UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut komunikačních studií a žurnalistiky, katedra mediálních studií

Tomáš Povejšil

Obchodování s osobními údaji získanými online

Diplomová práce

Praha 2017

Autor práce: **Tomáš Povejšil**

Vedoucí práce: **JUDr. PhDr. Josef Benda, Ph.D., LL.M., Ph.D.**

Rok obhajoby: **2017**

Bibliografický záznam

POVEJŠIL, Tomáš. *Obchodování s osobními údaji získanými online.* Praha, 2012. 98 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut komunikačních studií a žurnalistiky. Katedra mediálních studií. Vedoucí diplomové práce JUDr. PhDr. Josef Benda, Ph.D., LL.M., Ph.D.

Abstrakt

Doba nových médií a big data umožnila, že se z osobních údajů stala cenná komodita. V diplomové práci je popsán málo známý trh s osobními údaji a praxe společností, které s nimi obchodují. V USA mají společnosti označované jako data brokers rozsáhlé databáze obsahující překvapivě citlivé osobní údaje o miliónech osob.

V této diplomové práci jsou také představena některé rizika nedostatečné ochrany soukromí občanů v současné digitální ekonomice a jsou zde identifikované budoucí možnosti ochrany soukromí v digitálním světě.

Těžištěm práce je komparativní analýza právní regulace data brokers v USA, Kanadě a EU. Na základě této analýzy lze shrnout, že americká legislativa neobsahuje unifikovanou ochranu osobních údajů, ale spíše roztříštěnou regulaci obsaženou ve více právních normách, která rozsáhlou činnost data brokers umožňuje, a to i bez vědomí fyzických osob.

Oproti tomu legislativa v EU a Kanadě je více nakloněná ochraně soukromí a osobních údajů. V EU reguluje nakládání s osobními údaji směrnice implementována členskými státy; od května 2018 bude tato směrnice nahrazena novým nařízením GDPR, které bude přímo účinné ve všech státech EU. Obě tyto normy fakticky znemožňují obchodování s osobními údaji v rozsahu, v jakém je to možné v USA.

Abstract

In today’s world of new media and big data, our personal data is a valuable commodity. This Master's thesis presents a little-known industry of personal data brokers. Databases of US data brokers contain surprisingly detailed and sensitive information of millions of Americans. The thesis also contains an analysis of risks related to insufficient protection of personal information in digital economy along with possibilities how to enhance our digital privacy in connection with data brokers.

The core of the thesis is a comparative analysis of data broker legislation in the US, Canada and the European Union. The analysis shows that in the US there is no unified regulation of personal data protection from activities of data brokers but several laws partially regulating some aspects of personal data protection; this system allows trade in personal data even without the acknowledgement of the persons.
On the other hand, regulation in the EU and Canada favours protection of personal data and privacy. In the EU each member state has its legal act on personal data protection based on the EU directive. In April 2018 this directive will be replaced by General Data Protection Regulation which will be directly applicable in all member states. Both current and future legislation, however, make the data broker industry as described in the US practically impossible.

Klíčová slova

Obchodování s osobními údaji, data broker, internet, data mining, GDPR, ochrana osobních údajů

Keywords

Personal data trading, data broker, internet, data mining, GDPR, personal data protection

Rozsah práce: 168 898 znaků vč.mezer

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 15.5.2017 Tomáš Povejšil

Na tomto místě bych rád poděkoval rodině, přátelům a vedoucímu práce, kteří mně pomohli a podpořili při tvorbě tohoto díla.

