způsobila vytvoření řady doplňků pro prohlížeče a další řady nástrojů pro kontrolu soukromí. Tyto metody a nástroje jsou vyjmenované formou doporučení pro jednotlivce.

1 Vymezení tématu a základní pojmy týkající se osobních údajů a personalizace

Autor této diplomové práce si dovoluje definovat větu, která se snaží o zachycení (ne)rovnovážného stavu, neboli podstatného konfliktu mezi uživatelem a společnostmi, poskytujícími reklamu – existuje byznys model, kde z jedné strany je přání zákazníka zachovat rozumnou míru soukromí a přání inzerentů maximálně snížit, nebo úplně odstranit parametr soukromí pro stoprocentně přesné cílení reklamy. Následně si autor pokládá dotaz, co vedlo k současné situaci.

Velká část vedoucích IT technologických společností vznikla na základě poskytování bezplatného servisu pro uživatele a jejich primárním cílem bylo zdokonalit nabízený software, nabízené služby. Následně se tyto společnosti některou jejich devizou dostaly do reklamní branže a tím se jejich primární cíl změnil na neustálé sledování zákazníků všude, kde se pohybují na webu a zaznamenávání toho, co přesně dělají. Jasně příklady ukazují na to, že nejprve se mění politika a filosofie společnosti, až následně se mění technologie. Co může v nastalé situaci uživatel dělat? Je zřejmé, že nikdo se nevzdá technologii, které usnadňují každodenní rutinní činnosti, poskytují velmi jednoduché, rychlé a bezplatné komunikace s přáteli a kolegy, stejně tak jako zábavy na dosah ruky. Nikdo nepřestane nakupovat online, chodit na web nebo prohlížet internetové stránky. Uživatel musí nejprve vědět o současné situaci, o tom, co se děje s jeho osobními údaji. Je velká pravděpodobnost toho, že určitá část uživatelů své chování na sociálních sítích nezmění, stejně tak jak nezmění nastavení soukromí v prohlížeči, nebude tomu tak ale u většiny. Nicméně problém zůstává stejný – uživatelé musí vědět o realitě nakládání s jejich osobními údaji, musí mít k dispozici nástroje (nejlépe zabudované do prohlížeče) pro nastavení potřebné úrovně ochrany soukromí, nastavení množství sdílených o sobě dat online a případné eliminaci sledování chování.

V následující části autor rád představí nejvíce využívané metody pro sledování chování uživatelů online. Tou první a nejvíce populární jsou cookies.

1.1 Cookies

Cookies jsou stále problémem pro soukromí webových uživatelů, mnoho roků po té, co obráncové soukromí vyvolali první vlnu znepokojení o jejich použití pro sledování osob při brouzdání na webu. Základním typem cookies je HTML cookie. Existují ale další druhy, které jsou modernější, a jejich funkcionalita pokročila dál, než u jejich předchůdce.

Široký pohled na soubor technologických možností, kterými cookies dnes útočí na naše soukromí, poskytuje práce *Cleaning Up After Cookies*², kterou opublikovala Katherine McKinley v roce 2008 ve společnosti iSEC Partners. McKinley popisuje pět sledovacích metod typu cookies, které naprosto přesahují možnosti tradiční HTTP cookies.

1.2 HTML cookies

V současnosti, praxe instalování cookies je jedním z hlavních mechanismů, které používají reklamní společnosti jako Google a Facebook pro sledování a vytváření profilů uživatelů na webových stránkách. Často v průběhu času budují jediný velmi obsáhlý profil. Mnozí pokročilí uživatelé internetu reagují na tuto hrozbu použitím nástrojů pro správu cookies zabudovaných v prohlížeči pro omezení počtu cookies, které přijímají nebo pro omezení doby jejich úschovy. Avšak se ukazuje to, že situace s cookies je v současnosti docela složitější, a stránky, které chtějí sledovat uživatele, mají nové technické možnosti, které jsou příliš průbojné pro to, aby jim uživatele mohli vzdorovat. Tradiční "cookie" je HTTP cookie, vynalezená Lou Montulli a Johnem Giannandream v Netscape v roce 1994, dnes ale mnoho prohlížečů implementují řadu technologií, podobných těm cookies se sledovacím chováním, které jsou narozdíl od HTTP cookies snadno přehlédnutelné a velmi špatně kontrolovatelné.

Samy o sobě cookies nenesou žádnou hrozbu. Jsou to malé textové soubory informací, které se dají uložit na počítači klienta. Ukládat a číst cookies umějí skripty klientské (JavaScript) i serverové (PHP). Každý cookies soubor má název a hodnotu, informaci o vypršení (datum a čas ve formátu GMT) a rozsah platnosti (odkud se obsah cookie může načíst). Z bezpečnostních důvodů je ukládání všech souborů na straně uživatele zakázáno, cookies jsou jedinou výjimkou. Cookies se ukládají do dočasných souborů. Samotný uživatel se může na ně podívat přes možnosti prohlížeče, taktéž uživatel může cookies promazávat nebo úplně vypnout (což znamená zákaz ukládání).

Server je schopný během sčítání informace z obsahu cookies vykonávat určité kroky. Například při přihlašování na určitém webu, který vyžaduje autorizaci, v souboru cookies se uloží přihlašovací jméno a heslo, což zbaví uživatele nutnosti znovuznání výše zmíněných údajů při opětovném načítání. Stejný princip práce s cookies se hojně

² MCKINLEY, Katherine. *Cleaning Up After Cookies: Version 1.0*. [online]. 2008, s. 12 [cit. 2012-11-07]. Dostupné z: https://www.isecpartners.com/media/11976/iSEC_Cleaning_Up_After_Cookies.pdf

využívá i v oblasti elektronických obchodů, kdy se při vytváření objednávky dočasná informace o obsahu košíku ukládá do souboru cookies.

V prostorách internetu již dlouho existují weby, které uživatel může nastavit dle vlastních potřeb a chutí, například změnit pořadí zobrazování informací, nastavit barevnou sadu. Znovu se pro tuto personalizaci používají soubory cookies.

Poslední v tomto výčtu, ale první v hojnosti využití, je používání cookies v reklamní branži na internetu, hlavně pro cílenou reklamu – definování cílové skupiny dle zeměpisné polohy, sledování zájmů uživatelů, vyhodnocení počtu zobrazení informace a jiné.

V případě, že by cookie snažil nastavit jiný objekt stránky, který se do obsahu stránky načítá z jiné domény, jde o tak zvanou cookie třetí strany (third part cookie)³.

1.2.1 Cookies třetích stran

Cookies jsou zpětně odesílané pouze internetovým stránkám, které je nastavily nebo serverům ve stejné internetové doméně. Nicméně, webová stránka může obsahovat obrázky, odkazy, webové štenice, HTML IFrame, javascript, nebo jiné moduly uložené na serverech v jiných doménách. Cookies, které jsou staženy a následně uloženy během stahování těchto součástí na počítač uživatele, jsou nazývané cookies třetích stran. V případě, že uživatel navštíví webovou stránku www.aaa.cz, která obsahuje obrázek přicházející z jiné domény, například z www.reklama.cz, server stránky www.reklama.cz posílá prohlížeči uživatele cookie obsahující malý kus dat, číslo indikující unikátního uživatele v jejich systému, a ukládá informaci, o stránce ze které uživatel přichází. Následně, když uživatel navštíví server www.bbb.cz, který také obsahuje reklamní bannery z www.reklama.cz, cookie uživatele je odesláno serveru www.reklama.cz, a neomylně dává vědět výše zmíněnému serveru to, že si uživatel prohlíží stránku www.bbb.cz, následně že tentýž uživatel před určitou dobou navštívil stránku www.aaa.cz.

Některé internetové stránky, například patřící reklamním společnostem, používají cookies třetí strany pro sledování uživatele na více webech. Reklamní společnosti mohou sledovat uživatele napříč všemi weby kde má umístěné bannery nebo reklamy.

³ JANOVSKEÝ, Dušan. Cookies. *Cookies* [online]. [cit. 2012-11-07]. ISSN 1801-0458. Dostupné z: <http://www.jakpsatweb.cz/enc/cookies.html>

Znalost uživatelem navštívených stránek dovoluje reklamním společnostem zacílit reklamu do předpokládaných preferencí uživatele.

Výše zmíněným činností se říká profilování – vytváření profilů je potenciální hrozbou pro soukromí uživatelů i v rámci jednoho webu, jedné domény, nemluvě o tom, když se profil vytváří z údajů procházení více stránek.

1.2.2 Flash cookies

Tento typ cookies existuje na 98 %⁴ všech počítačů, napříč všemi operačními systémy. Adobe Flash Player, který je začleněn do webových stránek, spravuje cookies nazývané LSO⁵, které uchovávají až 100 KB informací a doba expirace těchto cookies dle výchozího nastavení je nekonečná. Tyto soubory cookie jsou uloženy vně prohlížečové kontroly. Internetové prohlížeče neposkytují možnost uživateli prohlížet či mazat cookies uložené Flash aplikací, uživatelé nejsou informováni o tom, že takové cookies jsou instalovány, a tyto cookies nikdy nepozbudou platnosti. Flash cookies sledují uživatele stejným způsobem, jako standardní HTTP cookies. Ve skutečnosti, všechny informace v těchto cookies zůstanou po dobu neurčitou, dokud nebudou odstraněny vydávající internetovou stránkou, nebo uživatelem, který bude muset podstoupit zdoluhavému a nejasnému procesu.

Studie⁶ tvrdí, že více než 50 % webů používá Flash Cookies k ukládání informací o uživateli. Některé je používají i pro obnovení klasických HTTP cookies smazaných uživateli. Často se děje totiž to, že Flash Cookies obsahují totéž, co HTTP cookies. Používány jsou i vládními weby. Pravidla na ochranu soukromí jen výjimečně upozorňují na používání Flash cookies. Zatímco řada uživatelů ví jak a kde smazat klasické cookies, u Flash cookies je to problém – LSO se v podstatě vůbec nezabývá ochranu soukromí a jsou využívány velmi skrytě.

Není žádný snadný způsob detekce, kdy internetové stránky používají Flash cookies pro sledování pohybu uživatele. Neexistuje žádný seznam, nemusí na stránce být flash GUI

⁴ ADOBE. *Adobe Flash runtimes: statistics* [online]. [cit. 2012-11-07]. Dostupné z: <http://www.adobe.com/products/flashruntimes/statistics.html>

⁵ Adobe pojmenovává Flash cookies jako Local Shared Objects. Kromě Flash cookies existují další technologie s velmi podobným chováním - HTML 5 DOM storage, Microsoft Silverlight cookies, Microsoft Internet Explorer User Data Persistence a Google Gears data

⁶ MCKINLEY, Katherine. *Cleaning Up After Cookies: Version 1.0*. [online]. 2008, s. 12 [cit. 2012-11-07]. Dostupné z: https://www.isecpartners.com/media/11976/iSEC_Cleaning_Up_After_Cookies.pdf

nebo viditelná aplikace pro to, aby se na počítač uživatele uložily flash cookies. Ve skutečnosti, většina stránek využívajících Flash pro sledování pohybu uživatelů nevytváří GUI, panely toolbars nebo aplikace, které jsou na stránce viditelné.

Většinou je tomu tak, že malý flash modul, o velikosti 2 KB nebo méně je stažen do vašeho prohlížeče na každé navštívené stránce stejným způsobem jak se stahují gif, jpg nebo jiné obrázky. Smysl existence tohoto malého, neviditelného modulu je zaznamenávání odeslaných požadavků stránky, přihlašovacího jména uživatele nebo jakékoliv jiné hodnoty relace.

V průzkumu ⁷ se zjistilo, že Flash cookie jsou hojně užívané populárními internetovými stránkami, a většina uživatelů pravděpodobně o nich neví nebo neví jak je vymazat. Zpracovatelé průzkumu rovněž zjistili, že alespoň jedna významnější stránka užívá je způsobem, který porušuje vlastní pravidla reklamního průmyslu o sledování uživatelů.

Navíc, výzkumníci z univerzity Berkeley zjistili, že Flash cookies jsou často užívané pro vědomé narušování politiky nastavení HTTP cookies uživatelů. Konkrétněji se jedná o to, že internetová stránka může úmyslně skladovat stejnou *informaci* najednou v obou cookies - HTTP a Flash cookies souborech. Když uživatel maže HTTP cookies, stránka je může "obnovit" z kopie, která bylo uložena ve formátu Flash cookie. Je zřejmé to, že správci stránek tímto způsobem obcházejí přání mnoha uživatelů nebýt sledován pomocí cookies, ale našli způsob jak obejít nastavení soukromí uživatelů.

Tato útočící na soukromí marketingová praxe potřebuje větší zkoumání. Pro větší přehled v nastalé situaci jsou zapotřebí další výzkumy, aby bylo jisté, jestli další druhy cookies (HTML 5 DOM storage, Microsoft Silverlight cookies, Microsoft Internet Explorer User Data Persistence a Google Gears data) využívají stejné praktiky, jako ty s Flash cookies. Není vyloučeno, že Flash cookies jsou pouze špičkou ledovce další generace sledovacích technologií.

Mezitím, vývojáři prohlížečů by měli dělat více pro to, aby uživatelé věděli, rozuměli a kontrolovali způsoby, jakým jsou sledovány pomocí každé z těchto technik. Bohužel, co se týče Flash cookies, Adobe udělalo výše zmíněné extrémně obtížným tím, že jsou ukládány mimo kontrolu prohlížeče, a vzhledem k tomu, že oficiální Flash plug-in není Open Source, uživatelé nemohou jej snadno upravit dle své potřeby. Existující plug-in

⁷ SOLTANI, Ashkan, Shannon CANTY, Quentin MAYO, Lauren THOMAS a Chris Jay HOOFNAGLE. Flash Cookies and Privacy. [online]. 2009 [cit. 2012-11-07]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

BetterPrivacy ve Firefox se pokouší zabránit vytváření Flash cookies jejich vyhledáváním na pevném disku a pravidelným mazáním, ale Adobe mohl tuto situaci výrazně zjednodušit synchronizací jejich nastavení s nastavením soukromí v prohlížeči ⁸.

Představme si situaci, kdy uživatel načítá webovou stránku s jedním Flash elementem. Následně si uživatel může přát tu samou stránku prohlížet anonymně v prohlížeči jiném. Použitím univerzálního data skladu, Flash poskytuje vývojářům jedinou metodu pro sběr dat napříč všemi prohlížeči, které může uživatel používat. Toto je problém, protože v režimu anonymního prohlížení jsou data z Flash cookies stále dostupná a modul na stránce stále má přístup ke stejným Flash datům, jako primární prohlížeč. Průzkum objektů nacházejících se v lokální paměti Flash na počítači uživatele našel soubor hodnot, díky kterému lze jednoduše identifikovat následující informace: uživatelské jméno, přezdívka, identifikační čísla nebo otisky či kódy relace bankovní multifaktorové autentizace (například the Bank of America, Hampden Bank a Security Bank Corporation) ⁹.

Dle výchozího nastavení Flash videa nemají přístup ke kameře nebo mikrofону, pokud uživatel nedá vyslovené povolení. Nicméně publikovaný společnosti Adobe článek týkající se soukromí pro Flash aplikace a moduly nehovoří jasně, zda toto povolení platí pouze pro filmy načítané ze stejné domény, které uživatel dával povolení, nebo jestli toto povolení platí pro širší okruh stránek, jak je tomu v případě načítání videí souborem crossdomain.xml ¹⁰. Na daných stránkách uživatel může pravým tlačítkem myši upravit nastavení. Nicméně v tomto nastavení uživatel může upravovat hodnoty pouze pro danou doménu, globální nastavení a přehled povolení uživatel získá pouze v modulu Settings Manager na stránkách Adobe, dostupném online.

⁸ Adobe aktuálně poskytuje rozhraní pro správu Flash cookies, ale většina uživatelů o tom vůbec netuší, toto rozhraní není integrováno do cookie politiky prohlížeče, zabývá se hlavně nastavováním povoleného prostoru pro ukládání cookies, než samotnými otázkami soukromí. Rozhraní rovněž neposkytuje takovou škálu možností, jakou poskytují plug-iny prohlížečů, vyvinuté třetími stranami

⁹ MCVEY, Kathleen. Arcot Systems to Protect Online Identities at Top Philippines Bank. [online]. 2008 [cit. 2012-12-07]. Dostupné z: <http://www.reuters.com/article/2008/03/10/idUS121553+10-Mar-2008+MW20080310>

¹⁰ Pro další informace ke crossdomain.xml viz STAMOS, Alex. Vulnerabilities 2.0 in Web 2.0: Next Generation Web Apps from a Hacker's Perspective. [online]. roč. 2007 [cit. 2012-12-07]. Dostupné z: <https://www.isecpartners.com/media/12946/Attacking-AJAX-Applications-Web20-Expo.pdf>

1.2.3 Ostatní cookies

Vedle shora uvedených klasických HTML a Flash cookies existují následující technologie s velmi podobným chováním - HTML 5 DOM storage, Microsoft Silverlight cookies, Microsoft Internet Explorer User Data Persistence a Google Gears data.

Technické podrobnosti a způsoby sběru informací se autor rozhodl v této práci nepopisovat z toho důvodu, že tyto technologie jsou velmi podobné těm HTML a Flash cookies, o kterých se mluvilo dříve v této kapitole, a můžou se lišit pouze povoleným objemem ukládaných dat, povolené „životnosti“, funkčnosti nebo podporovanými aplikacemi. Stejně vlastnosti jsou následující – nové druhy cookies jsou modernější, propracovanější a hlavním způsobem sbírají, uchovávají a poskytují data uživatelů pro potřeby reklamních společností třetích stran.

1.3 Alternativa cookies

Některé operace, pro účely kterých se používají cookies, můžou je realizovány pomocí jiných nástrojů. Tyto alternativy mají i své nedostatky, kvůli kterým vývojáři dávají v praxi přednost cookies. Většina těchto alternativ umožňuje sledovat chování uživatele, i když méně spolehlivým způsobem, nežli cookies. Jako výsledek, nedotknutelnost soukromí je ohrožená, dokonce i tehdy když cookies jsou úplně vypnuté v prohlížeči nebo se nenastavují serverem.

Údaje prohlížeče

Běžný uživatel internetu má k dispozici omezené množství nabízených internetových prohlížečů. Každý z nich je vyvíjen jinou společností, které mají různé obchodní modely a metody generování zisku, následkem čehož jsou různé úrovně ochrany soukromí uživatele.

Autor této diplomové práce používá prohlížeč Mozilla Firefox a níže uvádí výsledek vyhodnocení unikátnosti prohlížeče na stránkách Panopticlick¹¹. Testovaný prohlížeč je dle poskytnutých údajů unikátním mezi dalšími 2,5 milióny testovaných jednotek.

Metody testování se zakládají na složitých algoritmech, ale obecná rovina logiky je velmi jednoduchá. Stránka Panopticlick porovnává sdílené prohlížečem data dle různých kategorií – typ a verze prohlížeče, akceptované záhlaví stránek, podrobnosti o

¹¹ Panopticlick [online] [cit. 2012-05-29]. Dostupné z: panopticlick.eff.org

plug-inech prohlížeče, časové pásmo, velikost obrazovky, dostupná písma systému, aktivovaná cookies a supercookies.

Seznam plug-inů prohlížeče a seznam dostupných fontů v počítači autora jsou nezávisle na sobě dostačující pro stoprocentně přesnou identifikaci – každý z nich byl naprosto unikátní v seznamu dříve testovaných 2,5 milionů zařízení.

IP adresa

Tato metoda sledování uživatelů spočívá v uchovávání IP-adres počítačů, prohlízejících stránky. Daná technika existuje od samotného vzniku World Wide Web, která požaduje znalosti IP-adresy zákazníka pro nahrání internetové stránky. Tuto informaci lze uchovávat na serveru vně závislosti od toho, jestli se cookies používají nebo ne.

Nicméně tento způsob je méně spolehlivý, než cookies, jelikož počítače a proxy mohou být používány několika uživateli, a jeden počítač může používat různé IP-adresy v různých relacích.

Sledování dle IP-adres se může stát nemožným při použití programů ochrany anonymity (například Tor). V takových systémech jeden prohlížeč může mít několik IP-adres, a několik uživatelů můžou využívat jednu IP-adresu, v důsledku čeho sledování IP-adresy není účinné.

Některé velké poskytovatelé internetu, včetně AOL, propouští celý web traffic přes síť proxy, což rovněž dělá dotyčnou metodu neúčinnou.

Webové štěnice

Pixely, známé jako „webové štěnice“ (web bug), jsou obsažené na webech nebo v některých e-mailech a umožňují shromažďování informací o návštěvnících webů nebo o příjemcích e-mailů, o jejichž existenci nemá většina uživatelů Internetu dosud ani tušení. Webové štěnice teoreticky představují malé riziko, ale ve spojení s jinými technikami mohou ohrozit soukromí. Tyto webové štěnice uživatel nemá šanci poznat zaprvé kvůli jejich samotné velikosti, zadruhé kvůli tomu, že jejich barva je většinou stejná jako barva pozadí.

Když se návštěvník připojí k webu, obsahujícímu webové štěnice, poslední mohou zaznamenat takové informace jako IP adresu návštěvníka, druh používaného webového prohlížeče, dříve navštívené webové servery apod. Až potud se nejedná o žádné velké riziko, protože tyto informace zůstávají anonymní, ale ve spojení se souborem cookie, který sbírá jiné druhy informací, umožňují webové štěnice sestavovat úplné profily uživatelů Internetu bez jejich vědomí. Největší obavy se nepochybně objevují při jejich

použití v e-mailech (například v bulletinech nebo marketingových materiálech): webové stránice umožňují jejich odesílateli kontrolovat, zda je adresa uživatele Internetu platná, nebo zjistit jeho zvyky, pokud jde o čtení e-mailů.

URL (formulářová data)

O něco progresivnější metoda je založena na aplikaci dat do URL. Většinou se používá prostor v pro formulářová data (parametry, nachází se za znakem „?“), ani není výjimkou využití jiných prostor. Programovací jazyky Java a PHP tuto metodu aktivně využívají při vypnutých cookies.

Webový server doplňuje parametry k URL stránky v momentě jejího odesílání do prohlížeče. Když uživatel pokračuje na uvedené URL, prohlížeč vrací parametry dotazu serveru.

Z tohoto pohledu formulářová data URL a cookies jsou velmi podobné - jsou to dílčí fragmenty informací serveru, které jsou odesílány zpátky prohlížečem. Existují ale i následující rozdíly - jelikož jsou formulářová data součástí URL, tak při opakovaném využití stejného URL – serveru odesílají se stejná data. Například, když nastavení uživatele jsou zakódované v parametrech formulářových dat a uživatel toto URL odešle jinému uživateli, tyto nastavení budou platit i pro jiného uživatele.

Navíc, nejsou žádné záruky toho, že při opakovaném navštěvování stejné stránky parametry zůstanou stejné. Například při přechodu na jednu a tu samou stránku z jiné vnitřní stránky webu a z vnějších vyhledávačů parametry formulářových dat budou jiné, kdežto by cookies zůstaly stejné.

Jiný nedostatek formulářových dat URL se projevuje v otázkách bezpečnosti – ukládání identifikátoru relace v URL zjednodušuje podmínky pro uskutečnění útoku. Předávání identifikátoru „osobně“ je méně nebezpečná.

Skrytá pole formuláře

Jedním ze způsobů sledování relace pomocí běžící na samotném serveru programu je použití web formulářů se skrytými poli. Tato metoda je velmi podobná té s formulářovými daty v URL a má skoro stejné silné a slabé stránky. Taktéž, když parametry formuláře jsou odesílány HTML cestou GET, pak se pole fakticky stane součástí URL, kterou prohlížeč odešle na server. Nehledě na to většina formulářů se zpracovává pomocí metody http POST, během které posílaná informace není součástí URL ani cookies.

Tento přístup má následující dopady na sledování uživatele – zaprvé, zapouzdření informace do HTML kódu a POST, nikoli do URL, znamená, že uživatel si jí vůbec nevšimne, zadruhé, se informace o relaci nekopíruje spolu s URL (když se například odkaz posílá emailem). Slabá stránka této metody je v tom, že informace o relaci se nachází přímo v HTML kódu, proto se stránka musí generovat pokaždé, když jí volají, což zvyšuje zatížení serveru.

HTTP-autentizace

Protokol http zahrnuje do sebe základní autentizaci a šifrování, které povolují přístup na stránku, pouze tehdy, když uživatel uvede správné uživatelské jméno a heslo. Pokud server požádá přihlašovací údaje, pak prohlížeč dotazuje uživatele na potřebné údaje a po jejich obdržení a kontrole ukládá, aby je uživatel pro přístup k jiným stránkám na doméně nemusel pokaždé zadávat. S pohledu uživatele je účinek naprosto stejný jako při použití cookies – přihlašovací jméno a heslo se vyžadují jen jednou, poté uživatel získává přístup k celému webu. Při základní typu autentizace se přihlašovací jméno a heslo odesílá na každý požadavek prohlížeče nešifrované. To znamená, že přihlašovací údaje mohou být zlomyslníkem odcizené. Během šifrované relace přihlašovací jméno a heslo se odesílají šifrované náhodným klíčem vygenerovaným serverem.

Ukládání dat na straně klienta

Některé prohlížeči umožňují ukládání dat lokálně na počítači uživatele pro následující zpětné vyvolání. Například Internet Explorer podporuje ukládání dat v historii, vybraném XML skladišti nebo umožňuje přímé uložení celé stránky na pevný disk ¹².

O něco jiný mechanismus se využívá v prohlížečích, které cashují soubory javascript, využívané na stránce. Například stránka může obsahovat odkaz `<script type="text/javascript" src="example.js">`. Během načítání stránky se stahuje i example.js. Následně se skript dostává do cache a nevyžaduje opakované stažení při nové návštěvě stránky. Ve výsledku, pokud skript obsahuje takový parametr jako `id=324546`, pak tento identifikátor platí i pro jiný požadavek z jiné stránky, dotazující skript example.js.

¹² Introduction to Persistence: Cookies. [online]. roč. 2011 [cit. 2012-12-07]. Dostupné z: <http://msdn.microsoft.com/en-us/library/ms533007%28VS.85%29.aspx>

1.4 Personalizace

Na pojem personalizace se můžeme dívat ze dvou mezi sebou provázaných pohledů.

První je trend ve vývoji webových stránek, kdy personalizace vyjadřuje možnost přizpůsobit webovou stránku svým potřebám. V některých případech může jít například o výběr z různých předpřipravených grafických podob prezentace až po komplexní úpravu stránky pomocí přidání prvků a funkcí podle potřeb uživatele ¹³. Různé internetové zdroje se shodují na tom, že se pod pojmem personalizace rozumí zobrazování aktuálních informací podle zadaných hodnot (zobrazování počasí podle regionu atd.). Dalším krokem v možnostech personalizace je manipulace s obsahem stránek samotných. Tím se rozumí buď možnost skrýt určité informace, nebo naopak přidávat informace z jiných zdrojů. Z toho můžeme vyvodit, že personalizace je jakási přidaná hodnota, kterou uživatel si sám vytvoří pomocí jemu nabízených nástrojů.

Pohledem druhým, který je zmiňován pouze v poslední době a to zdaleka ne tak často, je personalizace neviditelná – ta, o které uživatel netuší. Tady autor má na mysli dvě podoby – filtrování výsledků vyhledávání a reklamy na webu, které jsou určeny pro konkrétního uživatele.

Personalizaci ve vyhledávání se plně věnuje Eli Pariser, autor knihy „The Filter Bubble“, kde hlavně hovoří o společnosti Google a 57 signálech, které jsou s naprostou jistotou schopné velmi efektivní identifikace každého uživatele, ať se jedná o registrovaného nebo neregistrovaného zákazníka služeb Google. Bublině filtrů autor věnuje samostatnou podkapitolu.

Reklamy na webu a personalizace jsou zároveň s pojmem cílené reklamy. Autor si dovoluje tvrdit, že personalizace v tomto ohledu je spíše směr vývoje, jakýsi trend, jedním projevem kterého je cílená reklama. Tady je třeba mít na paměti myšlenkový řetěz pojmů Online sledování – Profilování – Behaviorální cílení reklamy. Pojem Online sledování se objevuje skrze celou práci. Další dva pojmy profilování a behaviorální cílení reklamy jsou podrobně popsány v následujících podkapitolách.

1.5 Profilování

Existují dva hlavní postupy pro vytváření profilů uživatelů: i) **prediktivní profily** jsou vytvářeny dedukcí na základě dlouhodobého pozorování chování jednotlivých uživatelů

¹³ Adaptic [online]. [cit. 2012-11-08]. Personalizace. Dostupné z WWW: <http://www.adaptic.cz/znalosti/slovnicek/personalizace/>.

a kolektivního chování, zejména sledováním navštívených stránek a inzerátů, které byly prohlédnuty nebo na které bylo kliknuto, ii) **jmenovité profily** jsou vytvářeny z osobních údajů, které samotné subjekty údajů poskytují internetové službě (například při registraci). Oba přístupy lze spojit. Prediktivní profily mohou být navíc později změněny na jmenovité, když subjekt údajů vytvoří osobní údaje pro přihlášení na internetové stránky ¹⁴.

Profilování se odkazuje na celý proces budování a aplikaci profilů vygenerovaných počítačovými profilovacími technologiemi. Co charakterizuje profilovací technologie je použití algoritmů nebo jiných matematických technik, které poskytují možnost objevení vzorů či korelací ve velkých množstvích dat, shromážděných v databázích. O profilování se konkrétně jedná, když tyto vzory či korelace jsou užívané pro identifikaci nebo reprezentaci lidí.

Jeden z nejvíce náročných problémů informační společnosti je rostoucí přetížení daty. S digitalizací všech druhů obsahů stejně tak, jako zlepšením a poklesem ceny zaznamenávajících technologií, množství dostupných informací se stalo enormním a exponenciálně se zvětšuje. Tím pádem se stalo velmi důležitým pro společnost, vlády, a jedince rozlišování informací od informačního hluku, odhalování těch užitečných dat které jsou zajímavá. Vývoj profilovacích technologií musí být viděný na základě těchto skutečností. Tyto technologie existují pro efektivní sběr a analýzu dat a následně pro nalezení nebo testování znalosti ve formě statistických vzorů mezi daty. Tento proces je nazývaný Knowledge Discovery in Databases (KDD, neboli Data Mining), který poskytuje pomocí profilovacího programu, na základě žádosti, soubory souvztažných dat nazývaných (a následně používaných) "profily".

Z technické stránky může být profilování rozděleno do několika kroků:

- Předběžná příprava: Profilovací proces začíná se specifikací použitelného okruhu působnosti a identifikací cílů analýzy
- Sběr dat: Cílový soubor dat nebo databáze pro analýzu je vytvořen výběrem relevantních dat s ohledem na existující znalost okruhu působnosti a porozumění datům
- Příprava dat: Data jsou předzpracována pro odstranění hluku a snižování složitosti eliminací atributů

¹⁴ Stanovisko 2/2010 k internetové reklamě zaměřené na chování. [online]. 22. června 2010 [cit. 2012-12-08]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf

- Dolování dat: Data jsou analyzovaná pomocí algoritmu nebo heuristicky vyvinuta v souladu s daty, modelem a cílem
- Interpretace: Získané vzory jsou ohodnocené na základě jejich relevance a platnosti odborníky a/nebo profesionály v aplikačním okruhu působnosti
- Aplikace: Vybudované profily jsou aplikované, například na kategorie osob, za účelem testování a dolazování algoritmů
- Instituční rozhodnutí: Odpovědné osoby následně rozhodují o tom, jaké činnosti nebo jakou politiku aplikovat na skupiny nebo jedince, jejichž data se shodují s relevantním profilem

Shromažďování údajů, příprava a dolování - to všechno patří do fáze, ve které je profil ve výstavbě. Ať tak nebo onak, profilování odkazuje na použití profilů, což znamená používání profilů pro identifikaci či kategorizaci skupin nebo individuálních osob. Jak můžeme vidět v šestém korku (aplikaci), proces je opakující se. Existuje zpětnovazební smyčka mezi stavbou a použitím profilů. Výklad obsahu profilů může vést k opakování – pravděpodobně i doladování určitých předchozích kroků v profilovacím procesu v reálném čase. Proces profilování je jak dynamický tak i adaptivní.

Profilovací technologie vyvolaly spoustu etických, právních a jiných obav týkajících se soukromí, rovnoprávnosti v souladu se zabezpečením a důvěryhodnosti profilovacích technologií. Početné orgány a jednotlivci varovali před dostupností nové technologické infrastruktury, která může vyplynout na základě polo-autonomních profilovacích technologií. Soukromí je jedním z hlavních vytýčených problémů. Profilovací technologie umožňují dalekosáhlé monitorování individuálního chování a preferencí. Profily mohou odhalit osobní či citlivé informace o jednotlivcích, které samotné jednotlivce si nemusí ani uvědomovat.

Profilovací technologie jsou od jejich základů velmi diskriminační nástroje. Dovolují totiž bezpříkladné druhy sociálního třídění a segmentace, které mohou mít škodlivé účinky. Existuje velká pravděpodobnost toho, že lidé spadající do určitého profilu mohou platit vyšší ceny, přicházet o důležité nabídky či příležitosti a taktéž mohou podléhat vyšším rizikům, jelikož uspokojování jejich potřeb je méně výnosné. Ve většině případů si tyto dotčené osoby ani nebudou uvědomovat shora zmíněné skutečnosti z důvodu neviditelnosti profilovací činnosti a samotné profily jsou často chráněné duševním vlastnictvím nebo obchodním tajemstvím. Vše shora napsané

představuje hrozbu pro rovnost a solidaritu občanů. Ve větším poměru, profilování může způsobit segmentaci společnosti.

Jedna z problematik ležících v základě potenciálních porušení soukromí a nediskriminace je to, že proces profilování je nejčastěji neviditelný pro ty, kteří jsou profilováni. Toto vytváří potíže nebo dělá naprosto nemožnou obranu proti profilování a ruší principy očekávaného procesu: jestliže osoba nemá přístup k informacím, na základě kterých přichází o výhody nebo podstupuje rizikům, pak nemá naprosto žádné možnosti bránit se takovému způsobu zacházení.

Profily mohou být použité proti profilovaným osobám, když skončí v nepovolaných rukou. Důležitý problém příbuzný tomu s ochranou soukromí je krádež identity. Když aplikace profilů způsobuje škodu, pak se musí stanovit osoba, která bude za vzniklou škodu odpovídat. Bude to programátor, poskytovatel servisu profilování nebo držitel výsledných profilů? Tato záležitost je o to komplexnější v případě, kdy se aplikace a rozhodování o profilech provádí automatizovaně, jak je tomu v případě Autonomního Computingu nebo Ambientní Inteligence založených na automatizovaných rozhodnutích vyhodnocovaných profilů.

Jeden z hlavních zdrojů informací užívaných pro profilování je sledování na webu, myšleno sledování uživatelů při prohlížení stránek na jedné doméně nebo na doménách různých. Shromážděná data zahrnují sekvenci navštívených webů a spatřených jednotlivých stránek na jednom webu, čas utracený na každém webu. Ať tak nebo onak, sledování zvyků a preferencí (tracking) je nedovolené v případě, že data obsahují jakoukoliv osobně identifikovatelnou informaci, jako jméno, adresu, telefonní číslo a tak dále. Webové sledování je převážně prováděno monitorováním IP adres, a používání takových technik jako cookies, anebo modernější supercookies ¹⁵.

1.6 Behaviorální marketing

Internetová reklama je klíčovým zdrojem příjmu pro mnoho internetových služeb a je důležitým faktorem při růstu a šíření internetové ekonomiky. Specifické postupy při používání reklamy zaměřené na chování však vyvolávají významné obavy týkající se ochrany údajů a soukromí. Základní internetová technologie umožňuje poskytovatelům sítí za účelem reklamy dlouhodobě sledovat subjekty údajů na různých internetových

¹⁵ MCKINLEY, Katherine. Cleaning Up After Cookies: Version 1.0. [online]. 2008, s. 12 [cit. 2012-11-07]. Dostupné z: https://www.isecpartners.com/media/11976/iSEC_Cleaning_Up_After_Cookies.pdf

stránkách.. Reklama zaměřená na chování je založena na sledování uživatelů surfujících po internetu a na postupném vytváření profilů, které jsou později využívány k poskytování reklamy těmto uživatelům, která odpovídá jejich zájmům ¹⁶.

Reklama zaměřená na chování má tyto aktéry: a) *poskytovatele reklamních sítí*, kteří jsou nejdůležitějšími šířiteli reklamy zaměřené na chování, protože spojují vydavatele s inzerenty; b) *inzerenty*, kteří chtějí propagovat výrobek nebo službu konkrétní cílové skupině, a c) *vydavatele*, kteří jsou vlastníky internetových stránek a usilují o příjmy z prodeje prostoru pro zobrazování inzerátů na svých internetových stránkách.. Kromě reklamních sítí by reklama zaměřená na chování mohla být také poskytována prostřednictvím reklamy na internetových stránkách. Pomocí této metody inzerent označí vydavateli svoji zamýšlenou cílovou skupinu na základě kritérií, která mohou jít nad rámec demografických informací, jako je tradiční trojice „věk, pohlaví a země“, a která mohou být daleko přesnější (jako jsou klíčová slova nebo zájmy). Úkolem vydavatele je pak s použitím technologie pro cílení reklamy zobrazit reklamu zvolené cílové skupině. Vydavatel zároveň kontroluje umístění a šíření inzerátů. Tato metoda se používá u některých platform sociálních sítí a umožňuje, aby byli uživatelé vybíráni na základě svých zájmů.

Poskytování inzerátů prostřednictvím reklamních sítí v zásadě funguje takto: vydavatel vyhrazuje vizuální prostor na svých internetových stránkách pro zobrazení inzerátu a přenechává zbytek procesu reklamy jednomu nebo více poskytovatelům reklamních sítí. Poskytovatelé reklamních sítí mají vůči vydavatelům odpovědnost za co možná nejúčinnější šíření inzerátů. Poskytovatelé reklamních sítí ovládají technologii pro cílení reklamy a související databáze. Čím je reklamní síť větší, tím má větší zdroje pro monitorování uživatelů a „sledování“ jejich chování ¹⁷. Inzerent obvykle jedná se zástupci jedné nebo více reklamních sítí a nebude nutně znát totožnost všech vydavatelů (pokud vůbec nějakého), kteří budou jeho inzeráty šířit. Vydavatel může mít současně několik smluv s různými reklamními sítěmi, například na vyhrazení různých míst na internetových stránkách pro různé reklamní sítě.

¹⁶ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf

¹⁷ New York Times, „To Aim Ads, Web is Keeping Closer Eye on You“, 10. března 2008. Článek poskytuje statistiku o frekvenci, se kterou velké reklamní sítě sledují jednotlivé návštěvy na internetových stránkách. V případě reklamní sítě Yahoo! byl průměrný uživatel (z USA) na konci roku 2007 údajně sledován 2 520 krát měsíčně.

2 Specifika vybraných serverů a služeb

2.1 Prohlížeče a politika společnosti

Před vydáním společnosti Microsoft prohlížeče Internet Explorer 8, tým pracující na vývoji se rozhodl implementovat nové funkcionality, které by se zabývaly soukromím uživatelů. Tyto funkcionality měly podporovat management cookies třetích stran pro umožnění uživateli být anonymním pro reklamní společnosti díky blokování odchozí informace ohledně jejich chování online. Následně se ale do situace zapojilo reklamní oddělení Microsoft, stejně tak, jako i externí reklamní společnosti, které samozřejmě nechtějí přicházet o zisk, který jim vynáší sledování a následné profilování uživatelů.

Prvním velkým kamenem úrazu v tomto tématu je to, že velké nadnárodní společnosti poskytující online software a služby zdarma mají do své struktury začleněné i oddělení zabývající se inzercí. Tato situace jasně znázorňuje i případné vnitřní konflikty. Následně, když si představíme ryze hypotetickou situaci, kdy vnitřní spory a dohody ve společnosti Microsoft mohou být vyřešené, pak vydáním nových funkcionalit, zapouzdřených do prohlížeče IE 8, společnost Microsoft může učinit velkou škodu společnosti Google – lídrovi na trhu s cílenou reklamou a sledováním uživatelů internetu, což si samozřejmě nepřejí. Kromě Google na trhu s osobními údaji působí nesčetné množství dalších společností, které Microsoft taktéž nechce poškodit z toho důvodu, že jsou závislé na dopadu jejich produktu, na jakémśi ekosystému fungování větších a menších společností tohoto sektoru, na tom, jak hojně budou produkty společnosti Microsoft využívány a konečně bez podpory menších skupin reklamních společností by Microsoft nemohl vzdorovat konkurenci Google.

Abychom se vrátily k připravovanému v roce 2010 updatu Internet Explorer 8 a shora zmíněné funkcionality pro ochranu soukromí uživatelů, autor musí konstatovat, že finální verze prohlížeče sice uvedené funkcionality obsahuje, ale jsou skoro nepoužitelné – při zavření a znovuotevření prohlížeče se funkcionalita vypíná – musí se pokaždé znovu zapínat, neobsahuje zdaleka tolik možností, co obsahoval pilotní projekt. Ve své podstatě přesto, že tuto funkcionalitu zahrnuly do nové (v roce 2010) verze prohlížeče je skoro nepoužitelná. Výsledkem je to, že největší dopad znovu ucítí uživatel prostoru internetu.

Abychom nezapomněli na ostatní společnosti a jejich prohlížeče, musí autor zmínit nejprve prohlížeč Chrome od společnosti Google. Jelikož společnost Google je daleko

více závislá na příjmech z cílené reklamy, pak to má samozřejmě dopad na to, že vývojáři prohlížeče Chrome nebudou v žádném případě usilovat o zabudování nových funkcionalit pro ochranu soukromí. V tomto ohledu Google a Microsoft se pohybují v naprosto diametrálně rozlišných směrech vývoje.

Apple a jejich prohlížeč Safari je nejagresivnější obránce soukromí uživatelů, například už jenom tím, že dle výchozího nastavení jsou vypnuta všechny cookies třetích stran. To platí nejen pro instalovaný prohlížeč na platformě OS X, ale i pro Windows, iPad a iPhone zařízení. Tato situace, dle názoru autora, nastala ne kvůli tomu, že by společnost Apple pečovala o osobní údaje a soukromí uživatelů, ale kvůli absenci společnosti Apple na trhu s reklamou (i to se v průběhu roku 2011 začalo měnit).

2.2 Google

Společnost Google nabízí širokou škálu služeb na svých serverech Google vyhledávač, Google Plus, Gmail, Google Mapy, Google Earth, Google Zprávy, Google Talk, Google Dokumenty (nyní Google Disk), Google Play, Google Photo, Google Video a Google Kalendář. Dále společnosti Google patří celosvětově známé služby jako YouTube, Picasa a Blogger. Všechny služby jsou zdarma. Ve Spojených státech amerických Google má 70-75% podíl v používaných online vyhledávačích. Ve Spojeném království, Jižní Americe, Belgii nebo Švýcarsku tento podíl stoupa přes hranici 90%¹⁸. Za celou svou historii společnost Google koupila celkem 9 podniků, zabývajících se pouze reklamní činností. Celková hodnota nákupů 7 společností činí \$4,56 mld., cenu posledních dvou koupí společnost skrývá.

Celkové tržby za rok 2011 tvoří částku \$37,9 mld., z toho tržby za reklamu \$36,5 mld., což tvoří 96,3%. Google vyvinul dva velmi ziskové reklamní modely - Google AdWords a Google AdSense.

AdWords

Reklama AdWords se objevuje na stránkách výsledků vyhledávání nad vyhledanými odkazy, pod a z pravé strany a nesou označení „Sponzorované odkazy“. Inzerenti používají AdWords pro vytváření kampaní, účelem kterých je zobrazení krátkého reklamního textu a odkazu na vlastní stránku, dle předem definovaných klíčových slov.

¹⁸ Google's Market Share in Your Country. [online]. 2009 [cit. 2012-12-07]. Dostupné z: <http://googlesystem.blogspot.cz/2009/03/googles-market-share-in-your-country.html>

Google využívá složité algoritmy pro zobrazení relevantních reklam ke konkrétním požadavkům vyhledávání.

Inzerenti neplatí za zobrazování, ale za samotný klik uživatele na inzerovaný odkaz.

Ceny kliku se různí od 10 centů (USD) do stovek dolarů (USD).

AdSense

AdSense funguje na stejném principu jako AdWords. Rozdíl je v tom, že se reklamy zobrazují na stránkách nepatřících společnosti Google. Vývojář webové stránky se může zapojit do AdSense a zobrazovat reklamy Google.

Čtenář této práce si může položit dotaz: „Díky čemu je Google natolik úspěšný v prodeji PPC kampaní?“. Odpověď je v efektivitě, přesněji v cílení reklamy. Díky vytvářeným profilům uživatelů Google zná jejich chování, záliby, osobní a citlivé údaje. Na základě výše zmíněných profilů každý uživatel vidí reklamu šitou na míru.

Google a soukromí

Google má přístup k těm nejtajnějším informacím o uživateli – ukládá historii vyhledávání, využívá software, který prohledává obsah elektronických zpráv a zaznamenává objevená klíčová slova v obsahu zpráv, to samé dělá i s dokumenty na cloudu Google, díky servisu Latitude neustále zná aktuální (a nejen) polohu jednotlivce, zaznamenává historii prohlížených videí na YouTube, pamatuje si odebírané kanály na stejnojmenném serveru, má přístup k našim fotografiím přes desktopovou aplikaci Picasa, má osobní a citlivé údaje z Google+ a Gmail, pamatuje si údaje debetních (nebo kreditních) karet, kterými uživatelé platí přes Google Checkout.

Shora jsou vyjmenovány očividné a nikoho nepřekvapující fakta o společnosti Google. Už o něco méně lidí ví to, že Google vlastní řadu serverů (google-analytics-com, doubleclick.net aj.), které pomocí různých technologií sledují a vytváří profily každého uživatele internetu. Registrace na žádném servisu Google není potřeba.

Spojením anonymních (dle tvrzení Google) údajů o pohybu, chování a nejen uživatele – jeho profilu – s údaji, zaznamenanými na jakémkoliv servisu, tato společnost v mnoha případech ví více, než naše blízké.

Nikdy v historii lidstva žádná společnost neovládala takovým množstvím informací, jak tomu je v případě Google.

Google a vlády

Na svých stránkách Google zveřejnil statistika předávání veškerých dat jednotlivých uživatelů vládám nebo vládním orgánům jednotlivých států ¹⁹.

Rok 2009			
Stát	Počet požadavků na data o uživateli	Procento kladně vyřízených žádostí	Počet požadovaných uživatelských účtů
USA	3580	-	-
Rusko	-	-	-
Belgie *	67	-	-
Rok 2010			
Stát	Počet požadavků na data o uživateli	Procento kladně vyřízených žádostí	Počet požadovaných uživatelských účtů
USA	8888	94%	-
Rusko	-	-	-
Belgie *	156	73%	-
Rok 2011			
Stát	Počet požadavků na data o uživateli	Procento kladně vyřízených žádostí	Počet požadovaných uživatelských účtů
USA	12271	93%	23300
Rusko	100	0%	112
Belgie *	189	67%	135

Tabulka č. 1 - Statistika žádostí a předaných dat jednotlivým státním orgánům (vlastní zpracování, zdroj: Google)

* Česká republika v tomto seznamu neexistuje. Autor se rozhodl o porovnání s jinou zemí EU se stejným počtem obyvatel
- Data nejsou dostupná

Autorovi se nepodařilo zjistit důvod, proč se statistické údaje pro rok 2012 nejsou k dispozici.

2.3 Facebook

Facebook byl založen v roce 2004 Markem Zuckerbergem. Tato sociální síť umožňuje vytvoření profilu, rozmístění informace o sobě, přidávání kamarádů – jiných uživatelů Facebook do svého seznamu přátel, posílat zprávy, měnit status, psát zprávy na vlastní „zed“ nebo zed kamarádů, nahrávat fotografie a video, vytvářet skupiny nebo zájmové stránky nebo se k nim přidávat.

Uživatelé Facebook, pomocí aplikací mohou hrát hry, sdílet multimediální obsah nebo komunikovat s přáteli. Aplikace na Facebook není nic jiného, než webová stránka, která prostřednictvím API komunikuje s Facebook a integruje nebo rozšiřuje jeho funkce. Aplikace může mít mnoho podob, od hry typu piškvorky až po promyšlené online hry typu Mafia Wars, mohou mít podobu nejrůznějších soutěží, multimédií, nebo přímo

¹⁹ Google Transparency Report. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.google.com/transparencyreport/userdatarequests/?p=2009-12>

nabídek různých společností, které propagují svoji produkci. Vždy však jde o dvě věci – prodej virtuálních peněz uživatelům aplikací a/nebo sběr osobních údajů a jejich případný následný prodej.

V říjnu 2012 počet aktivních uživatelů společenského webového systému Facebook přesáhl hranici 1 miliardu. Přibližně 81 % aktivních uživatelů tohoto servisu pochází mimo USA a Kanady. V roce 2011 tržby společnosti Facebook dosáhly částky \$3,71 mld. Z toho okolo 90 % tvoří tržby z reklamy²⁰.

Facebook byl dočasně nebo nastalo zakázán v následujících státech – Čína, Irán, Uzbekistán, Pákistán, Sýrie a Bangladéš z různých uváděných důvodů. Velké množství států zakázalo navštěvování této sociální sítě vlastním občanům například z důvodů proti islamisticky naladěného nebo religiózně diskriminujícího obsahu, který Facebook obsahuje. Stejná situace se zakázaným Facebook je i na mnoha pracovních místech, kde k zákazu došlo pro zlepšení pracovní efektivity nebo pro zamezení možnosti úniku cenných pro společnost informací. Facebook je zakázán i na některých školách pro sdílení nevhodného obsahu.