Institut komunikačních studií a žurnalistiky FSV UK Teze MAGISTERSKÉ diplomové práce	
TUTO ČÁST VYPLŇUJE STUDENT/KA:	
Příjmení a jméno diplomantky/diplomanta: Povejšil Tomáš	Razítko podatelny:
Imatrikulační ročník diplomantky/diplomanta: 2015	
E-mail diplomantky/diplomanta:	
Studijní obor/forma studia: Mediální a komunikační studia, navazující magisterské, kombinovaná	
Předpokládaný název práce v češtině: Obchodování s osobními údaji získanými online	
Předpokládaný název práce v angličtině: Trading of personal data acquired online	
Předpokládaný termín dokončení (semestr, akademický rok – vzor: *ZS 2012/2013*) (diplomovou práci je možné odevzdat nejdříve po dvou semestrech od schválení tezí) LS 2016/2017	
Charakteristika tématu a jeho dosavadní zpracování (max. 1800 znaků): V současném světě hraje Internet klíčovou roli snad v každém odvětví lidské činnosti. Během aktivity online se o každém uživateli ukládá značné množství informací, které mohou měnit vlastníky bez vědomosti samotných osob, kterých se tyto informace týkají. V médiích se stále častěji mluví o možnosti zneužití těchto dat, především ve spojitosti se společnostmi typu Google a Facebook, jejichž obchodním modelem je poskytovat reklamu šitou na míru na základě informací, které jim jejich samotní uživatelé více, či méně dobrovolně poskytnou. Malá pozornost je však věnovaná společnostem, které shromažďují data o návštěvnících menších stránek, jejichž primárním cílem není sbírat osobní údaje, přesto i návštěvou těchto webů jsou vytvářeny osobní údaje se kterými je dále nakládáno. Existují společnosti specializující se na získávání údajů s cílem jejich kapitalizace. Z osobních údajů získaných online se tedy stává komodita, která je však obchodována bez vědomosti jejích tvůrců. Pokud samotný uživatel stránek neví o zanechávání osobních údajů na různých stránkách, je jen malá pravděpodobnost, že z toho bude, na rozdíl od obchodníků s osobními údaji, profitovat.	

Téma je doposud zpracováno v menší míře v podobě článků v novinách, magazínech a odborných periodicích. Dle mojí rešerše neexistuje kniha věnující se pouze tématu „personal data trading“ či „personal data brokers“. Díky svojí aktuálnosti lze najít několik reportů na uvedené téma vydaných veřejnými orgány po roce 2005.

Předpokládaný cíl práce, případně formulace problému, výzkumné otázky nebo hypotézy (max. 1800 znaků):
Cílem práce je zanalyzovat praxi obchodníků s osobními údaji získanými online a zanalyzovat právní regulaci tohoto, relativně neznámého, trhu; dále posoudit legalitu a legitimitu tohoto business modelu.

Předpokládaná struktura práce (rozdělení do jednotlivých kapitol a podkapitol se stručnou charakteristikou jejich obsahu)**:**

Úvod-cíl práce, metodika, prameny, dosavadní stav bádání

Průmysl s osobními údaji- kde a jak se získávají osobní údaje, klíčoví hráči na světovém a českém trhu

Právní ochrana osobních údajů-definice osobních údajů, analýza právních předpisů ČR, EU, USA s ohledem na regulaci obchodování osobních údajů, problematika zastaralosti současného práva s ohledem na digitální svět a možnost aplikace práva na záležitosti spojené s moderními trendy

Férovost business modelu- odměny pro poskytovatele osobních údajů, přiměřenost odměny pro uživatele za jejich data, alternativy k současnému mainstreamovému proudu, budoucí trendy

Závěr-shrnutí, další potenciální směr výzkumu

Bibliografie

Vymezení podkladového materiálu (např. titul periodika a analyzované období)**:**

Vzhledem k faktické neexistenci hranic na Internetu, bude třeba využít analýzu nejen národních

právních norem, ale i tu evropskou a mezinárodní. Pro splnění cíle práce bude potřeba zanalyzovat lidskoprávní dokumenty, zaručující ochranu soukromí a dále také normy, jejichž objektem je regulace obchodování s daty. Práce bude zaměřena primárně na evropskou praxi, avšak s ohledem na dominantní pozici USA v oblasti nových medií bude nutné zaměřit se i na praxi v této zemi; proto bude třeba získat z odborných knih a článků informace týkající se obchodní činnosti společností specializujících se na data trading. Práce se bude zabývat především aktuálním stavem a prognózou do budoucna.
Metody (techniky) zpracování materiálu: Analýza právních předpisů a business modelu, komparace norem, dedukce
Základní literatura (nejméně 5 nejdůležitějších titulů k tématu a metodě jeho zpracování; u všech titulů je nutné uvést stručnou anotaci na 2-5 řádků)**:** Data Brokers, A Call for Transparency and Accountability, Federal Trade Commission - obsáhlá a doposud nejaktuálnější analýza amerického trhu, kterou vydal regulátor v USA v roce 2014, upozorňující na hrozby současného stavu (www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf) The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information, Paul N.Otto, AnnieI Antón, David L. Baumer, North Carolina State University Technical Report (https://www.semanticscholar.org/paper/The-ChoicePoint-Dilemma-How-Data-Brokers-Should-Otto-Ant%C3%B3n/43685dba37726d66a071d7844f9ab0b9057180bd/pdf) – Praktický studie fungování společnosti (data broker), která přeprodává získané osobní údaje dalším subjektům. Ve studii jsou popsány hrozby, které hrozí uživatelům a doporučení pro obchodníky s informacemi. Příručka evropského práva v oblasti ochrany údajů, Agentura Evropské unie pro základní práva, Rada Evropy, 2014 (https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=15363) –podrobná příručka evropské legislativy věnující se ochraně osobních údajů, rozebírá osobní údaje z mnoha úhlů pohledu, včetně pozice zpracovatelů a správců osobních údajů, právní teorie ohledně platného souhlasu se zpracováním osobních údajů nebo např. právní apekty pohybu údajů mezi různými státy

Zákon č. 101/2000 Sb., o ochraně osobních údajů v aktuálním znění
Český právní akt věnující se ochraně osobních údajů, obsahující práva a povinnosti subjektů nakládání s osobními údaji, včetně sankcí za případné porušení této normy. Ve spojitosti s českými lidsko-právními dokumenty tvoří kostru české úpravy.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
-nová směrnice Evropské komise o ochraně osobních údajů vstupující v účinnost 5.5.2016 (členské státy Evropské unie musí novou úpravu transponovat nejpozději do 5.5.2018) bude spolu s nařízením Evropského parlamentu a Rady č. 2016/679 tvořit kostru evropské právní úpravy.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
-nové nařízení Evropského parlamentu a Rady č. 2016/679 bude, spolu se směrnicí Evropské komise č. 2016/680 o ochraně osobních údajů, tvořit kostru evropské právní úpravy, a tedy, díky své povaze přímo závazného právního dokumentu, bude klást povinnosti na subjekty spadající do působnosti práva Evropské unie.

Compromised Data, From Social Media to Big Data, Axel Bruns, et al., Bloomsbury Academic, 2015
-Kniha popisuje změnu sociálních webů ve spojitosti s ekonomckými aktivitami. Autoří, mimo jiné hovoří o digitálním osvícenstv, které však bylo změněno ekonomickou motivací, jelikož provozovatelé sociálních sití provádí extenzivní social data mining

Convergent Media and Privacy, Tim Dwyer, Palgrave Global Media Policy and Business, 2015
-Profesor na The University of Sydney rozvádí znepokojivou praxi medií v oblasti osobních

údajů ohrožující soukromí digitálních občanů (digital citizens). Kniha obashuje konrétní příklady z oblasti správy osobních dat, mobilních aplikací a reklamy.

Vzhledem k rychlému technologickému rozvoji budu často čerpat z aktuálních odborných článků.

Diplomové a disertační práce k tématu (seznam bakalářských, magisterských a doktorských prací, které byly k tématu obhájeny na UK, případně dalších oborově blízkých fakultách či vysokých školách za posledních pět let)

Přeshraniční zpracování osobních údajů v sociálních sítích, Vojtěch Martinka, 2016

Ochrana osobních údajů, Mgr. Martin Šolc, 2014

Ochrana osobních údajů online, Jakub Míšek 2014

Ochrana osobních údajů na internetu podle práva Evropské unie, Mgr. Edita Krejčířová, 2013

Ochrana dat na sociálních sítích, Jana Mikšíčková, 2012

Datum / Podpis studenta/ky

16.5.2016

……

TUTO ČÁST VYPLŇUJE PEDAGOG/PEDAGOŽKA:

Doporučení k tématu, struktuře a technice zpracování materiálu:

Případné doporučení dalších titulů literatury předepsané ke zpracování tématu:

Potvrzuji, že výše uvedené teze jsem s jejich autorem/kou konzultoval(a) a že téma odpovídá mému oborovému zaměření a oblasti odborné práce, kterou na FSV UK vykonávám.