Problémy Facebook vyplývají i z koncentrace citlivých osobních dat a spousty aplikací, které k nim mají přístup. Aplikace může napsat kdokoli a poté data použít ke svým účelům.

Facebook neustále podléhá obviněním státních orgánů USA, Kanady nebo států EU týkajících se oblasti ochrany osobních údajů. Jedná se většinou o zákony kvůli shromažďování osobních údajů uživatelů (v případě stížnosti ze strany Kanady se hovoří o neúplném smazání účtu a následně osobních údajů uživatelů) nebo jejich nedovolené uchovávání.

²⁰ FORM 8-K, UNITED STATES SECURITIES AND EXCHANGE COMMISSION. Results of Operations and Financial Condition. [online]. 2012 [cit. 2012-12-08]. Dostupné z: <http://pdf.secdatabase.com/700/0001193125-12-316895.pdf>

3 Typické přístupy neodpovědného nakládání s osobními údaji

Uživatelé zůstávají v nevědomosti toho, že jsou neustále na webu sledováni. V obsahu studie²¹ týkající se pochopení internetovými uživateli podstaty behaviorální reklamy z roku 2010, Aleecia McDonald žádala účastníky průzkumu, aby si představili, že reklamní společnosti určují, které reklamy se budou zobrazovat, a to na základě několika faktorů, jedním z kterých je historie webového prohlížení. Jen 51 % účastníků připustilo, že toto je něco, co "se děje poslední dobou docela často". Když si autorka zažádala, aby účastníci průzkumu představili to, že zobrazované reklamy na serverech poskytujících emailové služby jsou taktéž určeny dle klíčových slov, obsažených ve zprávách, ještě menší množství dotazovaných sdělilo, že si toho jsou vědomé. Většina účastníků netušila, že tato praxe je velmi obvyklá, a téměř 30% věřilo, že se praxe takového typu nikde nestane realitou. Jeden účastník během výzkumu řekl, že behaviorální reklama zní jako něco co může vymyslet jen paranoidní mozek a zdaleka ne to, co může být realitou.

Obráncové soukromí říkají, že tato neznalost o převládání online sledování, vede lidi k tomu, aby se chovaly na webu tak, jako kdyby byly anonymní a dělá je naprosto neschopnými v obraně před nechtěným sledováním a únikem osobních údajů.

"Spotřebitelé považují vyhledávač za jejich osobního psychiatra, jejich rabína, jejich kněze, jejich lékaře," vysvětluje Christopher Soghoian²², obhájce soukromí který studuje ochranu dat a soukromí na doktorském studiu na univerzitě Indiana. "lidi napíšíou nejdůvěrnější věci do vyhledávacích strojů a jiných webových stránek v první řadě proto, že si myslí, že jsou anonymní. Uživatelé jsou schopné psát takové dotazy na odborných stránkách nebo fórech, které by nepoložily vlastnímu osobnímu lékaři. A ve skutečnosti nejsou ani anonymní".

Vše shora zmíněné je hlavním důvodem neodpovědného nakládání s osobními údaji. Přestože existuje určitá část uživatelů internetu, kteří tuší o online sledování, pouze malá část z nich si je vědoma jak daleko sáhnají chapadla společností, žíznivých po osobních údajích a ještě menší část dělá něco málo pro ochranu svého soukromí.

²¹ LASZLO, Joseph, Director of Research, IAB. News Media Workshop – Comment, Project No. P091200. [online]. 2010 [cit. 2012-12-08]. Dostupné z: http://www.iab.net/media/file/News_Media_Workshop_-_Comment_Project_No.P091200.pdf

²² Privacy researcher and activist. SOGHOIAN, PH.D., Christopher. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.dubfire.net/>

4 Typické způsoby zneužívání osobních údajů, včetně porušování jejich ochrany a jejich analýza

Málo internetových uživatelů si jsou vědomé toho že, při surfování na webu, podléhají stálému dozoru stovkami různých soukromých společností. Tyto společnosti, nazývané reklamní sítě, sledují internetové uživatele napříč webem, sbírají nejrůznější osobní informace o uživatelích – jejich pohlaví, věk, příjem, poloha, zdravotnické záležitosti, sexuální orientace, politická přídružení, hudební preference a mnoho dalších. Reklamní sítě pak užívají tuto informaci k tomu, aby prodávaly velmi personalizované online reklamy uživatelům Internetu. Tento proces je známý jako behavioral targeting (reklama založena na základě chování uživatele). Reklamní sítě ale mohou užívat informace, které sbírají i jinak, než pro účely behaviorálního targetingu. Kromě využívání (čti zneužívání) osobních údajů uživatelů, nacházejících se na Internetu, pro cílenou reklamu, reklamní sítě prodávají informaci třetím stranám, mezi kterými může být i překvapivě vláda. Mezi těmito informacemi můžou být velmi citlivé údaje, které se v nepovolaných rukou můžou stát zbraněmi ²³.

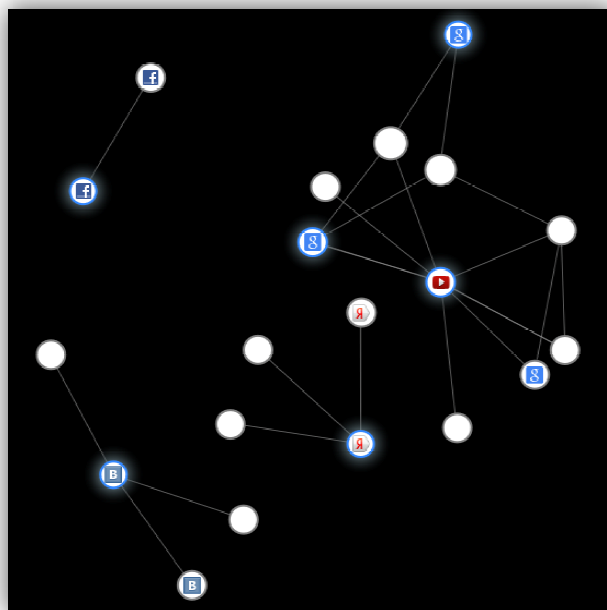
4.1 Definice sledovacích serverů třetích stran

Díky plug-inu, konkrétně Collusion, uživatel má možnost v reálném čase sledovat, jaké třetí strany instalují cookies (třetích stran) na počítač a tím sledují pohyb a chování autora na webu nebo kam navštívené servery odesílají informace o pohybu a chování uživatele. Tento plug-in zobrazuje vazby mezi navštívenou stránkou a dalšími servery, které sledují chování uživatele pomocí pavučiny vazeb.

Před samotným začátkem autor vymazal z paměti počítače HTML a Flash cookies. Pro účely tohoto pátrání po reálných datech autor navštívil weby Facebook, Google, Youtube, Yandex, Amazon a nakonec Seznam.

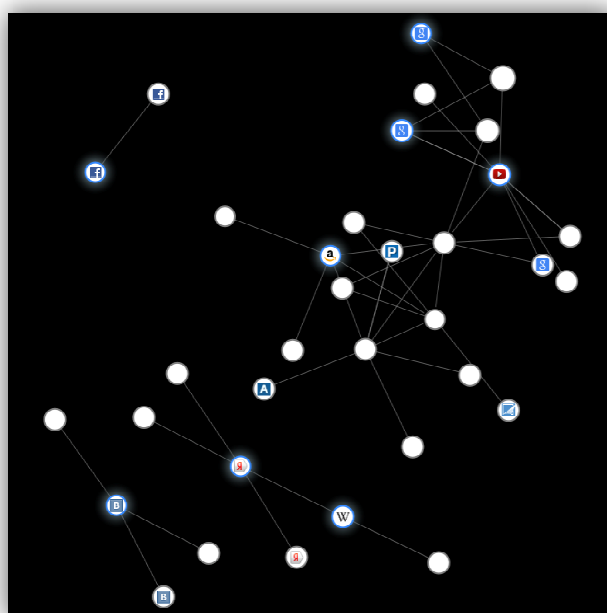
²³ Brotherton, E.A. 2012, "Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine", *Emory Law Journal*, vyd. 61, č. 3, str. 555-600.

I. část výzkumu



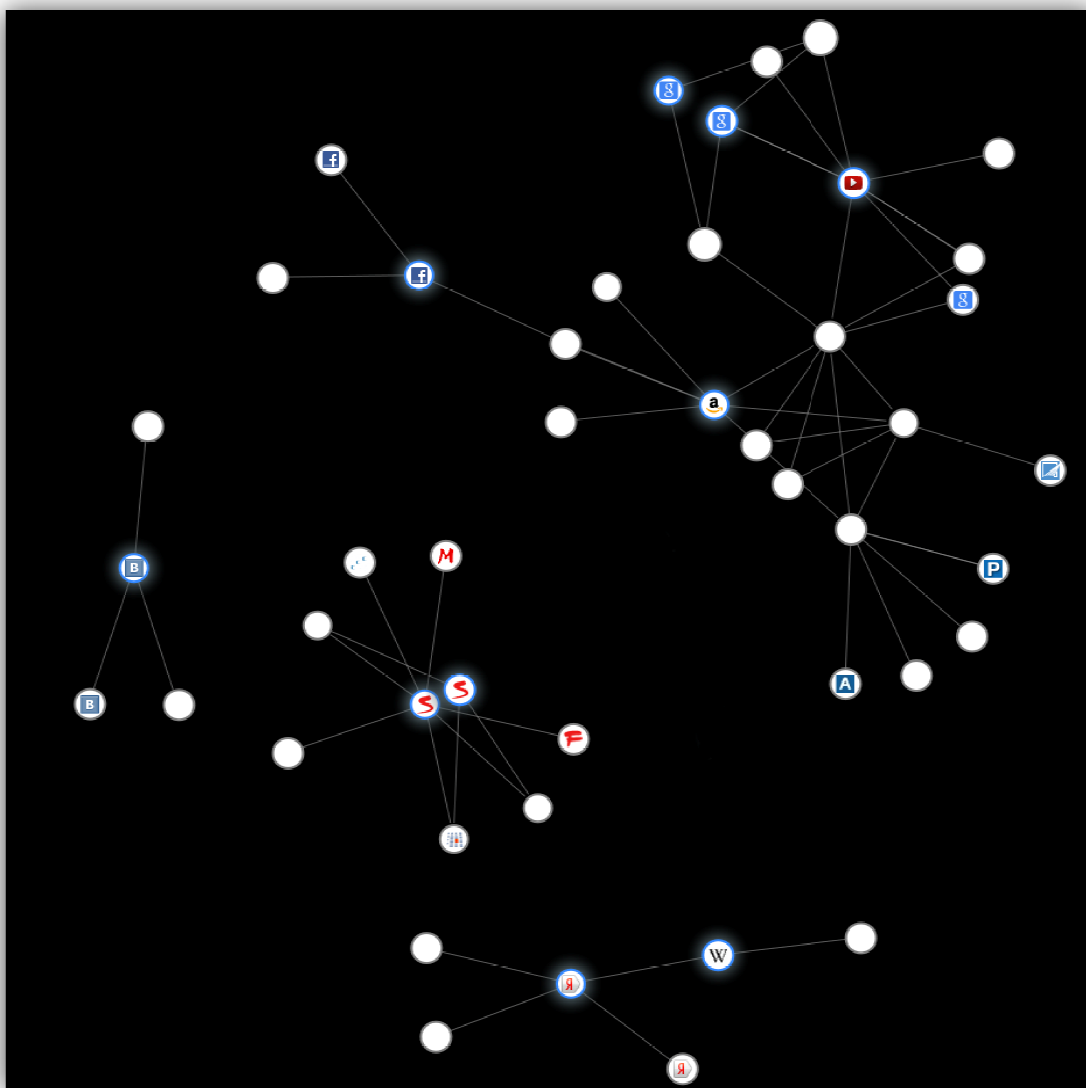
Obrázek č. 1 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)

Na tomto obrázku jsou vidět zvýrazněné ikonky navštívených webu facebook.com, vk.com, yandex.ru, google.com(cz) a youtube.com. V sekvenci návštěv stránek byl server youtube.com poslední. Po načtení obsahu stránky společné weby třetích stran google.com a youtube.com se spojily, tzn. že tyto weby poznaly, že autor nejprve navštívil jednu stránku, poté stránku druhou.



Obrázek č. 2 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)

Tento obrázek se liší pouze tím, že na něm přibyl server amazon.com. Jelikož je to jeden z nejpopulárnějších internetových obchodů současnosti, webů třetích stran, sledujících pohyb autora, patrně přibylo. Dle pavučiny na obrázku je zřejmé, že některé z těchto webů třetích stran jsou ty původní, co si spojily historii procházení nejprve stránky google.com, poté stránky youtube.com.



Obrázek č. 3 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)

Na tomto obrázku přibyl web seznam.cz, který stejně jako ostatní servery poskytuje ostatním pěti webům informace o pohybu autora.

Další postřeh, který můžeme vyvodit z uvedených obrázků je to, že weby, nacházející se na generické doméně .com jsou informačně spjaté ihned na první pohled. Vyhledávač seznam.cz sdílí data s ruským serverem yandex.net . Na druhé straně ruský vyhledávač yandex.ru sdílí data přes weby třetích stran s webem vk.com přes server yadro.ru.

Během pátrání autor přišel na následující - Facebook instaluje cookies i když uživatel není přihlášen, po opakovaném vymazání HTML cookies (nikoli Flash cookies) a načtení stránek jako facebook.com, vk.com a jiných si prohlížeč pamatoval přihlašovací jméno (v seznamu uložených přihlašovacích údajů tyto záznamy neexistovaly) – je zřejmé, že přihlašovací jméno se ukládá do Flash cookies a je zpětně vytvořeno do HTML cookies.

Dole se nachází tabulka s adresy navštívených stránek a webů třetích stran, které buď ukládaly cookies nebo sledovaly pohyb autora, nebo obojí.

Web	Stav	Požadovaný server	Servery třetích stran instalující cookies	Počet cookies
facebook.com	nepřihlášen	facebook.com		9
	přihlášen		fbcdn.net	-
			akamaihd.net	-
vk.com	nepřihlášen	vk.com		3
			userapi.com	-
			scorecardresearch.com	2
			yadro.ru	2
			login.vk.com	4
google.com	nepřihlášen	google.com		2
			youtube.com	5
			accounts.google.com	5
			accounts.youtube.com	2
			googleusercontent.com	-
			googlesyndication.com	-
	přesměrováno	google.cz		3
			gstatic.com	-
youtube.com	přihlášen	youtube.com		9
			doubleclick.net	-
			googlesyndication.com	-
	přehrávání videa		googletagservices.com	-
			yting.com	-
			youtube-nocookie.com	-
			plus.google.com	1
yandex.ru	nepřihlášen	yandex.ru		3
			mc.yandex.ru	1
			tns-counter.ru	1
			yandex.st	-
			yandex.net	-
wikipedia.org	-	ru.wikipedia.org		1
			wikimedia.org	-
amazon.com	nepřihlášen	amazon.com		6
			voicefive.com	6
			dimestore.com	1
			imrworldwide.com	2
			amazon-adsystem.com	2
			tag.admeld.com	1

			openx.net	1
			rubiconproject.com	2
			tap.rubiconproject.com	1
			ads.pubmatic.com	2
			submatic.com	3
			doubleclick.net	-
			images-amazon.com	-
			atdmt.com	-
			ssi-images-amazon.com	-
			ahmeld.com	-
			twimg.com	-
			imrworldwide.com	-
			fbcdn.net	-
seznam.cz	nepřihlášen	seznam.cz		3
			imedia.cz	2
			track.adform.net	2
			adform.net	1
			yandex.net	-
			im.cz	-
			gemius.pl	-
	vyhledávání		picsearch.com	-
			firmy.cz	
	přihlášen	szn.cz		2
			im.cz	-
			gemius.pl	-
			imedia.cz	2

Tabulka č. 2 - Adresy navštívených stránek a webů třetích stran (zdroj: autor)

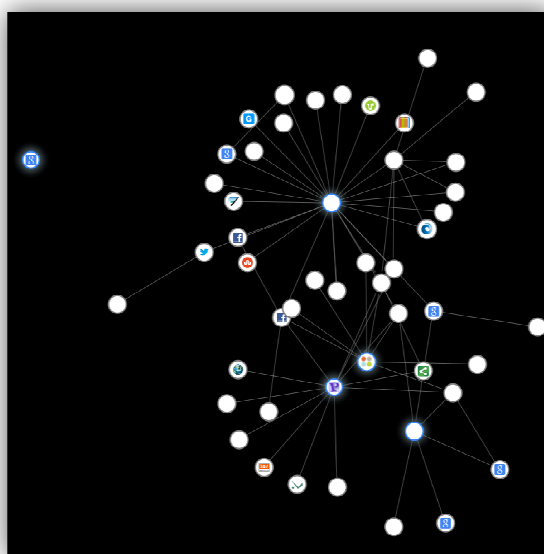
II. část výzkumu

Cílem druhé části pátrání je sledování zaznamenávání informací o pohybu autora během googlování slovního spojení „husky dog“ a navštěvování stránek na první pohled nespojených se servery Google nebo Facebook. Následovalo znovu vymazání cookies, vynulování paměti plug-inu Collusion.

Autor navštívil čtyři stránky, které se zobrazily na první straně vyhledávání Google:

- dogster.com
- petfinder.com
- pluspets.com a
- pets4homes.co.uk

Během pětiminutového brouzdání, kdy autor navštívil pouze hlavní stránky shora uvedených webů, se na počítači autora uložilo 27 cookies, ze kterých (což je logické) 22 patří třetím stranám.



Obrázek č. 4 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)

Na obrázku shora jsou vidět čtyři zvýrazněné kroužky – jsou to autorem navštívené weby. Kroužky nezvýrazněné jsou napojené weby třetích stran, kterým autorem navštívený server odesílá data. Dle obrázku je patrné to, že některé weby třetích stran jsou napojené na všechny čtyři autorem navštívené weby. Konkrétně:

- facebook.com, který odesílá veškerou komunikaci na fbcdn.net
- google-analytics.com
- doubleclick.com, který odesílá veškerou komunikaci na googlesyndication.com
- scorecardresearch.com
- googleapis.com

Spojením postřehu z první a druhé části pátrání autor sestavil tabulku serverů, sbírající data z více autorem primárně navštívených stránek.

Web	Napojené weby	Vlastník	Stát
doubleclick.net	youtube.com	Google Inc.	USA
	google.com		
	amazon.com		
googleusercontent.com		Google Inc.	USA
googleapis.com		Google Inc.	USA
google-analytics.com	google.cz	Google Inc.	USA
	google.com		
	youtube.com		
yimg.com	google.com	Google Inc.	USA
	youtube.com		
ssl-images-amazon.com	facebook.com	Amazon.com, Inc	USA
	amazon.com		
imrworldwide.com	amazon.com	The Nielsen Company	USA
	youtube.com		
	google.com		

akamaihd.net	facebook.com	Akamai Technologies	USA
	amazon.com		
dimestore.com	amazon.com	Knowledge Networks, Inc	USA
	youtube.com		
	google.com		
fbcdn.net	facebook.com, ostatní	Facebook, Inc	USA
scorecardresearch.com	vk.com, ostatní	TMRG, Inc	USA

Tabulka č. 3 - Servery, sbírající data z více autorem primárně navštívených stránek (zdroj: autor)

V tabulce shora jsou uvedeny servery třetích stran s největším počtem spojení k primárně navštíveným stránkám. Veškeré domény patří společnostem ze Spojených států amerických ²⁴. V následujících kapitolách autor bude hovořit o těch nejvýznamnějších a všudypřítomných serverech.

4.2 Google a DoubleClick

Společnost DoubleClick byla založena v roce 1996 a byla jednou z mála přeživších úpadek po internetové horečce v rocích 2000-2001. V roce 2007 Google koupila společnost DoubleClick za \$3,1 mld. (druhá největší akvizice v historii Google, první je nákup Motorola Mobility v srpnu 2011), což je skoro dvojnásobek částky zaplacené Googlem za server YouTube o rok dříve. V roce 2011 společnost DoubleClick vydělala přes 300 mln na display reklamách. Tyto údaje jsou dle názoru autora velmi důležité pro vytvoření objektivní představy o důležitosti tohoto serveru pro Google a celkově pro trh s display reklamami.

Google spojil funkcionalitu přinesenou společností DoubleClick s vlastním AdWords, čímž dosáhl nedotěrné reklamy nacházející se na nespočetném množství internetových stránek a miliardových zisků. Hlavním účelem existence tohoto serveru je shromažďování údajů o pohybu a chování uživatelů na internetových stránkách, součástí kterých jsou display reklamy, které pomoci instalovaných cookies toto sledování umožňují. Každé zařízení připojené k internetu vlastní IP adresu, která může být jednoduše přiřazena k jedinečnému účtu uživatele a ve spojení se zeměpisnou polohou a širokou škálou cookies nainstalovaných na zařízení uživatele si společnost Google vytváří přesné profily o jednotlivcích a bublinu filtrů šitou na míru. Spojením těchto dat s historií vyhledávání na Google, účtem Google+, emailovou službou Gmail,

²⁴ DOMAINTOOLS, LLC. *DomainTools* [online]. [cit. 2012-12-08]. Dostupné z: whois.domaintools.com

odebíranými kanály a historii prohlížení na YouTube a přiřazením unikátního ID je na světě osobní profil každého uživatele.

Taktéž společnost DoubleClick je kritizována za klamání uživatelů nabízením nefunkční možnosti nezúčastnění se online sledování. V souladu s tvrzením The Elvey Partnership IT Consulting Group ze San Franciska, tato možnost ovlivňuje pouze instalování cookies, nikoli sledování pohybu na základě zaznamenávání IP adresy.

4.3 Google Analytics

V souladu s definicí sledovacích serverů třetích stran v kapitole 4 a přílohou 1, autor této práce si dovoluje tvrdit, že Google Analytics je nejvýznamnějším a všude přítomným serverem třetí strany dotěrně sledujícím pohyb každého uživatele na síti.

Google Analytics je servis, nabízející společností Google, který generuje detailní statistika o pohybu uživatelů na internetové stránce. Základní funkčnosti služby jsou nabízeny zdarma až do 10 miliónů návštěv stránek za měsíc, což je naprosto dostačující pro většinu existujících internetových stránek. GA je schopný sledovat uživatele, které přišly ze všech destinací včetně vyhledávačů, display reklam, pay-per-click sítí, email marketingu a osamostatněných odkazů (např. odkaz v souboru DOC nebo PDF). GA se implementuje pomocí tagování stránek. Tag stránky v případě GA se jmenuje Google Analytics Tracking Code (GATC) je kus kódu JavaScript (webové štěnice), který majitel webu zahrnuje do každé jednotlivé stránky. JavaScript kód je spuštěn při každém načtení stránky, pomocí webové štěnice jsou data následně odesílána a shromažďována na serveru společnosti Google.

Ihned na začátku relace se do počítače uživatele instaluje větší soubor (ga.js, 18 KB), který následně načítá proměnnou čísla profilu uživatele. Řádek kódu je následující:

`_gaq.push(['_setAccount', 'UA-18830626-3']);`. Jelikož se tento soubor nachází v cash paměti, není nutno jej načítat při navštěvování každé další stránky webu. Když uživatel přechází ze stránky jedné domény, využívající službu GA, na stránku jiné domény, taktéž využívající službu GA, nacházející se v cash paměti soubor ga.js, si zaznamenává sekvenci procházení stránek a taktéž tyto data odesílá na server Google.

Navíc k odesílaným informacím na server Google, GATC ukládá na zařízení uživatele cookies, které uchovávají informaci o návštěvách konkrétního webu (pro identifikaci toho, jestli se jedná o nového nebo vracejícího se uživatele), datu a času aktuální návštěvy a referenční místo kampaně nebo adresy, odkud uživatel přišel na danou stránku.

Vzhledem k dostupnosti a oblibě webových vývojářů v jeho implementaci do svých webů je tento servis skutečně všudypřítomný. Shora uvedené vyvolává určité znepokojení. Kdykoliv uživatel navštíví stránku, používající GA, pokud má povolený JavaScript v prohlížeči, Google sleduje veškeré jeho chování.

Pokud návštěvník stránky používá Google Account jako identifikátor (ID) pro vytvoření komentářů nebo načítání obsahu ze serverů, které patří společnosti Google (Blogger, YouTube, Gmail aj.), pak Google spojí získané data z GA s veškerými údaji, které uživatel sdílí na jakémkoliv profilu Google.

Spojením informací získaných pomocí služeb DoubleClick a Google Analytics společnost Google automatizovaně vytváří stínové profily (shadow profile) jednotlivých uživatelů, které jsou přiřazené k jednotlivým účtům. Autor této práce níže přikládá obrázek, znázorňující jemu přiřazené hodnoty a parametry během jednoho týdne. Je třeba podtrhnout tu skutečnost, že se veškeré úkony provádějí bez jakéhokoliv souhlasu uživatele.

Vaše kategorie

Níže naleznete přehled zájmů, které Google přiřadil k vašemu souboru cookie.

Domov a zahrada - Domácí nábytek - Pohovky a křesla	Odebrat
Internet a telekomunikace - E-mail a zprávy	Odebrat
Krása a fitness - Péče o obličej a tělo - Vůně a parfémy	Odebrat
Lokality ve světě - Asie - Západní Asie - Turecko	Odebrat
Lokality ve světě - Evropa	Odebrat
Nakupování - Aukce	Odebrat
Počítače a elektronika - Software	Odebrat
Počítače a elektronika - Software - Software pro podnikání a zvýšení produktivity	Odebrat
Práce a vzdělávání - Práce	Odebrat
Práce a vzdělávání - Práce - Životopisy a portfolio	Odebrat

Přidat nebo upravit zájmy

Vaše demografické údaje

Tyto demografické údaje, které Google přiřadil k vašemu souboru cookie, můžete zkontrolovat níže. Váš věk a pohlaví vyvozujeme ze stránek, které jste navštívili.

Věk: 25–34	Odebrat
Pohlaví: Muž	Odebrat
Název jazyka: ruština	Odebrat

Přidat nebo upravit demografické údaje

Váš soubor cookie

Google uchovává v souboru cookie následující informace, aby mohl propojit vaše nastavení reklam s prohlížečem, který používáte:

id=22e75d1d6d0100e6||t=1353175905|et=730|cs=002213fd480d7b9be92233967f

Obrázek č. 5 - Zobrazení preferencí přiřazených uživateli (zdroj: autor)

4.4 Facebook

Facebook vytváří záznamy o internetových uživatelích v první chvíli pro kohokoliv, komu přidělí unikátní cookie – tu je možné získat návštěvou Facebook (uživatel nemusí být přihlášen) nebo návštěvou jakékoliv stránky, obsahující některý z prvků Facebook – Like/Líbí prvky, komentáře a řada dalších.

Cookies přihlášeného uživatele:

facebook.com	a_user	836475038
facebook.com	a_xs	37af98gj84pdkg965jrkmw548d6fk487sgdk5
facebook.com	act	22956273849506%7G5
facebook.com	c_user	736475038

facebook.com	datr	tUZOTmY7Jkr559fKeyT623Lpft7gdN
facebook.com	L	2
facebook.com	locale	cs_CZ
facebook.com	lu	jjuf567Hd89Kdg3205KljhFecscC
facebook.com	opened_p	88274503713653
facebook.com	p	87af98gj84pdkg965jrkmw548d6fk487sgdk5Y7Jk g965jrk...
facebook.com	presence	22956273849506
facebook.com	s	Y7Jkr559fKeyT6
facebook.com	sct	883274495
facebook.com	sid	1
facebook.com	xs	1%965jrkmw548d

Tabulka č. 4 - cookie přihlášeného uživatele (zdroj: autor)

Cookies odhlášeného uživatele:

facebook.com	a_user	836475038
facebook.com	a_xs	965jrkmw548d6fk487sgdk537af98gj84pdkg
facebook.com	act	49506%7G5229562738
facebook.com	datr	tUZOTmY7Jkr559fKeyT623Lpft7gdN
facebook.com	L	2
facebook.com	locale	en_US
facebook.com	lsd	b8dkY
facebook.com	lu	j9ecscKd05KljhFC juf567Hd8 g32
facebook.com	opened_p	88274503713653
facebook.com	p	9
facebook.com	presence	59fKeyT623L48d6fk4TmY7Jkr23L48d6fk4TmY7Jkr23L4...
facebook.com	reg_fb_gate	http%3A%2F%2Fwww.facebook.com%2Findex.php%3Flh...
facebook.com	reg_fb_ref	http%3A%2F%2Fwww.facebook.com%2Findex.php%3Flh...
facebook.com	W	131687645

Tabulka č. 5 - cookie odhlášeného uživatele (zdroj: autor)

Dle shora uvedeného příkladu je vidět ten nepatrný rozdíl mezi cookie přihlášeného a nepřihlášeného uživatele. Nejpodstatnější informace (Facebook ID) je stále přítomna. Z toho lze vyvodit to, že nehledě na to, jestli uživatel je nebo není přihlášen, Facebook stále ví, koho v dané chvíli sleduje. Tuto informaci sledují webové prvky s Like/Líbí tlačítky. Vše shora uvedené jen potvrzuje ten fakt, že Facebook nechal v únoru roku 2011 patentovat metodu sledování uživatelů napříč webem²⁵.

Po smazání veškerých cookies, odhlášení z aplikace Facebook, surfování internetu bude Facebook (konkrétněji fbcdn.net) ukládat zatím anonymní cookies. Po opětovném

²⁵ FACEBOOK, Inc. *Communicating Information in a Social Network System about Activities from Another Domain* [patent]. USA. 705/14.41, G06Q 30/00 20060101 G06Q030/00. Uděleno 22. září 2011. Dostupné z: <http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20110231240.PGNR.&OS=dn/20110231240&RS=DN/20110231240>

přihlášení vytvořené „anonymní“ cookies se přiřadí k účtu uživatele. Mezi vytvořenými cookie je i unikátní identifikátor s expirací dva roky (facebook.com - datr).

V posledních letech byl Facebook kritizován pro modifikování svých pravidel soukromí k tomu, aby mohl zveřejňovat více informací o uživateli. V roce 2009 Facebook odesílal identifikační čísla reklamním společnostem, za určitých okolností, kdy uživatel klikl na reklamu. Po zveřejnění této informace v médiích, Facebook ihned problém vyřešil.

Facebook aplikace

"Apps" neboli aplikace, jsou části softwarového kódu, které umožňují více jak 800 milionům uživatelů Facebook hrát hry či sdílet mezi sebou společné zájmy. Většina aplikací není vyvinuta Facebook, ale nezávislými softwarovými vývojáři. Dle odhadu, sektor aplikací, který zahrnuje Facebook a trh reklamy na smartphone aplikacích, v roce 2011 vygeneroval tržby v celkové hodnotě \$20 mld. prodejem stahovaných souborů, reklamy, prodejem "virtuálního zboží" a jiných produktů. Populární aplikace mohou rychle začít být virální ze dne na den a získat miliony uživatelů, mohou ale zmizet ze scény stejně tak rychle. Toto nebezpečí je vysvětlením proč některé aplikace usilují o získání peněz shromažďováním maximálně možného objemu dat s nadějí o následný jejich prodej.

V žebříčku 10 nejpopulárnějších aplikací na Facebook, všechny předávají identifikační čísla uživatelů externím společnostem. Tři z top 10 aplikací, včetně FarmVille, předávají osobní údaje o přátelích uživatelů externím společnostem. Přenesená informace je jedním ze základních stavení bloků Facebook: jedinečné "identifikační číslo Facebook" (Facebook ID) je přiděleno každému uživateli stránky. Jelikož identifikační číslo Facebook je veřejná část jakéhokoliv Facebook profilu, kdokoliv může použít toto číslo k tomu, aby pomocí standardního webového prohlížeče vyhledal jméno jednotlivce, dokonce když dotyčná osoba nastavila maximální úroveň privátnosti profilu. Pro jiné uživatele této služby, Facebook ID odhaluje informaci, kterou dotyčná osoba ohodnotila parametrem "sdílet se všemi" včetně věku, bydliště, zaměstnání a fotografií.

Mnoho z nejpopulárnějších aplikací na sociální síti Facebook předávají osobní údaje - konkrétněji zprostředkovávají přístup ke jménům a osobním údajům uživatelů a v

některých případech i ke jménům a osobním údajům přátel stovkám reklamních společností a společnostem zabývajícím se online sledováním.

Politika Facebook, týkající se ochrany osobních údajů, zakazuje vývojářům aplikací jakýmkoliv způsobem spolupracovat při předávání osobních údajů uživatelů této sociální sítě společnostem, které nepodepsaly souhlas o zákazu shromažďování osobních údajů. Nicméně studie společnosti PrivacyChoice ²⁶ tvrdí, že desítky nejpoužívanějších aplikací na Facebook spolupracuje s neschválenými společnostmi, ze kterých ta nejvýznamnější je Google – největší inzerent v prostředí internetu. Z toho vyplývá, že uživatele používající aplikace Facebook jsou sledované společnostmi Google a ostatními spolupracujícími s Google reklamkami. Google tomuto oponuje tím, že reklamní společnosti, využívající síť DoubleClick, musí souhlasit s podmínkami o neshromažďování identifikujících osobních údajů.

Brendan Wallace, spoluzakladatel Facebook aplikace "Identified", která poskytuje služby v oblasti kariérního networkingu řekl, že jeho společnost míří k tomu, aby vybudovala datový sklad. Brandan Wallace si není jistý, jak bude informace z datového skladu užívána, ale řekl, že "data jsou přesně to, k čemu chtějí mít všichni přístup". Aplikace "Identified", která není ani v top 100 aplikacích na Facebook, obdrží od každého uživatele datum a místo narození, bydliště, vzdělání a dosavadní praxe, a rovněž stejnou sadu informací od přátel uživatele.

Celá řada aplikací, vyhodnocených časopisem Wall Street Journal, posílaly Facebook ID přinejmenším 25 reklamním a shromažďujícím data společnostem, ze kterých několik budují profily internetových uživatelů sledováním jejich online aktivit ²⁷.

Obhájci online sledování argumentují, že tento druh sledování je benigní protože je prováděn anonymně. Nicméně v tomto případě „časopis WSJ zjistil, že jedna společnost shromažďující data - RapLeaf Inc., spojovala získané z aplikací identifikační čísla Facebook s její vlastní databází internetových uživatelů, za účelem prodeje. Jak se později zjistilo - RapLeaf předává získané informace desítkám jiných společností. Na

²⁶ BROCK, Jim. Facebook gives The Product more control over how it is sold. [online]. 2012 [cit. 2012-12-08]. Dostupné z: <http://blog.privacychoice.org/>

²⁷ ANGWIN, JULIA a JEREMY SINGER-VINE. Selling You on Facebook. [online]. 2012 [cit. 2012-12-08]. Dostupné z: <http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html#articleTabs%3Darticle>

což RapLeaf odpověděl, že přenos byl neúmyslný. "Nedělali jsme to úmyslně" řekl Joel Jewitt, viceprezident rozvoje obchodu v RapLeaf.

Facebook následně sdělil, že "učinil kroky pro významné omezení možnosti společnosti Rapleaf v používání jakýchkoliv dat z Facebook". Otevřenou otázkou zůstává jak může Facebook zabránit ve vykonávání činnosti, která je hlavní náplní a hlavním zdrojem příjmů společnosti, jako RapLeaf a o kolika dalších únicích uživatele služby Facebook stále neví.

V říjnu roku 2010 Facebook vytvořil ovládací panel, který umožňuje uživatelům podívat se na to, která aplikace přistupuje ke které kategorii jejich osobních údajů. Tento ovládací panel například ukazuje, kdy aplikace přistupuje k základním informacím o uživateli (včetně identifikačního čísla Facebook). Nicméně tento panel neposkytuje žádnou informaci o přístupu aplikací k osobním údajům přátel konkrétního uživatele.

Facebook a WolframAlpha

WolframAlpha je odpovídací stroj vytvořen firmou Wolfram Research. Je to služba, která se snaží přímo odpovídat na dotazy uživatele. Na rozdíl od vyhledávacích služeb, které poskytnou pouze seznam stránek, které odpověď mohou obsahovat. WolframAlpha je vytvořen na dřívějším produktu Mathematica, který využívá pro řešení algebraických úloh, numerických a statistických výpočtů, ale i vizualizaci výsledků. Odpověď se zobrazí v člověku čitelné a přehledné formě. Často je přiložen i postup vedoucí k výsledku.

Jednou z nespočetného množství nabízených služeb ²⁸ je i statistická analýza profilu Facebook. Na začátku procesu vedoucího k zobrazení výsledků analýzy je třeba udělit přístupu aplikaci WolframAlpha na stránkách Facebook k osobním údajům – konkrétně k příspěvkům uživatele a seznamu přátel. Autor chce podtrhnout, že shora zmíněná aplikace nevyžaduje přístup k žádným jiným údajům a uchovává data po dobu jedné hodiny – slouží pouze k uspokojení zvědavosti uživatele.

²⁸ WolframAlpha: Facebook. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.wolframalpha.com/input/?i=facebook>



Obrázek č. 6 - Načítání dat serverem WolframAlpha z Facebook (zdroj: autor)

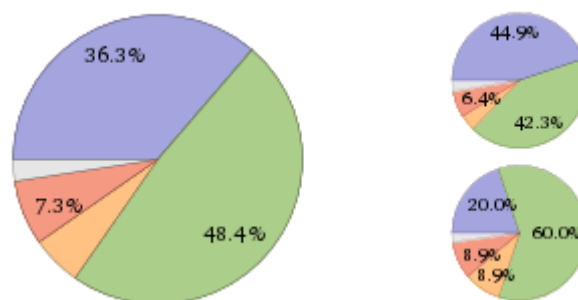
Výsledky dotazu na statistiku stránky uživatele poskytly následující informace – jméno, příjmení uživatele, datum narození a počet dnů zbývajících ke dni dalších narozenin, aktivitu uživatele po dobu posledních dvou let s počtem a poměrem sdílených odkazů a statusů, týdenní časový harmonogram s údaji o času aktivity a neaktivity uživatele, taktéž po dobu dvou let, statistika s počtem zveřejněných statusů, lajků a komentářů, infografika s nejpoužívanějšími slovy ve statusech, seznam přátel s největším počtem komentářů a lajků na sdílené odkazy nebo statusy, mapa s nejčastějšími místy check-inů.



Obrázek č. 7 - check-iny a oblako slov (zdroj: autor)

Dále aplikace poskytuje údaje o fotografiích, jejich popularitě (s počtem komentářů a lajků).

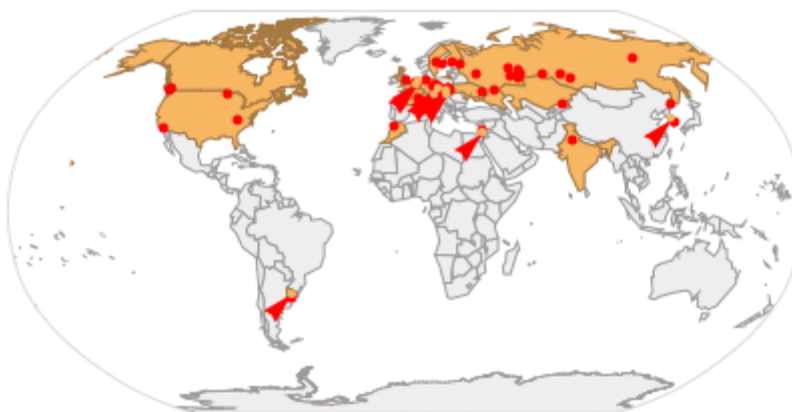
V další části se aplikace soustředí na přátele – poskytuje širokou škálu informací, která hlavním způsobem začíná na jejich identifikačních číslech Facebook, které jsou jedinečné, dále například poměr mužů a žen nebo údaje o poměru skupin dle stavu svobodný/zadaný.



Obrázek č. 8 - Statistické údaje o přátelích (zdroj: autor)

V diagramu shora fialová barva reprezentuje počet svobodných přátel, zelená barva počet přátel ve vztahu, oranžová barva zasnoubených a červená ženatých. Diagramy vpravo reprezentují stejná data, ale pouze u mužů (horní) a žen (dolní).

U přátel se zobrazují i takové informace jako diagram s věkovým rozdělením, tabulka s údaji o nejstarších a nejmladších přátelích, přesné údaje o lokalizaci přátel.



Obrázek č. 9 - Lokalizace přátel (zdroj: autor)

Nejenže aplikace WolframAlpha na Facebook má přístup k obecným údajům o přátelích, ale i k těm citlivým. Statistický výpis poskytuje údaje o politických názorech a náboženství.

Většina aplikací na Facebook jsou znatelně žízňivější nejen po informacích konkrétního uživatele, který danou aplikaci používá, ale i po údajích jeho přátel, které ani netuší o tom, že i jejich data jsou shromažďována. To se děje jen díky tomu, že někdo z jeho přátel používá aplikace, s podmínkami užívání, kterých souhlasil a vlastně někdo jiný za ně rozhoduje o tom, že jeho osobní údaje budou nejen shromažďována, ale následně na dobu neurčitou uložena, zpracována a případně následně prodána.

Facebook a žaloby

Kromě nesčetného množství žalob jednotlivců, nebo jejich uskupení, facebook systematicky podléhá žalobám ze stran státních orgánů jednotlivých států.

Kanada, 2009

V roce 2009 Facebook podlehl obviňování ze strany státních orgánů Kanady ve věci porušování kanadských zákonů kvůli shromažďování osobních údajů uživatelů, kdy se zřizovatelé Facebook mohli dostat před federální soud. Speciálně vytvořena komise na ochranu soukromí provedla šetření, z něhož vyplynulo, že provozovatelům Facebook zůstávají osobní údaje uživatelů i poté, co se někdo ze sítě "vyškrtne" - v takovém případě totiž je jeho profil jen "zmražen", zároveň se ale nemohou dostat ke svým nasbíraným kontaktům či fotkám. Odpovědný zástupce sociální sítě už uvedl, že Facebook vyhodnotí závěry komise a pokusí se najít vhodné řešení. V Kanadě využívá stránky zhruba třetina obyvatel.

Německo, 2011

Státní orgán v Hamburku, Německo, zabývající se ochranou dat a osobních údajů, začal proces podáním stížností na největší sociální síť světa ve věci automatického rozlišování obličejů. Žaloba hovoří o shromažďování velkého objemu biometrických údajů bez jakéhokoliv povolení ze strany uživatelů. Hlavním bodem neshody je nabízena Facebook možnost nezúčastnění se ve zpracování novou funkcionalitou, kdežto německý zákon o zpracování osobních údajů jasně hovoří o tom, že výchozí nastavení shora zmíněné funkcionality nesmí zahrnovat žádného uživatele do seznamu zpracovávaných osob do té chvíle, kdy uživatel projeví výslovnou touhu se do tohoto seznamu zařadit a následně vybere možnost zapnutí funkcionality.

Irsko, 2011

Irský úřad pro ochranu dat se na konci roku 2011 připravoval stížnost na společnost Facebook pro nesmazání posílaných mezi uživateli zpráv. Facebook je pouze archivoval, což je v přímém rozporu se zákony EU a Irska o ochraně osobních údajů a konkrétně se stále opakující se větou – každý má právo na to být zapomenutým na jakýmkoliv internetovým serveru.

Nehledě na všechny shora uvedené případy žalob různých organizací, provozovatelé Facebook mají v záloze jeden podstatný argument - souhlas s podmínkami služby, který jim poskytli sami uživatelé, když se na sociální síť registrovali.

4.5 Ostatní servery

Jelikož se autor této práce soustředí na situaci s ochranou osobních údajů v České republice, Ruské federaci a ve Spojených státech amerických, bylo by chybou nezmínit

základní servery, nabízející obdobné služby jako Facebook a Google, ale již na území evropského kontinentu.

Česká republika

Seznam.cz

Společnost Seznam.cz, a.s. patří do malého množství podniků, které stále vzdorují globálnímu hráči Google. Seznam.cz nabízí podobné služby jako Google, hlavně služby vyhledávače, elektronickou poštu a službu Seznam homepage, na které si uživatel může sestavit personalizovaný obsah z poskytovaných modulů služeb této společnosti.

Ruská federace

Vk.com

Vkontakte.ru (vk.com) je ruská sociální síť, která se nachází na první pozici dle popularity v Ruské federaci. Jedná se o obdobu amerického Facebook.

Yandex.ru

Společnost Yandex.ru je obdobou českého Seznamu. Nachází se na první pozici v popularitě mezi vyhledávači v Rusku.

Shora zmíněné servery spojuje nejen jimi nabízené služby, ale i mechanismy generování zisku. Je nutné podotknout jediné – zdaleka se nenachází na úrovni amerických společností, co se týče zacházení s osobními údaji. Tyto servery nedisponují tak velkou sítí spřátelených webu, nemají obdoby reklamní sítě Google AdSense a hlavně se musí řídit přísnými zákony Evropské unie a Ruské federace, které dávají menší prostor pro podnikatelskou kreativitu a větší ochranu osobních údajů.

4.6 Agregátory dat

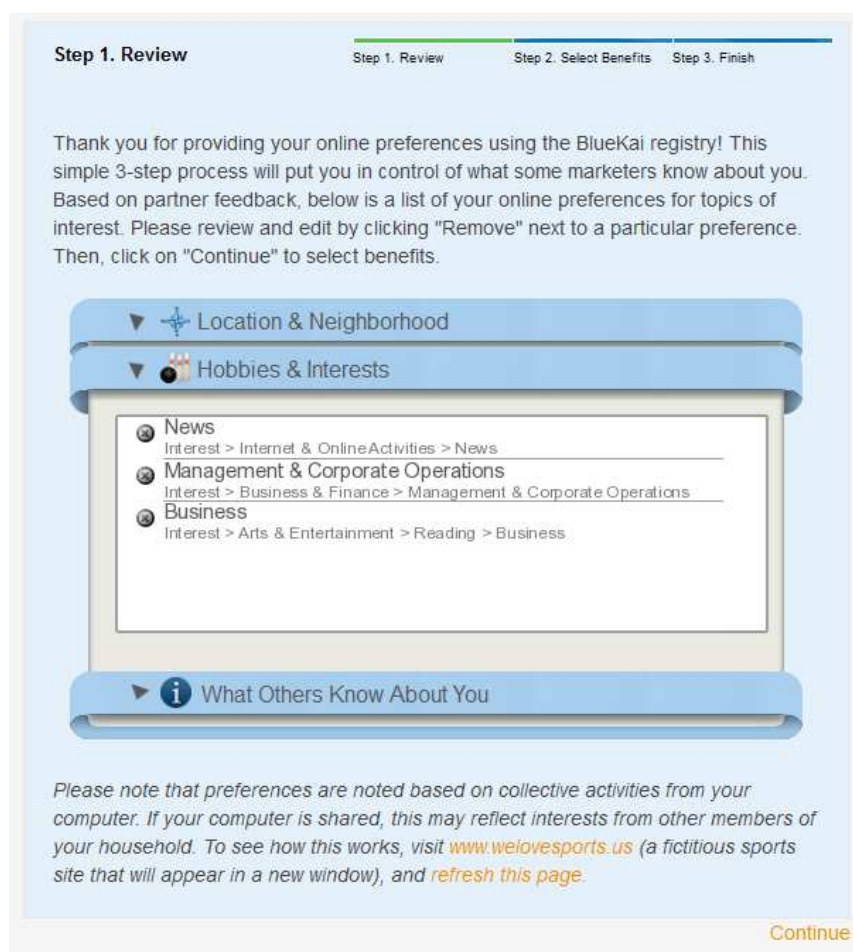
V anglicky psané literatuře se lze setkat s pojmem Agregátor Dat. Tento pojem v kontextu této diplomové práce můžeme aplikovat na servery sbírající údaje z celé řady různých webů. Příkladem agregátoru dat můžeme uvést takové společnosti jako RapLeaf, Bluekai, Acxiom, Lotame nebo ChoicePoint, které na jednotlivce sestavují informační portfolia z dat, nacházejících se v detailních databázích za účelem jejich dalšího prodeje.

Zdrojem informací pro agregátory dat jsou takové veřejné zdroje informací jako sociální sítě, registry dlužníků, informační centra s dobrovolnou registrací, síť spřátelených serverů, které poskytují agregátkům dat cookies uživatelů etc. Potřebná data jsou

vydolována, sestavena do reportů a předána objednavatelům. Zájemce o tyto soubory osobních údajů můžou být jak soukromé společnosti, banky nebo vládní orgány.

Agregátory dat, tedy společnosti, sbírají různé kategorie informací, některé se soustředí na data pro banky, které zajímají solventnost zákazníků, některé pro pojišťovny, některé zase pro marketingové agentury. Společným rysem agregátorů dat je (z hlediska evropských zákonů) systematické porušování zákonů. Stejně tak, jako v případě vyhledávacích serverů nebo sociálních sítí, jsou tyto weby registrované společnostmi se sídlem ve Spojených státech amerických.

Následuje příklad webu společnosti Bluekai, který jako jeden z mála nabízí náhled na přiřazené parametry jednotlivému uživateli (v konkrétním případě autorovi). Dole uvedený snímek obrazovky ukazuje tři kategorie údajů – zeměpisná poloha uživatele, zájmy a servery, které využívají mé údaje. Tento snímek byl pořízen po patnácti minutách brouzdání na webu; v záložce lokace stojí Česká republika.