Souhlasím s tím, že budu vedoucí(m) této práce.

……

Příjmení a jméno pedagožky/pedagoga Datum / Podpis pedagožky/pedagoga

Obsah

Obsah *1*

Seznam zkratek *1*

Úvod *2*

Představení tématu **2**

Cíl práce **3**

Použité zdroje **4**

Shrnutí obsahu **5**

1. Mediální diskurz digitálních médií a ochrany osobních údajů *7*

2. Rizika při obchodování s osobními údaji *10*

3. Obchodníci s osobními údaji *14*

3.1. Jaké údaje jsou sbírány **14**

3.2. Jak jsou údaje sbírány **15**

3.3. Využití údajů od data brokers **24**

4. Právní regulace obchodu s osobními údaji *28*

4.1. Právní regulace v Severní Americe **28**

4.1.1. USA 28

4.1.2. Kanada 32

4.2. Právní regulace v EU **33**

4.2.1. Definice osobních údajů 37

4.2.2. Současná regulace v EU 40

4.2.3. Regulace v EU od května 2018 46

5. Legitimita obchodování s osobními údaji *51*

5.1. Etika v době nových médií **51**

5.2. Konflikt práva na svobodu podnikání a práva na ochranu soukromí **52**

5.3. Konflikt informačních práv a práva na ochranu osobnosti **53**

6. Alternativní a budoucí trendy *55*

6.1. Rozšíření definice osobní informace 55

6.2. Samoregulace 56

6.3. Odměna za poskytnutí osobních údajů 58

Závěr 61

Summary 69

Bibliografie 71

Právní normy 71

Použitá literatura 72

Seznam příloh 81

Přílohy 81

Seznam zkratek

AEPD	Agencia Española de Protección de Datos
BDSG	Bundesdatenschutzgesetz
FCRA	Fair Credit Report Act
FTC	Federal Trade Commission
FTCA	Federal Trade Commission Act
GDPR	General Data Protection Regulation
GLBA	Gramm Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
ICT	Information and Communication Technologies
MPAA	Motion Picture Association of America
PIPEDA	Personal Information Protection and Electronic Documents Act
SDEU	Soudní dvůr Evropské Unie

Úvod

Představení tématu

V současném světě hraje Internet klíčovou roli snad v každém odvětví lidské činnosti. Lidé na internetu nakupují potraviny i dovolenou, plánují cestu po městě i do zahraničí, vyhledávají informace o nemocech, komunikují a s přáteli i s orgány státní moci, hledají a vykonávají zaměstnání, čtou noviny, sledují seriály a mnoho dalších věcí. Během aktivity online se o každém uživateli ukládá značné množství informací. Ty mohou měnit vlastníky bez vědomosti samotných osob, kterých se tyto informace týkají. V médiích se stále častěji mluví o možnosti zneužití těchto dat, především ve spojitosti se společnostmi typu Google a Facebook, jejichž obchodní model je postaven na příjmech z reklamy, šité na míru na základě informací, které samotní uživatelé více, či méně dobrovolně poskytnou. Malá pozornost je však věnovaná společnostem, jež shromažďují data, která o sobě uživatelé nepublikují veřejně. Jedná se například o informace o návštěvnících stránek, jejichž primárním cílem není sbírat osobní údaje. Nicméně, pouhou návštěvou těchto webů jsou vytvářeny údaje týkající se konkrétních osob, typicky ve formě cookies, se kterými lze dále nakládat. Kromě webových stránek jsou osobní údaje získávány i z dalších zdrojů, jako jsou veřejně dostupné databáze, online dotazníky, informace o uskutečněných online transakcích, použitím mobilních aplikací, počítačových programů nebo třeba použitím fitness hodinek, zaznamenávajících polohu a tep uživatele. Získané informace jsou různě kombinovány za účelem vytvoření uceleného profilu osob, který je pak komerčně používán především pro marketingové účely. Získané informace neslouží jen k popisu status quo, ale i k predikování budoucího chování lidí.