Obrázek č. 10 - Profil vytvořený na základě chování uživatele (zdroj: Bluekai)

Konkrétní seznam faktorů, dle kterých se dělá vyhodnocení, a přiřazují se parametry, web neuvádí, zato odhaluje, co vše může o každém obyvateli internetu vědět ²⁹:

Co o Vás můžeme vědět	Co o Vás nevíme
• Věková kategorie • Pohlaví • Rodinný stav • Vojenská evidence • Jazyk, kterým mluvíte • Úroveň vzdělání • Zaměstnání • Věkový rozptyl rozsah, pohlaví a přibližné množství dětí ve vaší domácnosti • Informace o zdravotním stavu a životním stylu (jestli se zajímáte o jógu, či zdravý životní styl) • Informace o bydlení (nemovitosti) (pronájem, vlastní, atd.) • Finanční statut (jestli máte hypotéku, platíte vaše účty online, hledáte půjčku na auto atd.)	• Žádné identifikační informace - Jméno a příjmení - Emailová adresa - Adresa - Rodné číslo - Datum narození • Číslo kreditní karty • Číslo řidičského průkazu • Osobní zdravotní informace • Náboženství

Tabulka č. 6 - Seznam údajů, které může/nemůže agregátor dat Bluekai vědět (zdroj: Bluekai)

Ihned na první pohled je zřejmé, že všechny údaje, nacházející se v první kolonce (Co o Vás můžeme vědět) jsou z pohledu evropské právní úpravy buď osobní nebo dokonce i citlivé. A to velmi. Shromažďováním těchto údajů se shora zmíněné právní úpravy velmi hrubě porušují.

Tvrzení o tom, že společnost Bluekai o autorovi, jako uživateli, nedisponuje některými údaji je velmi sporné. Pravdou může být skutečnost, že Bluekai tyto údaje neshromažďuje, ale může prodat soubor dat, které jsou přiřazené k IP adrese a jiný agregátor dat si k datum od Bluekai přiřadí data vydolovaná ze sociálních sítí. Tato situace není zdaleka hypotetická, důkazem toho je nesčetné množství žalob podaných na

²⁹ Doslovný překlad autora

americký úřad FTC ³⁰, které hovoří o prokazatelném spojování dat a profilování společnosti RapLeaf údajů z Facebook, vyhledávačů a agregátorů dat.

4.7 Bublina Filtrů

Pojem The Filter Bubble autor již zmínil dříve v této práci v úvodních kapitolách.

Marku Zuckerbergovi položili otázku o důležitosti News Feed ³¹, proč se jeví jako nejdůležitější na stránkách Facebook a je ihned na hlavní stránce. Na což odpověděl:

„A Squirrel Dying In Your Front Yard May Be More Relevant To Your Interests Right Now Than People Dying In Africa.“ Mark Zuckerberg, Facebook

V této části práce se autor věnuje myšlence relevance, o tom jak myšlenka relevance ovlivňuje internet a o tom, jak se nacházíme v zajetí vlastních zájmů – v Bublině Filtrů. Mnoho lidí jsou přesvědčeny v tom, že je internet spojuje s celým světem, s lidmi a zprávami z každého státu a každé části zeměkoule. Každý dostává nejčerstvější zprávy zbavené cenzury, má možnost podnikat mezi kontinenty, je ve spojení s přáteli po celém světě. Toto tvrzení se v poslední době začíná ztrácet na pravdivosti.

V současné chvíli dochází k určitým změnám v tom, jak se informace předává pomocí internetu a co je nejdůležitější – tyto změny jsou pro uživatele neviditelné. Ukažme si to na příkladu – osobní stránka na Facebook. Autor má na News Feed přátele, kteří milují kuchařství a neustále přidávají příspěvky o kuchařských návodech, restauracích a akcích v Praze. Kromě milovníků kuchařství se na News Feed objevují přátelé, kteří se zajímají o technologie, trendy vývoje ICT a zprávy ze světa financí. Všechny tyto příspěvky se mi zobrazují na News Feed. Jak je zvykem autora – přeskakuje příspěvky o kuchařství a kliká na zprávy týkající se financí či technologických novinek. Za nějakou dobu se příspěvky od „kuchařů“ přestanou zobrazovat a neobjeví se ani v případě, když budou psát o technologiích.

Facebook si zapamatovává volby, které uživatel kliká na News Feed a zobrazuje pouze ty zprávy, které zhodnotí jako „zajímavé pro uživatele“, ale ani se s ním neporadí.

„Filter Bubble je jak se zdá výsledek pozitivního trendu, ale když se zajímám pouze o Chivavy a italskou kuchyní, nikdy se nedozvím o obřím asteroidu, který upadnul několik set kilometrů od místa mého bydliště – samozřejmě do té doby, než nezačne padat popel.“

³⁰ Federal Trade Commission

³¹ Stránka vybraných příspěvků, jakási homepage stránky Facebook

Každý z nás podléhá riziku objevit se pod „skleněným poklopem“ vlastních zájmů“. Eli Pariser, The Filter Bubble^{32 33}

Kde se ale kromě Facebook setkáme s Filter Bubble? Google dělá naprosto to samé. Autor poprosil několik známých, aby vyhledali dvě různá slova a zpětně poslali seznam výsledků, který jim nabídnul Google. Výsledky vyhledávání jednotlivých uživatelů se lišily. V některých případech rozdíl byl v přehozených pozicích výsledků vyhledávání. V některých případech chyběly některé výsledky vůbec.

Výsledky i po odhlášení z Google účtu se nezměnily, uživatelé nebyly schopné opustit bublinu filtru – Google používá celkem 57 signálů, neboli typů personalizace – parametrů, které zhodnocují typ přístroje (PC), typ prohlížeče, IP, historii prohlížení a vyhledávání a jiné.

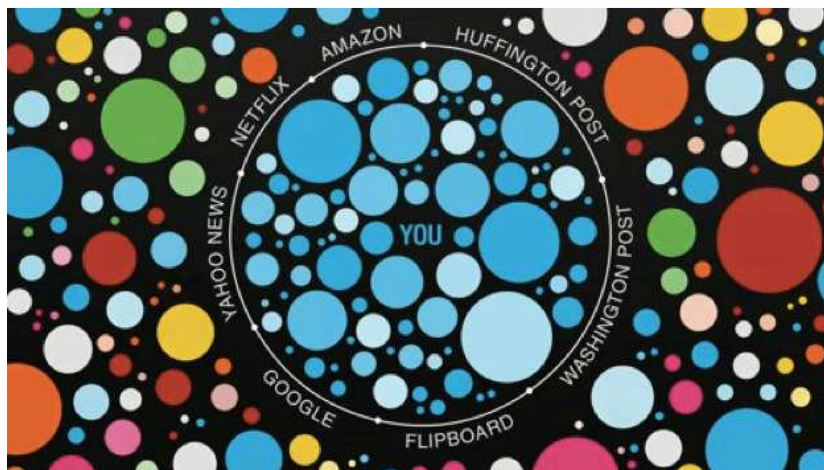
S trochou nadsázky může auto říci, že standardní Google již neexistuje a uživatele si toho nejsou vědomé, protože nevidí výsledky vyhledávání jiných lidí. To samé tvrzení jde přiřadit i k jiným společnostem, nejen ke Google a Facebook. Ostatní společnosti Yahoo News, Google News, Huffington Post, Washington Post, New York Times – všechny používají personalizaci. Všechny se vyvíjí ve směru personalizace. V současné době je tento trend ve začátcích, ale existuje velká pravděpodobnost toho, že brzy budou uživatelé dostávat pouze té údaje, které vyhledávač (sociální síť, informační portál, zpravodajství) poskytne, ale ne té, které opravdu potřebujeme. Tyto slova potvrzuje ex COO Google Eric Schmidt:

„Pro konzumenty, z určitého pohledu, bude velmi těžké zpracovat jakoukoli informaci, která není jakýmsi způsobem s ním spjata“ Eric Schmidt, Google

Ve své prezentaci Eli Pariser na TED2011 ukázal následující obrázek, který znázorňuje výsledek algoritmů personalizace a samotné filtry v celku.

³² PARISER, Eli. *The filter bubble what the Internet is hiding from you*. New York: Penguin Press, 2011. ISBN 11-015-0572-9.

³³ Pozn. Autora - Volný překlad



Obrázek č. 11 - Bublina filtrů (zdroj: Eli Pariser, TED2011)

Tato bublina filtrů je vesmír, ve kterém se nachází uživatelé, když brouzdají po internetu. Následně to, co se bude zobrazovat v této bublině filtrů, bude záviset na tom, kdo ti uživatelé jsou a čím se zabývají, tj. informace poskytovaná v rámci bubliny filtrů se bude skládat z profesionálních a soukromých zájmů. Z jednoho pohledu tento filtr dokáže v určitém smyslu ubránit jednotlivce před informační záplavou, pohled druhý už ale ve prospěch filtru nemluví – nejsou to samotné uživatelé, kdo rozhoduje o tom, jakou informaci dát do bubliny filtru a následně dostat. A co je ještě důležitější - neuvidí to, co zůstane mimo bublinu.

5 Technická a právní ochrana osobních údajů, porovnání situace v ČR, v Ruské federaci a v USA

V následující části autor přenáší pozornost na situaci s aktuálními zákony v České republice, Ruské federaci a ve Spojených státech amerických.

5.1 Česká republika

V případě České republiky se ochranou osobních údajů a celkově soukromí zabývá celá řada právních úprav jak tuzemských, tak i evropských. Soukromí obecně se definuje jako osobní oblast jednotlivce nebo skupiny. V češtině tento pojem do sebe zahrnuje hmotný a myšlenkový prostor jednotlivce a právo či schopnost zadržovat informace o sobě. V případě prostoru internetu pojem soukromí můžeme upřesnit jako schopnost uživatele nebo skupiny rozhodovat o přenosu informací o své osobě a zveřejňovat pouze některé z nich. Soukromí je někdy úzce spojeno s anonymitou, tedy přáním uživatele zůstat na internetu nepoznán.

Když bychom zmínily zpracování osobních údajů, pak nesmí dojít k porušení základních práv a svobod fyzické osoby, především je nutné zmínit článek 8 Evropské úmluvy o ochraně lidských práv a základních svobod, který zaručuje právo na soukromí³⁴.

Neméně důležitým právním předpisem je Úmluva č. 108 na ochranu osob se zřetelem na automatizované zpracování osobních dat, kterou přijala Rada Evropy 28. ledna 1981. „Účelem této Úmluvy je zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují (ochrana údajů)“³⁵.

Listina základních práv a svobod (dále jen „Listina“) jako součást ústavního pořádku České republiky, ve které je zakotveno i právo na ochranu osobních údajů. V čl. 7 Listina zakotvuje právo na nedotknutelnost osoby a jejího soukromí, v čl. 10 odst. 3 upravuje právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě a v čl. 13 stanoví, že nikdo

³⁴ Registry.cz [online]. 1994 - 2011 [cit. 2012-05-20]. Legislativní aspekty: Evropská unie. Dostupné z WWW: <<http://www.registry.cz/index.php?pg=legislativni-aspekty--evropska-unie>>.

³⁵ Úmluva č. 108 Hlava I článek 1

nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon; stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením³⁶. Příklady takového porušení se nachází nejen v kapitole 4.4 a 4.6 ve tvaru výčtu, ale jednotlivé případy autor zmiňuje skrze celou práci. Dále každému z nás náleží právo na ochranu před neoprávněným zasahováním do rodinného a soukromého života a před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě³⁷.

Základním právním předpisem upravujícím ochranu osobních údajů v České republice je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Účelem tohoto zákona je zajistit ochranu osobních údajů, způsob jejich zpracování v České republice a předávání osobních údajů do zahraničí, a upravit vztahy, které v souvislosti s nimi vznikají.

Zákon č. 101/2000 Sb. zakotvuje vymezení působnosti a pojmů, práva a povinnosti při zpracování osobních údajů, povinnosti osob, likvidaci osobních údajů, ochranu práv subjektů údajů, nápravu nemajetkové újmy či škody, předávání osobních údajů do jiných států. Na základě zákona dále dochází ke zřízení nezávislého Úřadu pro ochranu osobních údajů, úpravě jeho postavení, působnosti, organizace, činnosti kontrol či sankcionování. Úřad pro ochranu osobních údajů má kompetence správního úřadu. Vlivem mnoha technologických či vývojových změn byl tento zákon několikrát novelizován.

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci a fyzické a právnické osoby. Zákon se vztahuje na veškeré zpracování osobních údajů, tzn. na zpracovávání údajů automatizovaně či jinými prostředky.

Zákon se nevztahuje na zpracování osobních údajů, která provádějí fyzické osoby pro osobní potřebu. Jedná se o záležitosti týkající se zejména soukromého a rodinného života a nejsou určeny ke zveřejnění ani k podnikání (příkladem může být seznam různých výročí členů rodiny i širšího okruhu příbuzných). Zákon se ale naopak nevztahuje na nahodilé shromažďování osobních údajů za podmínky, že tyto nejsou

³⁶ Ochrana osobních údajů. BUSINESSINFO.CZ. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-opu-4637.html#b1>

³⁷ Zákon č. 2/1993 Sb., Listina základních práv a svobod

dále zpracovány. Nahodilé je opakem systematického. O nahodilé zpracování jde v případech, kdy údaje nejsou tříděny, pokud k jejich shromažďování nedává podnět správce, ale přichází zvenčí (např. nahodilý dotaz klienta u advokáta).

Zvláštní zákony stanoví zpracování osobních údajů pro účely statistické a archivnictví. Zde se nejedná o úplné vynětí z působnosti zákona o ochraně osobních údajů, ale jen o řešení otázky obecného a zvláštního zákona. Tedy pokud zákon o státní statistické službě nebo zákon o archivnictví a spisové službě obsahují zvláštní úpravu, má tato přednost před úpravou obecnou. Jestliže však takový speciální režim nebude, vztahuje se i na tyto případy zák. č. 101/2000 Sb. Podmínky zpracování osobních údajů pro účely statistické a archivnictví jsou tedy stanoveny příslušnými zákony, nestačí prohlášení správce, že si např. provádí statistické zjišťování nebo si vede archiv. Souhlas subjektu údajů není třeba také ke zpracování pro vědecké účely. Jakmile je to možné, musí být tyto údaje anonymizovány, tedy uvedeny do takové podoby, že je již nelze nikdy vztáhnout k subjektu údajů. Tyto údaje je též třeba náležitě zabezpečit proti jejich nelegálnímu použití.³⁸

Směrnice 95/46/ES

V současné chvíli je stěžejním dokumentem Evropské unie směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES ³⁹ (dále jen „Směrnice“) ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Směrnice 95/46/ES představuje na evropské úrovni referenční normu v oblasti ochrany osobních údajů. Zavádí právní rámec, jehož cílem je ustavení rovnováhy mezi vysokou úrovní ochrany soukromí jednotlivců a volným pohybem osobních údajů v rámci Evropské unie (EU). Za tímto účelem směrnice stanoví přísná omezení pro shromažďování a využívání osobních údajů a požaduje, aby byl v každém členském státě vytvořen nezávislý vnitrostátní subjekt pověřený ochranou těchto údajů. Tato směrnice se vztahuje na údaje zpracovávané automaticky (např. počítačové databáze zákazníků), jakož i na údaje, které jsou obsaženy v neautomatizovaném rejstříku nebo do něj mají být zařazeny (tradiční lístkové rejstříky).

³⁸ Ochrana osobních údajů. BUSINESSINFO.CZ. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-opu-4637.html#b1>

³⁹ EU. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: 13/sv. 15. 23.11.1995. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF>

Další právní předpisy upravující ochranu osobních údajů

Ochrana osobních údajů je zakotvena také v několika dalších zákonech.

- Občanský zákoník – na právní úpravu obsaženou v Listině navazují ustanovení zákona č. 40/1964 Sb., občanský zákoník, upravující ochranu osobnosti (viz § 11 a násl.).
- Obchodní zákoník – v zákoně č. 513/1991 Sb., obchodní zákoník, je upravena ochrana týkající se osobních údajů právnických osob. Jedná se zejména o ustanovení na ochranu obchodního tajemství (§ 17 a násl.). Proti porušení nebo ohrožení práva na ochranu obchodního tajemství přísluší podnikateli právní ochrana jako při nekalé soutěži upravená v ustanoveních § 53 až 55.
- Zákon č. 89/1995 Sb. o státní statistické službě – Ustanovení zákona (zejména § 16 až 18) upravují ochranu údajů, které od jednotlivých osob získávají Český statistický úřad (dále jen „ČSÚ“) nebo jiné státní orgány vykonávající státní statistickou službu.
- Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, která je povinna zabezpečit ochranu údajů (to se nedotýká jen ochrany osobních údajů ale i ostatních údajů, zvláště pak utajovaných informací) obsažených v evidencích před vyzrazením, zneužitím, poškozením, ztrátou a odcizením.

5.1.1 Evropa

V lednu roku 2012 Evropská komise vytvořila návrh Nařízení Evropského Parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), také pojmenovaný jako sušenkový zákon. V případě, že se tento návrh bude přijat jako směrnice, pak se bude postupovat stejným způsobem, jak se tomu dělo s nejvýznamnějšími směrnicemi pro ochranu soukromí uživatelů na webu. V případě, že se tento návrh bude přijat jako Nařízení, pak zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů České republiky pozbude platnosti. Dle odhadů by finální rozhodnutí mělo proběhnout v průběhu roku 2013 a v případě přijetí návrhu jako nařízení, pak by měl vejít v platnost po dvou letech.

Nejdůležitější změny, které tento Návrh přinese, tkví v následujícím:

- IP adresa a soubory cookies se budou považovat za osobní údaje (v současné chvíli se IP adresa jako osobní údaj považuje, tato skutečnost ale v zákoně není explicitně řečena)
- Každý subjekt údajů by měl mít právo na opravu osobních údajů, které se ho týkají, a „právo být zapomenut“
- Ve společnostech nad 250 zaměstnanců by se měli objevit povinní zmocněnci pro ochranu osobních údajů
- Narušení ochrany údajů se bude muset hlásit povinným zmocněncem do 24 hodin
- Povinný zmocněnec bude vést podrobnou dokumentaci o narušeních
- Vypracování mechanismů pro mezinárodní spolupráci mezi Komisí a orgány dozoru třetích zemí, zejména těmi, jejichž úroveň ochrany osobních údajů je považována za přiměřenou, a to s ohledem na doporučení Organizace pro hospodářskou spolupráci a rozvoj (OECD)

Předseda českého Úřadu pro ochranu osobních údajů Igor Němec osobně uvedl, že navrhované nařízení bude mít značný dopad nejen na společnosti, ale i na běžné uživatele. Nové nařízení by s sebou přineslo značné administrativní náklady. Kromě samotných personálních posil budou firmy například muset nakoupit hardwarovou infrastrukturu a software.

Shora zmíněný zákon vyvolává nesčetné množství sporů. Odpůrci tvrdí, že navrhované nařízení kvůli nadměrné zátěži může snížit konkurenceschopnost evropských firem, na které bude toto nařízení aplikováno. Společnosti, nacházející se mimo Evropu, budou ve výhodě, což může mít za dopad konec některých evropských společností, nebo jejich odchod do zahraničí. Některé odpůrci zpochybňují definici cookies jako osobního údaje. Až na několik výjimek odpůrci nového nařízení zastávají vedoucí pozice internetových společností nebo spolků reklamních agentur.

5.1.2 Vymezení pojmů souvisejících se zákonem o OOÚ

V této části jsou vyjmenovány a definovány nejdůležitější pojmy ze zákona o ochraně osobních údajů. Jelikož autor tyto pojmy dříve nerozpracovával, tak se podrobně

soustřeďuje se na veškeré drobnosti a rozdíly. Pojmy použité v zákonech o ochraně osobních údajů jsou založeny na článku 2 směrnice 95/46/ES ⁴⁰.

Osobní údaje a subjekt údajů

Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.

Pojem „osobní údaje“ je velice důležitý, protože zákony o ochraně osobních údajů se vztahují pouze na informace, které osobními údaji jsou. Ochranu jiných informací mohou stanovovat jiné právní předpisy. Osobní údaje tvoří soubor jednotlivých informací, které umožňují rozlišit příslušné subjekty údajů od jiných subjektů a kontaktovat je nebo poměrně jednoduše s nimi kontakt navázat a činit o subjektech údajů závěry, které je možné z takových údajů vyvodit. Při zpracování jsou tyto údaje považovány za osobní, pokud je možné z nich odvodit jejich vztah k příslušnému subjektu údajů.

Podnikatelé nejčastěji nakládají se základními informacemi o fyzických osobách, jako jsou jméno, příjmení, adresa, datum narození, identifikační číslo nebo jiné nejčastěji užívané údaje, které v každodenních situacích sdělujeme. Legislativa o ochraně osobních údajů neobsahuje kompletní seznam kategorií údajů, jelikož by vzhledem k šíři pojmu osobní údaj nebylo možné takový seznam vytvořit.

Citlivé údaje

Citlivými údaji se rozumí údaje, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost a údaje týkajících se zdraví nebo sexuálního života. Údaje týkající se protiprávního jednání, rozsudků v trestních věcech nebo bezpečnostních opatření, údaje týkající se správních sankcí nebo rozsudků v občanských věcech mohou mít podobný status.

Citlivé údaje zahrnují údaje, které označují etnický původ, údaje týkající se odsouzení za trestný čin, genetické a biometrické údaje, pokud umožňují přímou identifikaci nebo autentizaci subjektu údajů. Při aplikaci zákona je třeba brát v úvahu následující:

- Informace týkající se členství v politické straně jsou považovány za citlivé údaje, které odhalují politické názory nebo postoje

⁴⁰ *Ochrana osobních údajů: vybrané otázky: příručka pro podnikatele*. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011, 50 s. ISBN 978-80-210-5572-8.

- Za citlivé údaje se mohou také považovat údaje o odsouzení za trestný čin (záznam trestního rejstříku), toto platí, pokud existuje pravomocný odsuzující rozsudek
- Biometrické údaje lze obecně chápat jako údaje o měřitelných či objektivně klasifikovatelných parametrech lidského těla. Zákon o ochraně osobních údajů však vyžaduje ještě jedno kritérium, a sice možnost na základě těchto údajů někoho přímo identifikovat (pro ilustraci lze tedy říci, že se velikost nohy za citlivý údaj nepovažuje, ale otisk prstu ano)

Zpracování osobních údajů

Zpracováním osobních údajů (zpracování) se rozumí jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uschovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace.

Zpracování může být provedeno jednou nebo opakovaně. Je důležité mít na paměti, že i jednorázový úkon s osobními údaji, například jejich sdělení, je považován za zpracování. Nejběžnější úkony, které jsou považovány za zpracování osobních údajů, jsou focení, zvukové nebo obrazové zaznamenávání, stejně jako zaznamenávání fyzických charakteristik jednotlivce použitelných k osobní identifikaci (například otisky prstů, otisky dlaní, vzorky DNA a obrazy duhovky). Uschovávání osobních údajů je také považováno za zpracování. Technické zpracování osobních údajů je zvláštní formou zpracování. Skládá se z provádění technických úkonů souvisejících s úkony zpracování osobních údajů, bez ohledu na použité metody či prostředky nebo místo aplikace.

Soubory osobních údajů

Souborem osobních údajů (rejstřík) se rozumí jakýkoli uspořádaný soubor osobních údajů přístupných podle určených kritérií, ať již je tento soubor centralizován, decentralizován nebo rozdělen podle funkčního či zeměpisného hlediska.

Možnost vyhledávat podle určitých osobních kritérií (jméno, příjmení, datum narození, identifikační číslo) nebo neosobních kritérií (den vložení dat do souboru).

Typickým příkladem souboru dat (rejstříku) u podnikatelů jsou osobní záznamy zaměstnanců shromážděné v souvislosti s jejich zaměstnáním a prací, kterou vykonávají. Do této kategorie patří také databáze spotřebitelů. To platí bez ohledu na to, zda mají elektronickou nebo tištěnou podobu. Do této kategorie hlavním způsobem

spadají i vytvářené profily uživatelů internetu. Soubor vlastností definujících pohlaví, národnost, věk, záliby jsou ty pseudo-anonymní, decentralizované. Následně dobrovolně sdílené uživatelem údaje jako jméno, příjmení, datum narození, emailová adresa a všudypřítomná IP adresa jsou spojována datovými agregátory do centralizovaných souborů osobních údajů.

Správce

Správce se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů.

Správce rozhoduje o účelu a prostředcích zpracování osobních údajů a nese odpovědnost za zpracování osobních údajů a za jeho kontrolu. Správce mohou být veřejné orgány, orgány místní samosprávy, podnikatelské subjekty nebo fyzické osoby provozující ekonomickou činnost, pokud rozhodují o účelu a prostředcích zpracování osobních údajů.

Zpracovatel

Zpracovatelem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce.

Správce nemusí sám vykonávat veškeré úkony spojené se zpracováním osobních údajů. Může pověřit jiný subjekt, aby prováděl celé nebo jen část zpracování osobních údajů. Zpracovatel se nestává správcem údajů, jejichž zpracováním byl pověřen. Skutečnost, že subjekt pověřený zpracováním osobních údajů se nestává jejich správcem, s sebou nese konkrétní důsledky. Povinnosti uložené zákonem správci, například povinnost registrace, se na zpracovatele nevztahují. Také zpracovatel je však povinen osobní údaje chránit.