Big data is big business.[1] Informace jsou považovány za nejcennější komoditu současnosti.[2] Použití big data může přinést mnoho prospěšných informací, ať už

[1] *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. Dostupné z: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf Str. 41-42.

[2] Autor neuveden. *Regulating the internet giants: The world's most valuable resource is no longer oil, but data | The Economist:* [online]. The Economist Newspaper Limited, vyd. 2017-05-06 [cit. 2017-05-16].

společnosti jako celku, nebo jednotlivým obchodním společnostem. Big data, ale mohou také představovat hrozbu pro soukromí jednotlivců, o čemž pojednává tato diplomová práce. Z dostupných informací vyplývá, že množství osobních údajů, se kterými se obchoduje, je ohromný. Přesné informace o globálním trhu však známé nejsou, protože data brokers příliš informací o svém businessu neposkytují. Ani osoby, o jejichž údaje se jedná, nevědí, že je s jejich daty obchodováno. Pro ilustraci lze uvést, že američtí data brokers mají tisíce záznamů o téměř každém člověku ve Spojených státech. V roce 2014 jeden data broker uvedl, že každý měsíc do své databáze přidává 3 miliardy nových záznamů. Jiná společnost uvedla, že vlastní informace o 1,4 miliardě maloobchodních transakcí a její databáze obsahuje přes 700 miliard datových záznamů. Ukázka, co všechno může být takovým datovým záznamem, je v příloze na konci diplomové práce. Opravdový rozsah tohoto businessu v USA je však skryt před zraky samotných lidí i státních orgánů, protože data brokers nemusí zveřejňovat, jaké informace vlastní.

Toto multidisciplinární téma z oblasti médií, práva, ICT a businessu jsem si vybral kvůli dlouhodobému zájmu o problematiku ochrany osobních údajů. Po použití analytického nástroje Ghostery, který ukazuje, jakým společnostem webové stránky poskytují informace o mé návštěvě, jsem se začal zajímat o to, kdo jsou tyto společnosti a k čemu jim slouží získané informace. Tímto způsobem jsem objevil skrytý svět data brokers.

Cíl práce

Prvním cílem této diplomové práce je analýza trhu s osobními údaji získanými online a poodkrytí praxe společností specializujících se na *personal data mining* za účelem pozdější kapitalizace. Z osobních údajů se stává komodita, problémem však je, že osoby, jichž se údaje týkají, mají jen malou šanci zjistit, že jejich osobní údaje jsou předávány bez jejich souhlasu či dokonce vědomí. Druhým cílem této práce je zjistit, zda, případně jak je tento business regulován v Evropské unii a ve světě a jaké jsou možnosti obrany osob, které si nepřejí, aby s jejich údaji bylo obchodováno. Vzhledem

---

Dostupné z: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

k faktu, že právo EU komplexně pokrývá problematiku data brokers ve členských státech EU, není v práci věnována české úpravě zvláštní kapitola.

Práce se nezabývá zpracováním osobních údajů ve spojitosti s veřejnou mocí. Neobsahuje tedy analýzu praxe či regulace týkající se spolupráce orgánů v trestních či správních záležitostech, a to ať už vnitrostátní či mezinárodní. Práce si dále neklade za cíl podrobně či úplně obsáhnout technologickou stránku získávání osobních údajů v online prostředí, jelikož jak čtenář brzy pochopí, existují desítky metod, kterými lze osobní data získávat bez vědomí samotných osob.

Diplomová práce se zabývá rychle se vyvíjecími tématy, ICT a právní regulací, je tedy pravděpodobné, že obsah diplomové práce rychle zastará.

Použité zdroje

Téma je doposud zpracováno v menší míře v podobě článků v novinách, magazínech a odborných periodikách. Dle mé rešerše neexistuje kniha věnující se pouze tématu „personal data trading“ či „personal data brokers“. Anglicky psané odborné články se začínají objevovat od roku 2005.