Aplikací pojmů Správce a Zpracovatel na sektor, kterým se zabývá tato diplomová práce, vzniká jasný obrázek serverů, popsaných ve čtvrté kapitole, a jejich zjevná porušování legislativy.

Třetí osoba

Třetí osobou se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt jiný než subjekt údajů, než správce, než zpracovatel a než osoby přímo podléhající správci nebo zpracovateli, které jsou oprávněny ke zpracování údajů.

Příjemce

Příjemcem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo

jakýkoli jiný subjekt, kterému jsou údaje sdělovány, ať se jedná či nikoli o třetí osobu; orgány, které mohou získávat údaje v rámci zvláštního šetření, však nejsou považovány za příjemce.

Aby měly subjekty údajů zajištěnou možnost kontrolovat svá osobní data, má správce osobních údajů povinnost informovat je o tom, kdo jsou příjemci osobních údajů, které zpracovává.

Souhlas subjektu údajů

Souhlasem subjektu údajů se rozumí jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování.

Znamená svobodně udělený, výslovný a vědomý projev vůle subjektu údajů, kterým vyjadřuje nezpochybnitelný souhlas s částečným nebo úplným zpracováním svých osobních údajů. Takový souhlas je možné zrušit. Souhlas s použitím osobních údajů může být poskytnut písemně.

Opt in / opt out

Tyto dva pojmy opt-in a opt-out vyjadřují dvě základní stanoviska v oblasti získávání souhlasu jednotlivců pro zpracování jejich osobních údajů.

Opt out pravidlo – znamená, že nevyjádřím-li výslovný nesouhlas (např. s využitím svých údajů k marketingovým účelům), platí automaticky můj souhlas, tj. „od čeho se neodhlásím, to dostávám“.

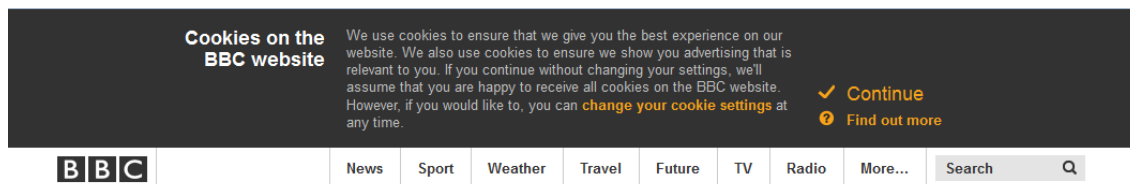
Opt in pravidlo – znamená, že nevyjádřím-li svůj výslovný souhlas, platí automaticky můj nesouhlas, tj. „k čemu se nepřihlásím, to nedostávám“⁴¹.

Dle aktuálně platné směrnice 95/46/ES a zákona České republiky č. 101/2000 Sb. stále platí pravidlo Opt out, to znamená, že ve všech státech Evropské Unie uživatel musí vyhledat v nastaveních webu sekci pro ochranu osobních údajů a ukládání cookies zakázat. Drtivá většina internetových stránek tyto možnosti nemají, proto je technicky nemožné se odhlásit od behaviorálního sledování. Výjimku tvoří Velká Británie.

Ve Velké Británii sušenkový zákon již byl zahrnut do místní zákonné úpravy a webové servery registrované na jejím území musí svým návštěvníkům podat vysvětlení o tom, z jakého důvodu se na koncové zařízení stahují cookies, k čemu slouží konkrétní druh cookies a v případě zájmu uživatel může stahování cookies povolit.

⁴¹ Slovníček nejdůležitějších pojmů. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.uoou.cz/uoou.aspx?menu=281&loc=455>

Když bychom vzali za příklad internetové stránky bbc.co.uk, tak návštěvníci z Velké Británie vidí nabídku pro povolení ukládání cookies, kdežto návštěvníci z jiných zemí vidí mezinárodní verzi tohoto webu.



Obrázek č. 12 - Příklad opt-in v praxi (zpracování: autor, zdroj: BBC UK)

5.2 Ruská federace

Vyčlenění kategorie osobních údajů z obecnější kategorie soukromého života je v Ruské federaci spojeno nejen s šířením automatizovaného zpracování a ukládání dat, a to zejména do počítačových databází, které jsou přístupné na dálku prostřednictvím technických komunikačních kanálů, ale i značné demokratizaci státu.

Ochrana soukromého života osoby z ústavního a legislativního hlediska v moderním Rusku je na docela dobré úrovni. Stačí uvést článek 23 a 24 Ústavy RF⁴², které zaručují právo na soukromý život, osobní a rodinné soukromí a soukromí korespondence, telefonních hovorů, telegrafních a další druhů zpráv. Rovněž, první část článku 24 Ústavy RF obsahuje nařízení, které uvádí, že „shromažďování, uchovávání a šíření informací o soukromém životě člověka bez jeho nebo jejího souhlasu není povoleno.“⁴³ Toto nařízení je zásadní a má fundamentální povahu, určuje význam a obsah velkého množství právních a správních předpisů různých úrovní, svědčí o přechodu státního režimu na cestu budování demokratické společnosti, v níž hlavní hodnotou je člověk. Lze s jistotou říci, že v současné době Ruská federace na této cestě čelí řadě problémů, mezi něž patří otázka zabezpečení ochrany soukromé sféry každého občana.

Vývoj problému vyvolává samozřejmou potřebu ve spolehlivé ochraně informačních zdrojů a procesů a uspořádání veřejných vztahů v této oblasti. Rusko se teprve začíná rozvíjet a zavádět do legislativní a exekutivní oblasti integrovaný přístup k ochraně osobních údajů. V tomto ohledu je důležité, aby daný přístup pokrýval celou řadu problémů, aby nebyl omezen pouze na posouzení jen jejich technických složek.

⁴² Ruská federace. Konstituce Ruské federace: Práva a svobody osob a občanů Ruské federace. In: FZ 2. Dostupné z: <http://www.gov.ru/main/konst/konst12.html>

⁴³ Ruská federace. Konstituce Ruské federace: Práva a svobody osob a občanů Ruské federace. In: FZ 2. Dostupné z: <http://www.gov.ru/main/konst/konst12.html>

Je třeba poznamenat, že zákonodárci během posledních desetiletí nenechali bez pozornosti nově vznikající informační prostředí a přijali řadu právních předpisů, mezi něž patří federální zákon „O informacích, informatizace a ochraně informací“, federální zákon „O účasti v mezinárodní výměně informací“, zákon „O osobních údajích občanů“. Ochrana osobních údajů pracovníků je popsána ve 14 kapitole zákoníku práce RF. Taktéž byly přijaté mezinárodní standardy bezpečnosti ISO 17779⁴⁴ a standardy správy dokumentů dle ISO 15489⁴⁵.

Federální zákon 152-FZ o Osobních údajích

Dne 27. července 2006 Ruská federace přijala zákon týkající se ochrany osobních údajů. Hlavní pohnutkou pro tento krok sloužila skutečnost krádeže i rozšiřování vládních databází finančních úřadů, rejstříku vozidel, policejních záznamů o jednotlivcích a jiných databází s citlivými údaji, které se prodávaly na nosičích nebo byly volně ke stažení na internetu. Jiným důvodem pro přijetí tohoto zákona byla nutnost sladit právní úpravu s Evropskou unií pro bezproblémový chod spolupráce na různých projektech, kde se předávají osobní údaje, a kde nesoulad v právních úpravách byl překážkou.

Federální zákon RF 152-FZ „O osobních údajích“ je zaměřen na ochranu práv a svobod jednotlivců při zpracování jejich osobních údajů, včetně práva na osobní a rodinné soukromí. Během posledních 6 let zákon procházel novelizacemi. Poslední změny byly provedeny 25. července 2011 prostřednictvím zákona N 261-FZ, v němž byl upřesněn rozsah federálního zákona, jeho základní pojmy, zásady a podmínky pro zpracování osobních údajů. Došlo i k podstatnému přepracování stávajících právních předpisů o přeshraničním převodu osobních údajů⁴⁶.

V souladu se zákonem se v Rusku zvyšují nároky a zpřísňují se požadavky na veškeré veřejné a soukromé společnosti a organizace a na fyzické osoby, které shromažďují, uchovávají, přenášejí nebo zpracovávají osobní údaje.

Přijetí federálního zákona "O osobních údajích" bylo reakcí zákonodárné moci na jeden z nejnaléhavějších problémů moderního Ruska - nekontrolovaná cirkulace soukromých

⁴⁴ Standard poskytuje poradenství v oblasti postupu řízení informační bezpečnosti pro ty, které jsou zodpovědní za vytvoření, realizaci a managementu informační bezpečnosti

⁴⁵ Standard reguluje správu dokumentů na všech nosičích v jakémkoliv formátu a vyžaduje vytvoření lokálních (interních) normativních dokumentů organizace

⁴⁶ Ruská federace. Federální zákon o ochraně osobních údajů. In: N-152FZ. 2006. Dostupné z: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=117587>

informací občanů, nedostatek respektu k osobním údajům obecně, a všudypřítomnost osobních záznamů Rusů formou databází. Lze konstatovat, že FZ má velký společenský význam.

Podle výzkumu holdingu ROMIR Monitoring, který se konal v lednu 2006 dle žádosti „RIO-Center“, ruští občané zcela podporují legislativní iniciativu orgánů. Například, pouze 3,4% respondentů věří v bezpečnost svých osobních údajů, a opačný názor - jistota v naprostém nezabezpečení jejich soukromých informací - má 24,4% občanů. Zatímco 74,1% respondentů podporuje nekompromisní boj proti šíření pirátských kopií provozních databází policie a 63,3% občanů věří, že stát je povinen sledovat shromažďování osobních údajů pro komerční subjekty. Autor si dovoluje podtrhnout ten fakt, že tato studie byla založena na reprezentativním vzorku 1600 občanů s trvalým pobytem ve 43 subjektech Ruské federace. Jinými slovy, je zřejmé, že již jen ze sociálního hlediska, je již dávno zapotřebí právní regulace sběru a zpracování osobních údajů občanů země.

Nehledě na shora zmíněné mnozí odborníci považují zákon „O osobních údajích“ za příliš obecný. Danou oblast je nutné lépe a hlouběji propracovat se zaměřením na mezinárodní praxi a jasnou segmentaci pro konkrétní trhy ⁴⁷. Tento zákon je směřován na zajištění ochrany práv a svobod jednotlivců při zpracování jejich osobních údajů a zároveň ochrany nedotknutelnosti osobního života a osobního a rodinného tajemství. V souladu se zákonem 152 FZ společnosti musely modernizovat systémy zpracování osobních údajů (spuštěné do 1. ledna 2010) do 1. července 2011. Nehledě na to do současné chvíle okolo poloviny společnosti ještě nezískaly licenci správce osobních údajů, což může vyvolat zákonnou odpovědnost.

Pojmy

Z důvodů stejných pramenů evropské a ruské právní úpravy zákonů týkajících se ochrany osobních údajů (Konvence Rady Evropy „O ochraně osobních údajů při automatizovaném zpracování“) pojmy uvedené v zákoně 152 FZ Ruské federace jsou velmi podobné těm, uvedeným v 101/2000 Sb. Nicméně jsou patrné i některé rozdíly. Ten nejnapadnější se týká popisu citlivých údajů. Zákon nedefinuje pojem Citlivých údajů, ale zahrnuje popis parametru citlivých údajů do kategorie Osobních údajů.

⁴⁷ KOROLYUK, Alexey. Experti tvrdí: "Zákon o osobních údajích musí být dopracován". [online]. 2011 [cit. 2012-12-08]. Dostupné z: <http://internet.cnews.ru/news/line/index.shtml?2011/06/30/445794>

Zákon 152 FZ také definuje pojem jako transhraniční předání osobních údajů, který ale platí pouze pro předání osobních údajů do jiných států správcem, registrovaným na území Ruské federace. Z čehož vyplývá, že zákon nepokrývá situaci online sledování uživatelů americkými servery.

5.3 Spojené státy americké

Soukromí a ochrana osobních údajů jsou ve Spojených státech regulované jinak, než v Evropské unii. Evropská unie dohlíží na privátní sektor užívající osobní údaje centrálně, kdežto regulace soukromého sektoru ve Spojených státech je minimální. Tyto rozdíly vychází z rozdílných koncepčních základů pro soukromí v každé jurisdikci. Ve Spojených státech ochrana soukromí je v podstatě ochranou svobody, to jest ochranou před vládou. Tento nedokonalý postoj naprosto nezastřešuje problematiku ochrany osobních údajů, kdy je třeba alespoň v rozumné míře kontrolovat činnost internetových společností pomocí vytvořeného rámce vymezujícího základní pojmy, týkající se ochrany osobních údajů.

Právní rámec pro soukromí ve Spojených státech je poněkud rozladěný a rozkouskovaný. Opatření týkající se soukromí existují v obecném právu, v konstitucích federálních a jednotlivých států, a následně v různých stanovách vytvořených pro specifické problémy, které vznikly v jiných sektorech a jurisdikcích. Ve srovnání s příkladem Evropské unie, obecné právo a ústavní ochrana pro ochranu soukromí je ve Spojených státech poněkud nepředvídatelné. V důsledku toho, je těžké artikulovat jakoukoliv souhrnnou právní teorii s ohledem na soukromí.

Soukromí fyzického prostoru či věcí všeobecně dostává silnou ochranu pomocí práva zajišťujícího soukromí jako takového. Nicméně zákony, zastřešující ochranu soukromí nejsou vhodné pro aplikaci na porušování ochrany osobních údajů v prostoru internetu, pokud údaje nebyly vzaty silou přímo od poškozeného, nebo z jiného soukromého zdroje, například z jeho čísla účtu v bance. Zatímco konstituce chrání osobní údaje proti proniknutí vlády, zájem o vytvoření právního rámce, který by chránil osobní údaje v prostředí internetu, se nezdá být velký. Stanovy vyplnily v mnoha případech nedokonalosti obecného a ústavního práva, ale kvůli jejich úzké aplikaci, absenci jednotného rámce a v některých případech i právním kolizím, dopad se nejeví být značným. Po jisté stránce legislativní úpravy jednotlivých států byly nejslibnější místem pro nové právní úpravy zajišťující ochranu soukromí, ale jejich účinnost je ohraničena kvůli omezením jurisdikcí a slabými schopnostmi prosazení. Tento rozkouskovaný

přístup je stále více problematický v prostředí, v kterém informační technologie expandují rychle a ovlivňují mnoho oblastí zákonů na ochranu soukromí. Reaktivní, přizpůsobivý proces přijatý americkými soudy dělá domáhání ochrany osobních údajů velmi obtížným. Celkem vzato, diskutovaná legislativa Spojených států poskytuje občanům větší ochranu proti shromažďování a zpracování osobních údajů vládou, než soukromým odvětvím. Významné je to, že evropská směrnice o soukromí (95/45/EC) pomoci stanovených limitů a pravidel řídí interakce na trhu. Spojené státy jsou méně ochotné pro ukládání vládních omezení na soukromá odvětví, a spíše spoléhá na omezení tržní. Tato situace zřejmě odráží tradiční nedůvěru Američanů v centralizovanou vládu. Následně se podíváme na existující právní úpravy, které alespoň nějakým způsobem zastřešují ochranu osobních údajů.

Zákon o soukromí z roku 1974

Tento zákon je jediný souhrnný federální zákon, který chrání informační soukromí. Tento zákon o soukromí platí pouze pro zpracování dat federální vládou, ale nikoli vládami jednotlivých států nebo soukromým sektorem. Tento zákon zavazuje státní orgány k tomu, aby sbíraly minimální množství informace a pokud možno přímo od jedince, kterého se tato informace týká, uchovávaly pouze příslušnou a nezbytnou informaci, udržovaly postačující a kompletní záznamy, a poskytovaly jednotlivcům oprávnění přístupu pro zhodnocení a opravy jejich záznamů, a také definovaly záruky bezpečnosti těchto informací.

Absence konstituční úpravy ochrany osobních údajů a soukromí

Absence definovaných konstitucí práv na soukromí (zvláště vzhledem k jejich existenci v několika konstitucích států) dává důvody ke značnému znepokojení a to ihned ze dvou hledisek. První je to, že precedenční přístup Spojených států bude neustále obnovovat již existující zásady, nebo nové zásady budou v rozporu s již existujícími - bude docházet ke střetu. Následkem toho, tyto zákony a jejich účinnost při ochraně soukromí buď bude klesat, nebo bude nulová. Druhý je to, že konstituce Spojených států nebude poskytovat adekvátní ochranu soukromí, zvláště vzhledem k trvalému technickému rozvoji.

Návrh zákona o ochraně soukromí online (OPPA)

Tento návrh existuje od května roku 2010. Návrh zákona o ochraně soukromí online nabízí principiální a jednotný přístup k ochraně osobních údajů ve Spojených státech. Tato zákonná úprava včleňuje principy poctivé informační praxe (FIP) které jsou srovnatelné s evropskými principy ochrany soukromí. Návrh zákona o ochraně

soukromí online měl potenciál být stejně efektivní jako evropské zákony o ochraně osobních údajů. Nicméně tento zákon o soukromí slábl s každou novou změnou a jejím návrhem v kongresu Spojených států, a to hlavně výměnou rozsahu definice osobních údajů. Aktuální koncept, například, do definice osobního údaje zahrnuje informace jako jméno, adresa, emailová adresa, telefonní číslo a číslo sociálního zabezpečení. Předchozí koncepty zahrnovaly dodatečnou osobní informaci, jako zdravotní informace, finanční informace, etnický původ, rasa, politické názory a sexuální orientace. Taková "citlivá" osobní informace, v aktuálním konceptu chybí, což dělá tento návrh neodpovídajícím úrovni evropského zákona.

5.4 U. S. – EU Safe Harbor

Směrnice evropské komise zabývající se ochranou dat, která vstoupila v platnost v říjnu 1998 (95/45/EC), zakazuje přenos osobních dat do zemí mimo Evropskou unii, které nespĺňují požadavky směrnice. Spojené státy a EU sdílejí stejný cíl zvyšování ochrany soukromí pro jejich občany, ale Spojené státy mají jiný přístup k soukromí než je ten evropský. Spojené státy užívají sektorový přístup, který spoléhá na rámec, do kterého je zapojena legislativa, nařízení, a samoregulace. Kdežto EU spoléhá na komplexní zákonný systém který vyžaduje, kromě jiného, vytvoření nezávislých vládních orgánů pro ochranu dat, registraci databází těchto orgánů, a v některých případech vyžadují schválení před samotným zpracováním osobních údajů. Následkem těchto rozdílů, směrnice by mohla významně komplikovat schopnost zapojení amerických společnosti do trans-Atlantických vztahů.

Za účelem překonání těchto rozdílů a poskytnutí usměrněných a efektivních prostředků americkým firmám pro dosažení potřebné úrovně, stanovené v evropské směrnici, Ministerstvo obchodu Spojených států po konzultacích s Evropskou komisí vyvinula rámec "bezpečný přístav" (Safe harbor). Evropsko-americký rámec Safe harbor, který byl schválen Evropskou Komisí v roce 2000, je důležitou cestou pro americké společnosti v předcházení přerušování jejich obchodních činnosti s EU. Také tento rámec jakýmsi způsobem předchází případným žalobám ze strany úřadů členských států EU, které jsou pod záštitou zákona o ochranu soukromí. Certifikace podniku v souladu s rámcem Safe harbor hovoří o souladu jeho vlastnosti s požadavky, které pokládá evropská směrnice.

Rozhodnutí americké společnosti o zapojení do programu Safe harbor je dobrovolné. Pro vstup do tohoto programu společnost musí přivést vlastní politiku ochrany soukromí

k takovému stavu, kdy bude vyhovovat požadavkům shora zmíněného rámce a rovněž požadavkům evropské směrnice (95/45/EC). Pro získání nebo prodloužení certifikátu společnost se musí jednou ročně podrobit kontrole vlastními pracovníky a vydat potvrzení o souladu se zásady programu Safe harbor, které zahrnují následující:

Oznámení

Organizace musí informovat jednotlivce o účelech, pro které jsou sbírány a užívány jejich data. Společnost musí poskytovat informaci o tom, jak jednotlivce mohou kontaktovat organizaci - s jakýmikoliv dotazy či stížnostmi, o tom jakým třetím stranám se data o uživatelích odesílají.

Volba

Organizace musí dát uživatelům možnost výběru (opt out), zda jejich osobní údaje budou odeslány třetím stranám nebo užívána pro účel neslučitelné s účely pro které byly původně shromažďovány nebo následovně oprávněný jednotlivcem. Pro sdílení citlivých informací třetím stranám nebo využití osobních údajů za jiným účelem než byly shromažďovány se společnost musí dotázat pro výslovný souhlas (opt in).

Další přenos (Přenos třetím stranám)

Pro zveřejnění informací třetí straně, organizace musí přenos oznámit uživateli a zajistit to, že třetí strana je také zapojena do programu Safe harbor. Jinou možností je získání čestného prohlášení třetí strany o tom, že splňuje veškeré náležitosti, stanovené v programu Safe harbor.

Zpřístupnění

Uživatele musí mít přístup k jejich osobním informacím , které společnost shromažďuje a musí být schopen opravit, zlepšit, nebo vymazat informaci , která je nepřesná.

Bezpečnost

Organizace musí učinit rozumná opatření pro ochranu osobních údajů. Nesmí dojít k jejich ztrátě, nesprávnému použití, neoprávněnému přístupu, odhalení, změně či zničení.

Datová integrita

Osobní informace musí být relevantní k účelům, pro které jsou shromažďována. Společnost by měla podniknout rozumné kroky pro zajištění odpovídajícího zacházení s daty, jejich přesnost, kompletnost a aktuálnost.

6 Porovnání situace ve výše uvedených zemích, jejich vyhodnocení a doporučení pro zlepšení situace v ČR

V této kapitole si autor vytýčil za cíl porovnání právních úprav, politik společnosti a vyvození jakéhosi objektivního obrázku, obecného pohledu na situaci s osobními údaji. Tuto situace autor vidí obrazně jako rovnováhu, kde na straně jedné je uživatel, na straně druhé jsou soukromé společnosti, které generují zisk díky osobním údajům, a zákony jednotlivých států, které se nachází někde uprostřed.

Česká republika, jak již bylo řečeno výše, se v otázce ochrany osobních údajů řídí směrnicemi Evropské unie. Pokud bude přijato nařízení „Sušenkový zákon“, o kterém autor taktéž pojednával v dřívější kapitole, pak vztah právní úpravy České republiky nejenže bude velmi těsný – budou jednotné, proto ve svých úvahách autor spíše hovoří o právní úpravě EU, nežli České republice.

První věci, kterou je nutno zmínit ihned na začátku je to, že evropská právní úprava ochrany osobních údajů je pramenem pro federální zákony Ruské federace. Nehledě dále na rozdíl v právních systémech Evropy (kontinentální) a Spojených států (angloamerický), poslední taktéž následuje směr vývoje právních úprav Evropy.

Věci druhou je lokace společností Facebook, Google a jiných. Díky technologickému pokroku, minimální regulaci ze strany státu a nesčetného množství dalších faktorů shora zmíněné společnosti mají svá sídla ve Spojených státech a pouze některé výjimky mají registrované pobočky na území Evropské unie.

6.1 Porovnání a vyhodnocení

Jak již bylo zmíněno dříve v textu této práce společnosti Facebook a Google mají svá sídla v Irsku. Auto si dovoluje tvrdit, že tomu tak je z více důvodů, ale hlavním důvodem jsou daňové výhody lokalizace pobočky společnosti v této zemi ⁴⁸. Zpráva Bloomberg hovoří o snížení odváděných daní společnosti Google o \$3.1 miliard za roky 2007 až 2010. Ta skutečnost, že sídla shora zmíněných společností se nachází na území EU, jednoznačně hovoří o tom, že poskytované služby a podmínky užití musí být v souladu s právní úpravou, týkající se ochrany osobních údajů EU. Společnost Facebook ve svém prohlášení to dokonce i konstatuje.

⁴⁸ DRUCKER, Jesse. Bloomberg. Google 2.4% Rate Shows How \$60 Billion Lost to Tax Loopholes. [online]. 2010 [cit. 2012-12-08]. Dostupné z: <http://www.bloomberg.com/news/2010-10-21/google-2-4-rate-shows-how-60-billion-u-s-revenue-lost-to-tax-loopholes.html>

19. Ostatní

1. Pokud jste občanem USA nebo Kanady nebo máte v těchto zemích svou hlavní pobočku, představuje toto Prohlášení smlouvu mezi vámi a společností Facebook, Inc. V ostatních případech je toto Prohlášení smlouvou mezi vámi a společností Facebook Ireland Limited. Pojmy „nám“, „my“ a „naše“ označují společnost Facebook, Inc. nebo Facebook Ireland Limited, podle příslušnosti.
2. ...

Následně se vyžaduje souhlas od uživatele o tom, že jeho údaje se budou přenášet a zpracovávat ve Spojených státech amerických.