Pro zpracování diplomové práce jsem používal primárně anglicky psané zdroje, a to především vědecké články, reporty a tiskové zprávy státních i nadnárodních organizací a volně dostupné právní analýzy. Pro analýzu amerických data brokers hrály nezastupitelnou roli dva detailní reporty[3], ve kterých jsou popsány metody a rozsah obchodu s osobními údaji. Dále jsem použil evropské směrnice a nařízení na ochranu osobních údajů, spolu s několika českými, americkými, kanadskými a německými zákony na toto téma. V menší míře jsem využíval informace ze serózních periodik, která jsem použil především pro lepší pochopení méně známých témat a pro ilustraci, jak jsou tato témata pokryta v cizích zemích.

[3] Jsou jimi Data Brokers: A Call for Transaparency and Accountability a *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes.*

Vzhledem k tématu práce se zde často vyskytuje anglická terminologie, která převažuje i v neanglicky psané literatuře. Tyto pojmy jsou vysvětlené nebo přeložené, tak aby tématu porozuměl i neinformovaný čtenář. Některé pojmy jsou však ne zcela jasně definované nebo definic existuje více a terminologie není vždy konzistentní. Samotní obchodníci s osobními údaji jsou v literatuře označováni jako (personal) data traders, (personal) data brokers, data services providers, information broker a jinak. [4]

Pro snadnější referenci, v případě použití zdrojů ve formátu pdf, jsou v citacích čísla stran, která jsou uvedena v programu na práci s tímto formátem.

Shrnutí obsahu

Práce je rozdělena, kromě tohoto úvodu a závěru, do dalších 6 kapitol.

V první kapitole je obsaženo teoretické shrnutí problematiky z pohledu mediální teorie. Konkrétně se zde zabývám přechodem od tradičních médií k novým médiím, Webem 2.0 a pojmem big data. Všechny tyto oblasti úzce souvisí s komerčním zpracováváním osobních údajů v online prostředí a jejich následnou kapitalizací.

Ve druhé kapitole popisuji rizika, která přináší doba digitálních médií pro fyzické osoby. V této kapitole jsou popsány některé negativní jevy, které souvisí s činností data brokers a v širším kontextu i data mining v době nových medií.

Ve třetí kapitole se zabývám praxí společností, jež ve velkém měřítku využívají osobní údaje pro dosažení zisku. Ukázány jsou zde některé metody, kterými dochází ke sběru dat. Dále zde popisuji různé zdroje, ze kterých jsou data získávána a možnost následného použití produktů data traders.

[4] *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. Dostupné z: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. *S*tr. 43.

Ve čtvrté kapitole je analyzována normativní stránka činnosti data traders. Vzhledem k pozici USA jako světového leadera v oblasti digitálních technologií, sociálních sítí i nových médií, se zabývám v této kapitole analýzou právních norem, které dopadají na americké data brokers. Vzhledem ke geografické a částečně i kulturní blízkosti USA a Kanady se zde také krátce zabývám odlišným přístupem k ochraně osobních údajů v Kanadě.
Evropská unie se naopak jeví jako leader v ochraně soukromí svých občanů, z tohoto důvodu je dále podrobně rozebrána současná právní úprava regulující činnost obchodníků s osobními údaji na území členských států. Vzhledem k důležité právní reformě ochrany osobních informací se zabývám i novým nařízením, které bude od 25. května 2018 sjednocovat ochranu osobních údajů na území celé Evropské unie a v některých případech i mimo Unii.

V páté kapitole jsou představeny možné pohledy na činnost data traders. Podobně jako v jiných podnikatelských činnostech i zde dochází ke konfliktu protichůdných zájmů občanů, obchodních společností a států. Primárním účelem data brokers je dosahování zisku. Občané mají zpravidla zájem na ochraně svého soukromí. Moderní právní stát by měl nastavit normativní prostředí, tak aby tyto dva zájmy byly vybalancované pro spokojenou koexistenci společností i občanů. Do tohoto rozdělení zájmů však zasahují zájmy některých jiných subjektů nebo s nimi kolidují jiná práva přiznaná státem. Právo občana na soukromí může kolidovat nejen s právem společnosti na svobodné dosahování zisku, ale i s právem na přístup k informacím nebo právem na svobodu projevu.