17. Zvláštní ustanovení pro uživatele mimo Spojené státy americké

Usilujeme o vytvoření globální komunity s konzistentními standardy pro všechny, avšak současně respektujeme místní zákony. Pro uživatele a osoby, které nejsou uživateli a využívají službu Facebook mimo území Spojených států amerických, platí následující ustanovení:

1. Souhlasíte s přenesením a zpracováním svých osobních údajů ve Spojených státech amerických
2. ...

Jelikož Facebook je účastníkem programu Safe Harbor, tento přenos není ilegální, ale otázkou zůstává, jestli Facebook splňuje veškeré požadavky, které se kladou na jednotlivé účastníky tohoto programu. Kdyby tomu tak ale bylo, pak by nedocházelo k nárůstu stížnosti na Facebook u orgánů pro ochranu osobních údajů v Irsku.

Celkově situace se zásadami ochrany osobních údajů je velmi nevyvážená. Z jedné strany je uživatel, který je nucen souhlasit s podmínkami společnosti, například pokud jeho škola využívá takové moduly jako Google kalendář a je nucen pro zjištění rozvrhu být zaregistrován a přihlášen.

Ze strany druhé tyto podmínky svým samotným obsahem porušují zákony EU v nesčetném množství případů. Situace se stává o to složitější, když budeme hovořit o případech sledování na webu uživatelů, které nejsou, ani nebyly registrované na stránkách Google nebo Facebook, ale servery těchto stránek systematicky shromažďují, zpracovávají a využívají/prodávají osobní data za účelem generování zisku. Vše

⁴⁹ Facebook: Prohlášení o právech a povinnostech. FACEBOOK, Inc. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.facebook.com/legal/terms>

zmíněné je hrubým porušováním směrnic a nařízení EU a zákonů RF, týkajících se ochrany osobních údajů.

Samotná ujednání v sobě hlavně obsahují kromě velkého množství dat, které můžou provozovatele služeb shromažďovat, ještě tvrzení o tom, že shromažďovaná data se nepřisuzují k určité osobě. Toto tvrzení ale žádným způsobem nemůže být potvrzeno už jen kvůli zaznamenávání IP adresy (jak DoubleClick, Google Analytics atd), kterou evropské právní úpravy vyhodnocují jako osobní údaj.

Ještě větším rizikem pro soukromí je absence jakýchkoliv nástrojů kontroly toho, komu jsou shromažďována data předávána. Problémem pro soukromí je snadná těžba dat datovými agregátory z různých zdrojů, jejich následné vyhodnocení a vytváření profilů na základě výše zmíněné IP adresy (a nejen) na jednotlivce, které mohou obsahovat velmi podrobné a přesné údaje, mezi kterými se mohou objevit i údaje citlivé – a to z pohledu evropské právní úpravy.

Dalším velkým dotazníkem v tomto tématu je vymahatelnost. Jelikož data o uživateli putují do Spojených států, Evropská unie a Ruská federace nemají k dispozici žádné reálné a účinné nástroje. Společnosti nechtějí jít proti regulátorům v tom smyslu, že se chtějí vyhnout zveřejnění negativního stanoviska například WP27⁵⁰ o nedodržení pravidel a zákonů EU. Jakákoliv zmínka o nedodržování principů ochrany osobních údajů je pro společnosti zničující. Dle názoru autora toto bylo dalším důvodem pro vytvoření pobočky v Irsku, která by navenek jednala s orgány EU a vyvíjela snahu o zajištění odpovídající úrovně ochrany osobních údajů.

Česká republika a Evropská unie

Na začátku této práce (2. kapitola) autor uváděl základní ekonomická fakta o předních společnostech ve Spojených státech. Jejich obraty a tržby, jejich náklady na inovace a vývoj, jejich lidský kapitál a patenty nedávají velké šance pro to, aby úřady Evropské unie byly schopné bez přiměřeného odstupu sledovat jejich technologický vývoj. Úřady neodráží skutečný stav vývoje technologií. Právní úprava je pozadu moderního pokroku. Dalším problémem je samotná podstata internetu, která v sobě nese značnou volnost a určitý podíl nevymahatelnosti.

Nehledě na negativní pasáže se Evropa ukázala být lídrem v ochraně soukromí jednotlivce v digitálním věku. Velká část praktik při shromažďování prodeje a

⁵⁰ Pracovní skupina 27

předávání osobních údajů, které na denním pořádku ve Spojených státech a dalších zemích jsou v Evropě nezákonné. Někteří američtí pozorovatelé se dívají směrem k ustanovením EU s obdivem a doufají, že Američané sečtou za vhodné přijmout alespoň některé z přístupů ochrany spotřebitele proti invazi do jejich soukromí, nyní tak běžné v dnešním obchodním prostředí. Přestože jsme se zaměřili na ochranu osobních údajů, je třeba připomenout, že EU není pozadu ani v oblasti ochrany soukromí obecného, myšleno soukromí jako lidského práva, které je vyjádřeno evropské Úmluvě o ochraně základních lidských práv a svobod.

Evropští spotřebitelé by měli být opravdu vděční za komplexní standardy ochrany osobních údajů. Přestože nejsou dokonalé, jsou nesrovnatelně dál, než právní úpravy Spojených států.

USA

Američané si velmi cení vlastní svobodu. Jejich touhou je minimalizace vlivu vlády do interakce mezi jednotlivými občany. Toto je koncepční podpora aktuálního stavu ochrany soukromí zákonného systému v US. Američané věří tomu, že jestli vláda zanechá prostor internetu a týkající se sektor trhu bez dozoru, pak se o sebe bude schopen postarat sám. Otázkou je, jestli tento postoj zastává opravdu většina občanů Spojených států, nebo jestli to jsou zprávy, rozšiřované lobbisty vedoucích společností trhu.

Obrázek zachycující celkovou situaci v oblasti ochrany osobních údajů ve Spojených státech je velmi fragmentovaný. US Federal Trade Commission vydává pokyny a doporučení a hraje pouze donucovací roli. S použitím průmyslových a samoregulačních, odvětvově specifických norem (pro finance, dětská práva, federální orgány a zdravotní péči) a pravidel na státní úrovni, neexistuje žádný orgán, který by se zabýval pouze ochranou osobních údajů, vydával odpovídající zákony s obsahem odpovídajícím současné situaci.

Američtí obráncové soukromí vzhlížejí k evropskému kontinentu s úctou a tvrdí, že přístup Evropy je velmi kreativní. Evropské zákony na ochranu soukromí je viděné jako "poslední, nejlepší naděje" pro rozšíření sektoru ochrany soukromí občanů Spojených států, a obráncové soukromí v Americe vyzývají vládu k tomu, aby následovala a napodobovala Evropu. doposud Spojené státy neukázaly žádnou snahu o posun směrem k vytvoření souhrnné legislativy nebo odpovědného orgánu, obdobnému těm z EU, který by se této otázce plně věnoval. Autor si dovoluje tvrdit, že je velká

pravděpodobnost toho, že společnosti, těžící obrovské zisky ze ztráty soukromí občanů, pomocí určitých nástrojů nedovolí (nebo udělají maximální odklad) prosazení komplexní právní úpravy, která by byla alespoň nějakým způsobem podobná té evropské.

Ruská federace

Ochrana osobních údajů v kontextu právní úpravy Ruské federace je složena z více propojených mezi sebou částí. Nejprve bych znovu zmínil demokratizaci země, což vede k úpravám otázek ochrany soukromí jako takového, které svým obsahem zasahují i do prostředí internetu. Další složkou je těsná obchodní a politická spolupráce s Evropskou unií, která taktéž vyžaduje ochranu osobních údajů na evropské úrovni. Vládou Ruské federace se přijímají nové zákony upravující tento sektor. Jelikož, jak bylo zmíněno dříve, politika ochrany údajů se odvíjí od současného stavu evropské právní úpravy, musí autor konstatovat, že se chystají změny, které přinesou hlubší pohled na sektor ochrany soukromí na internetu, což je odrazem chystaných změn v právní úpravě Evropské unie (myšleno Sušenkové nařízení).

Na druhé straně problémy úniku dat z databází vládních orgánů zastiňují problémy s nepovoleným zásahem do soukromí uživatelů internetu soukromými společnostmi. Když bychom vzali v úvahu nedokonalost a nižší úroveň vývoje technologií společnosti sbírajících data o uživateli v porovnání se společnostmi americkými, pak je jasné, že se vláda musí nejprve soustředit na aktuálnější problémy současnosti.

6.2 Informační etika a soukromí

Informační etika je natolik široké a obsáhlé téma, kterému se může (a musí) věnovat vědecké práce o velikosti minimálně prací diplomových. Vzhledem k obsahovému omezení autor pouze vyjmenuje základní myšlenky, týkající se problematiky této diplomové práce.

Ochrana soukromí je velké téma informační etiky, které začalo být diskutováno od konce 19. století. Od devadesátých let se pak spolu s šířením internetu stala otázka ochrany soukromí jedním z nejdiskutovanějších problémů informační etiky. Ihned na začátku této podkapitoly je nutné podtrhnout, že autor nehledí na otázku soukromí v informační etice z pohledu konfliktu s právem na informace, kdy stát vyvíjí snahu o zajištění bezpečnosti občanů a snahu firem zajistit adekvátní pracovní úsilí svých zaměstnanců. Řeč půjde pouze o praxi a nástrojích, které umožňují oné obchodování s osobními údaji.

Kodifikace určitých pravidel správného jednání v informační praxi probíhá na několika rovinách – právní normy, mezinárodní úmluvy a profesní (a nejen) kodexy. Právní normy a mezinárodní úmluvy byly rozebrány v páté kapitole. Za zmínku (v rámci této práce) stojí následující kodexy: Desatero počítačové etiky Institutu pro počítačovou etiku, kodex asociace pro výpočetní techniku ACM, kodex Americké knihovnické asociace ALA a zásady síťové etiky (netiquette) od Virginie Shea. Nehledě na velké množství kolizí v pojmech kodexů, lze vyvodit obecně sdílené principy ⁵¹:

1. Informace by měly být volně šířeny.
2. Šíření informací by nemělo znamenat pro nikoho újmu.
3. Nepravdivé informace by neměly být šířeny.
4. Generovat nové informace je žádoucí.
5. Každý je odpovědný za důsledky svého jednání v informační oblasti.

Současně je ale vidět, že celá řada kauz informační etiky leží na rovině střetů mezi některými z těchto principů. Pojednáváme-li o soukromí, pak je nutné podtrhnout kolizi prvního principu s druhým. Přestože v otázkách soukromí se shora zmíněné kodexy jako jeden podtrhují nutnost respektování soukromí každého jedince, protikladem je princip volného šíření informací. Pátý princip hovoří o odpovědnosti za důsledkového jednání v informační oblasti, čímž se vracíme k problematice neinformovanosti uživatelů internetu o existujících hrozbách a o neochotě poskytovatelů služeb na internetu informovat o těchto hrozbách uživatelé.

Elektronická stopa, zanechaná každým uživatelem internetu může být využita několika způsoby. Na Internetu dnes existují detektivní služby, nabízející shromáždění online dostupných informací o komkoliv. Společnosti nabízí různé typy služeb v různých cenových kategoriích. Za poplatek je zákazníkům nabídnut profil obsahující podrobnosti o potyčkách se zákonem, výši daňových přiznání, účastech ve společnostech, bankrotech, finanční a majetkové situaci, rozvodech, členech rodin, sousedech etc ⁵².

Otevřenou otázkou této podkapitoly zůstává rovnováha mezi ochotou provozovatelů internetových sledovacích serverů podstoupit riziku snížení tržeb, kvůli omezení

⁵¹ ČINČERA, Jan. *Informační etika. Sylabus k bakalářskému studiu informační vědy*. 1. vyd. Masarykova univerzita, Filozofická fakulta, 2002. 82 s. ISBN 80-210-2981-1.

⁵² MOOR, James H. Towards a Theory of Privacy in the Information Age. In Baird, R. M., Reagan, R., Rosenbaum, S. E. *Cyberethics: social and moral issues in the computer age*. New York: Prometheus Books, 2000. S. 204

kontroly nad uživatelem a přístupu k jeho osobním údajům na jedné straně a uvědoměním skutečných rizik samotným uživatelem a vůbec snaha o jakoukoliv úroveň kontroly nad svými osobními údaji.

6.3 Obecná doporučení

Po zhodnocení současné situace na trhu s osobními údaji, kde uživatele platí za poskytované služby prakticky neomezeným přístupem do svého soukromí, právních úprav jednotlivých zemí, technologických vymoženosti a variace přístupu k ochraně osobních údajů si autor dovoluje definovat seznam obecných doporučení pro objektivní přístup k tomuto tématu.

Musím mít právo vědět.

Sociální síť či jiná internetová společnost by měla informovat uživatele o tom, že má v úmyslu shromažďovat, uchovávat, a zpracovávat údaje uživatele pro podporu firemní reklamní činnosti v rámci nebo vně vlastní reklamní sítě, nebo pro účely následného prodeje, prodeje licence nebo výměny s marketingovými společnostmi třetích stran. Uživatel by měl před samotnou interakcí s webovým serverem získat detailní popis toho jak, kým a po jakou dobu budou jeho osobní údaje užívány a následně by uživatel měl mít možnosti opt-in a opt-out. Tato volba by neměla být pohřbená mezi posledními řádky psané drobným písmem ujednání o ochraně soukromí, spíše by se měla zobrazit jasně a nepřehledně před samotnou interakcí počítače uživatele a webového serveru. Toto opatření tlačítka by mělo být vyžadováno zákonem a nikoli zůstat ve tvaru doporučení některých soukromých organizací zabývajících se ochranou soukromí.

Internetová společnost by mohla mít právo sledovat pohyby uživatele a jeho volby na její stránce pro účely zvýšení míry efektivity a přizpůsobení obsahu uživateli. Pokud společnost sleduje pohyb uživatelů napříč weby a po neomezenou dobu, musí získat vyslovený souhlas.

Musím mít právo na to být zapomenut.

Jestli internetová stránka, ať je to sociální síť nebo banka, uchovává osobně identifikovatelnou informaci o uživateli, musí mít nařízeno zákonem, že jakákoliv informace, uchovávána o jednotlivém uživateli musí být smazána neprodleně po té, co uživatel vyjádří přání opustit síť nebo komunitu. Stránky by měly garantovat že již nebudou sdílet data uživatele s partnerskými weby nebo společnostmi, že se data uživatele nebudou zobrazovat na stránkách, a že nikdo nebude schopen získat přístup k datům přes dříve vytvořené odkazy.

Jestli uživatel skladuje digitální soubory jako hudbu, video, aplikace, nebo dokumenty na serverech internetové společnosti, pak má právo požadovat o vrácení všech druhů uložených souborů a okamžité smazání těchto souborů z paměti serveru.

Mít právo na rozumnou míru ochranu mých dat.

Každá internetová společnost která uchovává data a osobní údaje pro jakýkoliv obchodní účel musí garantovat rozumnou míru bezpečí pro ochranu majetku uživatele - jeho dat.

Retroaktivní změny musím schválit předtím, než oni nabudou platnosti.

Stejně tak jako jakýkoliv správce (portfolia) aktiv, který využívá peníze zákazníka pro získání dalších peněz, musí internetové společnosti, využívající data o uživateli pro získání peněz, mít určité odpovědnosti. Když se správce aktiv rozhodne investovat do jiného fondu, než investoval doted, musí nabídnout zákazníkovi veškeré možné scénáře vývoje a získat jeho souhlas pro učinění jiných kroků, než těch dříve schválených. Stejně tak tomu musí být i v případě změny způsobu užívání osobních údajů a dat zákazníka, určených a popsanych ve schváleném ujednání o ochraně osobních údajů. Musí být nabídnuté možné scénáře vývoje a možnost úplného odmítnutí nových podmínek.

Měl bych být informovaný o tom, že služba, kterou užívám, plánuje sdílet má data s datovými agregátory.

Uživatel může souhlasit s tím, že sociální síť uchovává data o tom, kdo jsou jeho přátelé a koho daný uživatel "šťouchnul", ale pokud jsou tyto informace spojené s historií vyhledávání, webového prohlížení a nákupů, pak třetí strana má velmi podrobný přehled o jeho osobě. Servery, které takovéto chování praktikují musí srozumitelně popsat své chování a dát možnost uživateli nezúčastnit se shora zmíněného předávání dat.

Mám právo nebýt sledovaný na webu.

Na příkladu vytvořeného ve Spojených státech Nevolejte Mi Registru (Do Not Call Registry), uživatel musí mít právo na ochranu před praktikami řady společností, které sledují pohyb a chování online. Reklamní společnosti se snaží o dobrovolnou regulaci těchto praktik online pomocí seznamu NeSledovat (Do Not Track), ve kterém je uveden výčet zapojených společností a pomocí jednoduché navigace uživatel může "nezúčastnit se" online sledování. Některé společnosti, přes jejich dobrovolné zapojení do programu DNT nereagují na nastavení uživatele a v sledování pokračují.

Legislativa

Je na čase, aby vláda Spojených států nastavila právní rámec na federální úrovni, ve kterém by uživatelská data byla považována za hodnotný majetek, a internetové společnosti, které by tyto data ztratily nebo je používaly neodpovídajícím způsobem, by byly odpovědné za vzniklou škodu. Takového stavu lze dosáhnout ale pouze tehdy, když samotné uživatele budou požadovat změny ze strany zákonodárců. Bez nutné úrovně ochrany spotřebitele povinnosti internetových společností zůstanou nejednoznačné, a jedinci poškozené ztrátou dat budou na velmi nejisté právní půdě při vymáhání náhrady vzniklé škody. Z toho jednoznačně vyplývá potřeba osvěty uživatelů o současném stavu a hodnotě jejich osobních údajů.

Osvěta

Primární měnou v nové ekonomice jsou uživatelská data. Nicméně tato nesmírná hodnota údajů je zřejmá pouze společnostem obchodujícím s nimi a je méně zřejmá pro většinu uživatelů internetu. Spotřebitelé si musí být vědomé současné situace a musí vyžadovat odpovědný přístup a přiměřenou míru ochrany. Tato osvěta může probíhat na několika úrovních – rozvoj (jíž existujících) aktivit Úřadu pro ochranu osobních údajů v rámci České republiky, rozvoj aktivit Evropskou komisí v rámci EU a rozumná míra medializace tohoto problému. Medializací autor myslí vydání názorných, stručných a odůvodněných příkladů odcizení osobních údajů a hrozeb s ní spojených, a seznam doporučených kroků pro minimalizaci dopadů. Tato navrhovaná medializace bude samozřejmě „proti srsti“ velkým společnostem, které celou tuto problematiku záměrně spojují a dávají do kontextu svobody slova, volného šíření informace a regulace internetu a vystavují zároveň s cenzurou opakem pojmu svoboda. Což není realitou. Každý jedinec si musí uvědomit, že právě online sledování, vytváření profilů a behaviorální cílení je hrozbou pro výše zmíněnou svobodu a soukromí. Toto uvědomění nesmí následně zůstat na povrchním konstatování toho, že osobními údaji uživatel platí za služby a dobrovolně pokračovat ve sdílení všeho druhu.

Profesionálové, kteří se zabývají osvětou, by se musely před samotnou medializací problému primárně soustředit na samotné podstatě střetu zájmů internetových společností, uživatelů lhostejných k neoprávněnému nakládání s jejich osobními údaji a uživatelů, které si tohoto problému jsou vědomí a odpovědně přistupují k otázce ochrany soukromí. U samotných uživatelů v té či oné míře potřeba spolupatičnosti

(třetí kategorie potřeb dle pyramidy Maslowa) zamlžuje obzor a zkresluje představu o realitě zacházení s osobními údaji.

Další velmi důležitou věcí je možnost nahlédnout pod pokličku různých internetových hutí, které jsou po většině vytvářeny přímo nebo sponzorovány společnostmi, praktikujícími činnost narušování soukromí. Příkladem lze uvést společnosti Google vytvořenou stránku Take action⁵³, kde Google vyjadřuje své obavy z regulace internetu jednotlivými státy a uživatelé mohou dokonce podepsat petici. Velké množství faktů a údajů uvedených na této stránce jsou pravdivá a vyvozené obavy mohou nějakým způsobem být skutečností. Tyto údaje jsou ale jednostranné a neobjektivní, protože jejich hlavním účelem je udržet současný neregulovaný stav pro další kontrolu uživatelů a narušování soukromí, a neuvádějí úplný a objektivní obrázek nastalé situace.

Privacy by Design

„Má-li soukromí přežít, musí se jeho ochrana přizpůsobit změnám ve společnosti“ – říká ve své knize „Privacy by Design. Take the Challenge“ kanadská komisařka pro ochranu dat ve státě Ontario Ann Cavoukianová⁵⁴ - „Nové technologie by pro nás neměly být hrozbou, ale měly by být chápány jako výzva k novému postoji a pohledu na implementaci prvků zásad ochrany soukromí“. Termín „Privacy by Design“ zatím nemá ustálený český ekvivalent. Lze jej přeložit jako „naprojektované soukromí“ nebo „soukromí coby aspekt návrhu“. Jedná se o takový koncept ochrany soukromí, kdy prvky ochrany soukromí jsou předem zakotveny, naprojektovány, do různých technologií, či jsou předem zakomponovány do různých situací souvisejících s ochranou soukromí. Úřad pro ochranu osobních údajů v Praze ostatně již několik let upozorňuje na to, že specifická hlediska ochrany dat a soukromí je třeba uplatňovat již při samotné volbě a vývoji informačních systémů, nikoliv až po jejich zavedení v aplikační praxi.

Tento přístup je jakýmsi velmi dobrým doporučením pro zavádějící projekty. V případě již fungujících gigantů jako Facebook a Google, politikou ochrany soukromí kterých je One-size-fits-all, bude tento přístup nepoužitelný.

⁵³ Google: Take Action. GOOGLE. *Take Action* [online]. [cit. 2012-12-08]. Dostupné z: <https://www.google.com/takeaction/>

⁵⁴ CAVOUKIAN, Ann. *Privacy by Design*. Toronto, Ontario – Canada, 2009. Dostupné z: <http://privacybydesign.ca/publications/pbd-the-book/>

6.4 Doporučení pro uživatele

V této části autor definuje několik základních kroků, jakými může uživatel minimalizovat svou personalizaci na webu a maximalizovat ochranu osobních údajů.

Nastavení koncového zařízení

Smazat cookies

- Google Chrome: (Preferences -> Under the Hood -> Content Settings)
- FireFox: (Preferences -> Privacy -> Use custom settings for history)
- Safari: (Preferences -> Security)
- Internet Explorer: (Internet options -> Privacy)

Po smazání cookies je třeba nastavit parametry ukládání cookies takovým způsobem, aby jejich absence na jednu stranu nepřekážela pohodlnosti, na stranu druhou aby existence cookies třetích stran neumožňovala sledování napříč různými weby. Veškeré nastavení se dělají v prohlížeči.

Smazat Flash cookies

Pro smazání Flash cookies je třeba navštívit stránky Adobe Settings Manager ⁵⁵. Vestavěný modul nabídne 8 záložek ve kterých si uživatel může smazat již existující Flash cookies, tak i vybrat takové nastavení, které zabráni jejich dalšímu vytváření.

Vypnout sledování (cílenou reklamu)

V nastavení prohlížeče můžeme zakázat sledování našeho pohybu jinými servery.

- Google Chrome - 'Keep My Opt-Outs'
- IE9 - 'Tracking Protection'
- Firefox - 'Do Not Track'

Instalace plug-inů

Moderní internetové prohlížeči a plug - iny prohlížečů poskytují bohatý soubor rozhraní pro webové stránky pro ukládání dat na systémech uživatelů. Tato data se používají pro uchování přihlašovacích údajů (uživatelská jméno/hesla a jejich obdoby), sledování uživatelů, ukládání nastavení (personalizace rozhraní, ovládací prvky), data internetových stránek (bezpečnostní problematika, obrázky, cash), identifikační tokeny, či jiná data. Uživateli je nabídnuta celá řada plug-inů pro minimalizaci sledování na

⁵⁵ Adobe: Flash Player Help - Website Storage Settings panel. ADOBE. [online]. [cit. 2012-12-08].

Dostupné

z:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

webu a dopadu bubliny filtru. Fungují na principu automatického vyjadřování nesouhlasu pro sledování nebo správu cookies.

- Advertising Cookie Opt-out – plug-in vyvinutý přímo společností Google
- Better Privacy – maže Flash cookies na zařízení uživatele
- Ghostery – blokuje webové štenice na internetových stránkách
- TACO – automaticky vyjadřuje nesouhlas pro sledování – opt-out
- DoNotTrack – alternativa plug-inu TACO

Zapnutí anonymního prohlížení

Díky zapnutému anonymnímu prohlížení se uživatel zbaví nutnosti neustálého mazání cookies. Tato možnost je alternativou pečlivého nastavování ukládání cookies prohlížečem.

Úprava nastavení serverů

Opt-out

Navštívit web Your online choices ⁵⁶ a vypnout sledování všemi společnostmi. Tímto krokem uživatel vyjadřuje nesouhlas se sledováním a je na dobré vůli amerických společností, aby uživatele přestaly sledovat.

Smazat historii web-vyhledávání Google

V případě, že uživatel používá Gmail, Google Maps, AdWords, AdSense a jiné, má registrovaný účet Google. Tady se zaznamenává historie prohlížení, seznam může být i několik let starý.

Pro smazání této historie vyhledávání na Google stačí vybrat Nastavení účtu – v záložce Služby vybrat Přejít na webovou historii a smazat a/nebo vypnout Webovou historii.

Pečlivé nastavení soukromí na Facebook a Google+

Uživatel si musí být vědom veškerých možností, jak se jeho osobní údaje mohou dostat do nesprávných rukou. Je třeba velmi pečlivě nastavit možnosti soukromí, vybrat pouze důvěryhodné aplikace, se kterými sdílí údaje, nastavit minimální zobrazování veřejných informací, viditelnost profilu, zakázat používání jména a fotografie pro marketingové účely a sdílení osobních údajů. Na stránkách Google Dashboard ⁵⁷ jsou soustředěny

⁵⁶ HETZNER ONLINE AG, Berlin, Germany. *Your Online Choices* [online]. [cit. 2012-12-08]. Dostupné z: <http://www.youronlinechoices.com/cz/vase-volby>

⁵⁷ Google: Dashboard. GOOGLE. [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/dashboard>

informace o aktuálním nastavení soukromí uživatele pro jednotlivé služby. Na stránkách Google Historie ⁵⁸ uživatel může vypnout ukládání webové historie.

Nastavení zobrazování reklam uživatel najde na Google Nastavení reklam ⁵⁹.

Skrýt personální informaci na Facebook

Tato společnost ze všech ostatních udělala nejvíce pro to, aby privátní informace a soukromí byly veřejně přístupné. Facebook nebo pověřené jim třetí strany zpracovávají veškeré údaje a informace o uživatelích a jejich pohybu až do statistického zpracování počtu stisknutí tlačítka Like.

Možností pro skrytí personálních informací Facebook poskytuje více. Auto doporučuje podrobné procházení jednotlivých parametrů v nastavení soukromí.

Skrýt datum narození a používat přezdívky na sociální síti

Osob se stejným jménem se může vyskytovat větší množství. Přesnější identifikaci umožňuje datum narození.

Použití alternativních vyhledávačů

Vyhledávač DuckDuckGo ⁶⁰ na rozdíl od známých vyhledávačů nesbírá data o uživatelích a neupravuje dle nich výsledky vyhledávání. Jeho zakladatel Gabrel Weinberg ⁶¹ se rozhodl postavit gigantům Google a Bing a jeho vyhledávač denně zpracuje již okolo 45 miliónů dotazů.

Použití anonymního surfingu

Některé dostupné služby pomáhají maskování IP adresy. Pomoci cibulové metody navštěvovaný server nevidí skutečnou IP adresu koncového zařízení.

Takové stránky jako Torproject.org a Anonymizer.com propouští veškerý traffic ze všech webových prohlížečů přes vlastní servery a efektivně mažou veškeré údaje, které jsou schopné identifikovat uživatele.

⁵⁸ Google: History. GOOGLE. [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/history>

⁵⁹ Google: Nastavení reklam. GOOGLE. *Reklamy na webu* [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/ads/preferences>

⁶⁰ DuckDuckGo [online]. [cit. 2012-12-08]. Dostupné z: <http://duckduckgo.com/>

⁶¹ PAVEC, Jan. Hospodařské noviny. Nový vyhledávač chráné soukromí: Sledování uživatelů pomocí prohlížečů a vyhledávačů využívají reklamní agentury i politické strany. 05.12.2012.

Tyto metody ale mají i své negativní stránky – vyžadují instalaci tlustých klientů, zpomalují rychlost brouzdání na internetu a nemaskují jiné parametry identifikace (shora projednávané sdílené údaje, zobrazené pomoci serveru Panoptick).

Zůstat offline

Pokud uživatel učiní veškeré kroky pospané v této kapitole, nejsou žádné záruky toho, že zůstane stoprocentně anonymní. Přihlášení uživatele do jakéhokoliv serveru, ihned prozradí jeho identitu. Shora zmíněné kroky jsou doporučením, a to velmi účinným, pro snížení míry shromažďovaných osobních údajů, dopadu sledování a bubliny filtrů, ale jedinou stoprocentně účinnou metodou je zůstat offline.

Závěr

Společnost se v současné chvíli nachází uprostřed informační revoluce, a pouze teď si tuto skutečnost začíná uvědomovat. V poslední době se razantně změnily naše způsoby nakupování, naše vztahy s bankami a rutinní pracovní činnost, tyto změny vyúsťují do bezprecedentního množení záznamů a dat. Drobné detaily, které byly jednou zaznamenány do digitálních pamětí počítačů, se shromažďují do obsáhlých databází plných osobními daty. Denně sdílíme pomocí e-mailů a interakcí v sociálních sítích informace a multimediální soubory. Naše peněženky jsou plné kreditními, debetními bankovními karty, karty bonusových programů, slevovými karty, které zanechávají informační stopu o každém uživateli. S vývojem a zdokonalováním technologií jsou komerční společnosti schopné pomocí sledování na webu a zaznamenávání historie vyhledávání vytvářet velmi přesné profily všech, kdo se na internetu pohybuje. Digitální technologie zaznamenávají veškeré drobné údaje o tom, co máme a nemáme rádi. Veškerá data jsou uložena v binárním kódu tak, aby se pomocí určitých nástrojů dalo efektivně vytěžit maximální množství užitečných dat.

Internet se spolu se zlevňováním hardwaru exponenciálně rozšiřuje a osobní údaje se stávají velmi cennou komoditou, která je shromažďována, zpracovávána a následně předána nebo prodána třetím stranám. Na trhu s osobními údaji existují stovky společností, které budují obrovské databáze s profily, které zahrnují psychologické detaily, detaily o národnosti, pohlaví, důchodu, zálibech a nákupech. Střípky dat, které jednotlivec zanechává v průběhu každodenní existence a interakce na webu, jsou shromažďována a analyzována pro získání maximálně přesného obrázku o něm – obecný profil, kreditní historie, solventnost, oblíbené zboží, to vše pro maximálně přesné cílení reklamy, a nejen.

Jakákoliv webová reklama ukládá cookie do prohlížeče uživatele, která zaznamenává chování uživatele po dobu měsíců. Webové štěníce zaznamenávají pohyb a ukládají záznamy na serverech provozovatelů analytických služeb. Veškeré další technologické metody shromažďují data o chování a následně je prodávají obchodníkům, kteří je používají pro účely cílené reklamy, profilování a následný prodej profilů na požadavek soukromých společností nebo vlády.

Uživatelé internetu nahrávají obrázky, sdílí příběhy, a vkládají osobní data do oblíbené sociální sítě po několik let. Nyní sítě říkají, že všechny údaje uživatelů jsou veřejná a chystají se sdílet s reklamními společnostmi. Případy, kdy společnost, nabízející cloud

služby, kde uživatel má uložené jak soukromé tak i pracovní soubory a data, krachuje a veškerý uložený obsah prodává na aukci, jsou skutečnosti. Mnoho z uživatelů sdílí na internetu data s citlivým obsahem, multimediální soubory a informace z osobního života a nejsou si vědomé žádných hrozeb. Jedná z hrozeb je absence záruk zabezpečení osobních dat nebo náhrady škody při jejich ztrátě. Nebezpečí není omezené jen na pravděpodobnost toho, že data uživatele mohou být zničena. Osobní reputace může být vážně poškozena, jestli narušitel buď zveřejní citlivé informace, nebo zahájí vydírání dotčeného uživatele hrozbou zveřejnění.

Celý průmysl marketingových a reklamních společností vyrostl na základě ukládání HTML a Flash cookies do webových prohlížečů a jiných, než cookie metod, pro sledování uživatelů napříč webem a ukládání jejich chování a preferencí. Většina času uživatel netuší, že je sledován. Pokud si je uživatel toho vědom, existuje malá pravděpodobnost toho, že ví jak se toho sledování vyhnout. Toto uvědomění ale zdaleka nedosahuje úrovně reality a je někdy důvodem pro laxní přístup k ochraně vlastních osobních údajů. To je primární problém v oblasti ochrany osobních údajů.

Na poli tohoto tématu jsou tři významní hráči – soukromé společnosti, zisk kterých je přímo úměrný míře odhalení soukromí uživatelů jejich služeb, dále samotné uživatele, kteří se snaží (nebo ne) o maximální ochranu soukromí a vláda, která má různé role v závislosti na státu. Komise Evropské unie pro ochranu soukromí v dnešní situaci je příkladem pro úřady ostatních zemí. Evropskou unii byl vytvořen velmi důležitý orgán (Pracovní skupina 27), který je velmi moderní a snaží se o zachycení co nejaktuálnější situace pro vydání efektivních doporučení, ze kterých se následně tvoří směrnice nebo nařízení. Protikladem evropského přístupu je vláda Spojených států amerických – nesnaží se o žádnou systematickou a účinnou regulaci činnosti společností praktikujících online sledování a profilování. Dle názoru autora se toto děje ze dvou významných důvodů. Prvním je absence zájmu ze strany většiny občanů Spojených států ve vytvoření adekvátních legislativních úprav (příčinou toho může, nebo nejspíše je, nulová osvěta tohoto tématu). Příčinou druhou je neochota vlády vzdát se bezplatných zdrojů podrobných informací na jednotlivé osoby (počet žádosti amerických orgánů o poskytnutí kompletních profilů jedinců na společnost Google v roce 2011 přesáhl 23 tisíc).

Primární hrozbou je ale samotná podstata všech činností v řetězci pojmů týkajících se personalizace: online sledování – profilování – behaviorální cílení reklamy. Jak autor

této práce probíral v některých kapitolách – společnosti hrubě porušují evropské zákony na ochranu soukromí nejen svým podnikáním, ale i samotnými ujednáními o ochraně osobních údajů. Problémem ale zůstává vymahatelnost legislativních nařízení při přeshraničním převodu osobních údajů. Evropská strana, která vyvíjí maximální úsilí pro zajištění soukromí, nemá reálné nástroje ovlivňování společností, registrovaných ve Spojených státech. Hlavním nástrojem pak zůstává hrozba pro shora zmíněné společnosti vydání oficiálního stanoviska o nesouladu činnosti společnosti se zákony EU a jejich systematické porušování, které může negativně ovlivnit jejich podnikání. Díky těmto metodám evropská strana vyvíjí tlak na americké společnosti a nutí je ke konání kroků pro zlepšení ochrany soukromí a osobních údajů. Situace by byla o něco méně napjatá, pokud by ve Spojených státech existoval komplexní zákon, na který by se dalo apelovat u místních soudů. Tomu ale tak není. Návrh zákona, podobného směrnici 95/45/EC byl několikrát upravován a jeho současná podoba (která ještě není ani přijata) jen lehce připomíná evropskou směrnici. Další otázkou v hledání rovnováhy v kontextu mezinárodních vztahů jak států, tak i soukromých společností je postavení Evropské unie ve vztahu k vlastním podnikům z evropského prostředí.

Ze strany regulátorů při rozhodování o výběru politiky ochrany osobních údajů vznikají další potíže při hledání rovnováhy, vzniká otázka co je prioritní v tomto ohledu – jednice nebo firma. Zpřísněním zákona budou znevýhodněné evropské společnosti vůči těm zahraničním, což může být příčinou přenosu kapitálu za hranice EU. Kdežto zmírněním těchto zákonů budou trpět jednotlivci.

Samozřejmě, online sběr dat a cílená reklama může udělat online nakupování a rychlé vyhledávání pohodlnějším, ale je těžké určit kde můžeme načrtnout hranici mezi oprávněným a neoprávněným, opodstatněným a neopodstatněným užíváním a shromažďováním informací o zákaznících. V současné době jsou to samotné uživatelé, kdo může nejefektivněji minimalizovat rizika ztráty soukromí. Proto musí být vyvinutá určitá úsilí pro medializaci těchto hrozeb a zveřejnění nástrojů pro kontrolu soukromí.

Dále z pohledu občana Evropské unie je rozumné počkat na přijetí sušenkového nařízení a sledovat vývoj situace ve Spojených státech amerických a vztahu mezi nimi a Evropou.

Seznam použité literatury

Literatura

- Brotherton, E.A.** 2012, "Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine", *Emory Law Journal*, vyd. 61, č. 3, str. 555-600.
- CAVOUKIAN, Ann.** Don Tapscott. *Who knows?: safeguarding your privacy in a networked world*. Toronto: Random House of Canada, 1995. ISBN 03-942-2472-8.
- CAVOUKIAN, Ann.** *Privacy by Design*. Toronto, Ontario – Canada, 2009. Dostupné z: <http://privacybydesign.ca/publications/pbd-the-book/>
- ČINČERA, Jan.** *Informační etika. Syllabus k bakalářskému studiu informační vědy*. 1. vyd. Masarykova univerzita, Filozofická fakulta, 2002. 82 s. ISBN 80-210-2981-1.
- Chirita, P.A., Firan, C.S., Nejd, W.:** Personalized query expansion for the web. In: Proceedings of the 30th annual international ACM SIGIR conference on research and development in information retrieval, Amsterdam, The Netherlands (2007)
- MATES, P. -- SMEJKAL, V.** K ochraně soukromí a osobních údajů v telekomunikacích. *Právo a podnikání : odborný časopis pro obchodní, finanční a pracovní právo*. 2003. sv. XII, č. 6, s. 20--24. ISSN 1211-1120
- MATES, P.** Novela zákona o ochraně osobních údajů. *Daňová a hospodářská kartotéka*. 2001. sv. 9, č. 16, s. 183--186. ISSN 1210-6739
- MATOUŠOVÁ, M. -- HEJLÍK, L.** *Osobní údaje a jejich ochrana*. Praha: ASPI, 2008. ISBN 978-80-7357-322-5.
- MAŠTALKA, J.** *Osobní údaje, právo a my*. Praha: C.H. Beck, 2008. ISBN 978-80-7400-033-1
- MOOR, James H.** Towards a Theory of Privacy in the Information Age. In Baird, R. M., Reagan, R., Rosenbaum, S. E. *Cyberethics: social and moral issues in the computer age*. New York: Prometheus Books, 2000. S. 204
- Ochrana osobních údajů:** vybrané otázky: příručka pro podnikatele. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011, 50 s. ISBN 978-80-210-5572-8.
- PARISER, Eli.** *The filter bubble what the Internet is hiding from you*. New York: Penguin Press, 2011. ISBN 11-015-0572-9
- RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA.** *Biometrie a identita člověka*. Praha: Grada Publishing a.s., 2008.
- SKLENÁK, Vilém.** *Data, informace, znalosti a Internet*. Vyd. 1. V Praze: C.H. Beck, 2001, xvii, 507 s. C.H. Beck pro praxi. ISBN 80-717-9409-0.
- SOLOVE, Daniel J.** *The digital person: technology and privacy in the information age*. New York: New York University Press, c2004, xii, 283 p. ISBN 08-147-9846-2.

Internetové zdroje

ADOBE. *Adobe Flash runtimes: statistics* [online]. [cit. 2012-11-07]. Dostupné z:

<http://www.adobe.com/products/flashruntimes/statistics.html>

ADOBE. *Adobe Flash runtimes: statistics* [online]. [cit. 2012-11-07]. Dostupné z:

<http://www.adobe.com/products/flashruntimes/statistics.html>

Adobe: Flash Player Help - Website Storage Settings panel. ADOBE. [online]. [cit. 2012-12-08].

Dostupné z:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

Adaptic [online]. [cit. 2012-11-08]. Personalizace. Dostupné z WWW:

<http://www.adaptic.cz/znalosti/slovnicek/personalizace/>.

ANGWIN, JULIA a JEREMY SINGER-VINE. Selling You on Facebook. [online]. 2012 [cit. 2012-12-08]. Dostupné z:

<http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html#articleTabs%3Darticle>

Behavioral Advertising and Consumer Privacy Considerations, *Journal of Internet Law*, vyd. 15, č. 9, str. 3-12.

Barnett, E. 2012, *'Google is now deciding what's good for us'*, London (UK), United Kingdom, London (UK). [online]. [cit. 2012-12-08]. Dostupné z:

BROCK, Jim. Facebook gives The Product more control over how it is sold. [online]. 2012 [cit. 2012-12-08]. Dostupné z: <http://blog.privacychoice.org/>

BUSINESSINFO.CZ. Ochrana osobních údajů. [online]. [cit. 2012-12-08]. Dostupné z:

<http://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-opu-4637.html#b1>

Cox, J.T. & Cline, K.M. 2012, "Parsing the Demographic: the Challenge of Balancing Online [online]. [cit. 2012-12-08]. Dostupné z:

<http://search.proquest.com.ezproxy.vse.cz/docview/922731285/13ADD563D84CF41D004/>

Claire, C.M. 2012, *Google Searches Get Personal*, New York, N.Y., United States, New York, N.Y. [online]. [cit. 2012-12-08]. Dostupné z:

<http://search.proquest.com.ezproxy.vse.cz/docview/1033141609/13ADD563D84CF41D004/>

COOPER, Alissa. A survey of query log privacy-enhancing techniques from a policy perspective. *ACM Transactions on the Web* [online]. 2008-10-01, roč. 2, č. 4, s. 1-27 [cit. 2012-12-08]. ISSN 15591131.

DOI: 10.1145/1409220.1409222. Dostupné z: <http://portal.acm.org/citation.cfm?doid=1409220.1409222>

DOMAINTOOLS, LLC. *DomainTools* [online]. [cit. 2012-12-08]. Dostupné z: whois.domaintools.com

DRUCKER, Jesse. Google 2.4% Rate Shows How \$60 Billion Lost to Tax Loopholes. [online]. 2010 [cit. 2012-12-08]. Dostupné z: <http://www.bloomberg.com/news/2010-10-21/google-2-4-rate-shows-how-60-billion-u-s-revenue-lost-to-tax-loopholes.html>

EU. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *13/sv. 15*. 23.11.1995.

Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF>

Facebook: Prohlášení o právech a povinnostech. FACEBOOK, Inc. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.facebook.com/legal/terms>

Facebook: Results of Operations and Financial Condition. FORM 8-K, UNITED STATES SECURITIES AND EXCHANGE COMMISSION. [online]. 2012 [cit. 2012-12-08]. Dostupné z: <http://pdf.secdatabase.com/700/0001193125-12-316895.pdf>

FACEBOOK, Inc. *Communicating Information in a Social Network System about Activities from Another Domain* [patent]. USA. 705/14.41, G06Q 30/00 20060101 G06Q030/00. Uděleno 22. září 2011. Dostupné z: <http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20110231240.PGNR.&OS=dn/20110231240&RS=DN/20110231240>

Google's Market Share in Your Country. [online]. 2009 [cit. 2012-12-07]. Dostupné z: <http://googlesystem.blogspot.cz/2009/03/googles-market-share-in-your-country.html>

Google Transparency Report. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.google.com/transparencyreport/userdatarequests/?p=2009-12>

Google: Take Action. GOOGLE. *Take Action* [online]. [cit. 2012-12-08]. Dostupné z: <https://www.google.com/takeaction/>

Google: Dashboard. GOOGLE. [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/dashboard>

Google: History. GOOGLE. [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/history>

Google: Nastavení reklam. GOOGLE. *Reklamy na webu* [online]. [cit. 2012-12-08]. Dostupné z: <http://google.com/ads/preferences>

HOOFNAGLE. Flash Cookies and Privacy. [online]. 2009 [cit. 2012-11-07]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

HETZNER ONLINE AG, Berlin, Germany. *Your Online Choices* [online]. [cit. 2012-12-08]. Dostupné z: <http://www.youronlinechoices.com/cz/vase-volby>

JANOVSKÝ, Dušan. Cookies. *Cookies* [online]. [cit. 2012-11-07]. ISSN 1801-0458. Dostupné z: <http://www.jakpsatweb.cz/enc/cookies.html>

LASZLO, Joseph, Director of Research, IAB. News Media Workshop – Comment, Project No. P091200. [online]. 2010 [cit. 2012-12-08]. Dostupné z: http://www.iab.net/media/file/News_Media_Workshop_-_Comment_Project_No.P091200.pdf

KOROLYUK, Alexey. Expertů tvrdí: "Zákon o osobních údajích musí být dopracován". [online]. 2011 [cit. 2012-12-08]. Dostupné z: <http://internet.cnews.ru/news/line/index.shtml?2011/06/30/445794>

Luke O'Neil 2011, *OFF DUTY --- Gear & Gadgets: Not Me Dot Com --- Want an Internet that doesn't know your pant size? A guide to regain your privacy*, New York, N.Y., United States, New York, N.Y. [online]. [cit. 2012-12-08]. Dostupné z: <http://search.proquest.com.ezproxy.vse.cz/docview/872315249/13ADD563D84CF41D004/>

MCKINLEY, Katherine. Cleaning Up After Cookies: Version 1.0. [online]. 2008, s. 12 [cit. 2012-11-07]. Dostupné z: https://www.isecpartners.com/media/11976/iSEC_Cleaning_Up_After_Cookies.pdf

Panopticklick [online]. ? [cit. 2012-05-29]. Dostupné z: panopticklick.eff.org

Introduction to Persistence: Cookies. [online]. roč. 2011 [cit. 2012-12-07]. Dostupné z: <http://msdn.microsoft.com/en-us/library/ms533007%28VS.85%29.aspx>

PAVEC, Jan. Hospodařské noviny. Nový vyhledávač chráně soukromí: Sledování uživatelů pomocí prohlížečů a vyhledávačů využívají reklamní agentury i politické strany. 05.12.2012.

Ruská federace. Konstituce Ruské federace: Práva a svobody osob a občanů Ruské federace. In: *FZ 2*. Dostupné z: <http://www.gov.ru/main/konst/konst12.html>

Ruská federace. Federální zákon o ochraně osobních údajů. In: *N-152FZ*. 2006. Dostupné z: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=117587>

SOLTANI, Ashkan, Shannon CANTY, Quentin MAYO, Lauren THOMAS a Chris Jay MCVEY, Kathleen. Arcot Systems to Protect Online Identities at Top Philippines Bank. [online]. 2008 [cit. 2012-12-07]. Dostupné z: <http://www.reuters.com/article/2008/03/10/idUS121553+10-Mar-2008+MW20080310>

STAMOS, Alex. Vulnerabilities 2.0 in Web 2.0: Next Generation Web Apps from a Hacker's Perspective. [online]. roč. 2007 [cit. 2012-12-07]. Dostupné z: <https://www.isecpartners.com/media/12946/Attacking-AJAX-Applications-Web20-Expo.pdf>

STAMOS, Alex. Vulnerabilities 2.0 in Web 2.0: Next Generation Web Apps from a Hacker's Perspective. [online]. roč. 2007 [cit. 2012-12-07]. Dostupné z: <https://www.isecpartners.com/media/12946/Attacking-AJAX-Applications-Web20-Expo.pdf>

SOGHOIAN, PH.D., Christopher. Privacy researcher and activist. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.dubfire.net/>

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Slovníček nejdůležitějších pojmů. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.uoou.cz/uoou.aspx?menu=281&loc=455>

WolframAlpha: Facebook. [online]. [cit. 2012-12-08]. Dostupné z: <http://www.wolframalpha.com/input/?i=facebook>

WP27, Stanovisko 2/2010 k internetové reklamě zaměřené na chování. [online]. 22. června 2010 [cit. 2012-12-08]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf

Seznam obrázků

Obrázek č. 1 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)	26
Obrázek č. 2 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)	26
Obrázek č. 3 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)	27
Obrázek č. 4 - Pavučina relací mezi navštívenými weby a weby třetích stran (zdroj: autor)	30
Obrázek č. 5 - Zobrazení preferencí přiřazených uživateli (zdroj: autor)	34
Obrázek č. 6 - Načítání dat serverem WolframAlpha z Facebook (zdroj: autor)	39
Obrázek č. 7 - check-iny a oblako slov (zdroj: autor)	39
Obrázek č. 8 - Statistické údaje o přátelích (zdroj: autor)	40
Obrázek č. 9 - Lokalizace přátel (zdroj: autor)	40
Obrázek č. 10 - Profil vytvořený na základě chování uživatele (zdroj: Bluekai)	43
Obrázek č. 11 - Bublina filtrů (zdroj: Eli Pariser, TED2011)	47
Obrázek č. 12 - Příklad opt-in v praxi (zpracování: autor, zdroj: BBC UK)	57

Seznam tabulek

Tabulka č. 1 - Statistika žádostí a předaných dat jednotlivým státním orgánům (vlastní zpracování, zdroj: Google)	22
Tabulka č. 2 - Adresy navštívených stránek a webů třetích stran (zdroj: autor)	29
Tabulka č. 3 - Servery, sbírající data z více autorem primárně navštívených stránek (zdroj: autor)	31
Tabulka č. 4 - cookie přihlášeného uživatele (zdroj: autor)	35
Tabulka č. 5 - cookie odhlášeného uživatele (zdroj: autor)	35
Tabulka č. 6 - Seznam údajů, které může/nemůže agregátor dat Bluekai vědět (zdroj: Bluekai)	44