V šesté kapitole poukazuji na vypozorované trendy, které, podle mého názoru, budou v blízké budoucnosti formovat regulaci data brokers a ochranu osobních údajů. Ačkoliv jsem si vědom, že tyto budoucí prognózy mohou být značně nepřesné[5] a při zpětném ohlédnutí i úsměvné, lze v obchodování s osobními údaji pozorovat faktory, které naznačují, jak by mohl tento trh vypadat v následujících letech.

[5] TALEB, Nassim Nicholas. *The black swan: the impact of the highly improbable*. New York: Random House, 2007. 366 s. ISBN 978-140-0063-512. Kap. 10-13.

1. Mediální diskurz digitálních médií a ochrany osobních údajů

S vývojem digitálních technologií a především internetu dochází k projekci těchto inovací i do oblasti mediálních studií. Specializovaným mediálním oborem jsou tzv. „*nová média*“, která se vymezují především oproti tzv. „*tradičním médiím*“. Pojem nová média, není, podle mého názoru, zcela jasně definován. V době psaní této práce zahrnuje především digitální formy médií, tedy ty, jež lze zaznamenat pomocí binárního kódu, a proto i snadno kopírovat bez ztráty kvality. Mezi konkrétní formy nových médií pak patří, ku příkladu, digitální fotografie, audiovizuální díla, počítačové hry, virtuální realita, e-books či internet.[6] S pokračujícím technologickým vývojem se samozřejmě posunuje vnímání toho, co je nové. Digitální fotografie byla cirka před 15 lety novou technologií, v současnosti je standardem, jak mezi amatérskými fotografy, tak i mezi profesionály. Podobný osud jistě potká i ostatní nová média. Internet je v současnosti médiem, bez něhož se neobejde žádná rozvinutá společnost. Vzhledem k faktu že na internetových stránkách lze najít extrémní množství informací na jakékoliv téma a zároveň lze skrze něj sledovat i ostatní digitální média, nelze mu upřít nadřazené postavení v současné společnosti. Rapidní rozvoj digitálních médií a internetu je dokonce někdy označován jako *digitální revoluce*.[7]

Zhruba od roku 2004 hovoří mediální teoretici o nástupu Webu 2.0. Tento pojem označuje především dobu technologického a sociologického posunu, souvisejícího se změnou tvorby obsahu webových stránek a chování uživatelů na internetu. Dřív, v době Webu 1.0, byl standardní model, že provozovatelé webů tvoří veškerý obsah. Pokud byl tento obsah dostatečně zajímavý, mohl přilákat velké množství odběratelů. Ačkoliv

[6] MANOVICH, Lev. *The language of new media*. [online]. MIT Press, 2001 [cit. 2017-03-06]. Dostupné z: http://faculty.georgetown.edu/irvinem/theory/Manovich-LangNewMedia-excerpt.pdf. Str. 5-10.

[7] POVEJŠIL, Tomáš. *Právní regulace dostupnosti digitálního obsahu mladistvým*. Brno, 2014. Diplomová práce. Masarykova univerzita. Vedoucí práce Radim Polčák. Str. 8-9.

i před rokem 2005 existovala internetová fóra a chat, informace na internetu tekly primárně jedním směrem, a to od provozovatele webu k publiku.[8]

V současnosti provozovatelé webů stále častěji návštěvníkům nabízejí infrastrukturu pro sdílení informací s jinými návštěvníky. Uživatelé tuto infrastrukturu dobrovolně používají, vytvářejí tak obsah spolu s provozovatelem, anebo i bez jeho přispění. Zároveň je na Webu 2.0 interakce mezi uživateli snadnější a častější. Informace se proto nešíří jen lineárně, ale spíše všemi směry mezi samotnými uživateli. S odbouráváním technologických překážek, bylo stále snadnější a uživatelsky příjemnější publikovat vlastní obsah. Prostor online přestal být obskurním místem, tak jak tomu bylo v počátcích internetu. Online obsah začali běžně vytvářet i „normální lidé“,[9] ne jen skupina počítačových nadšenců.[10] Změna publika se v anglicky psaných publikacích označuje jako přeměna od *consumers* na *prosumers*, respektive od *usage* na *produsage*.[11]

Spolu se záměrným zanecháváním digitálních artefaktů, v podobě internetových obsahů, za sebou začali uživatelé/tvůrci zanechávat i nechtěnou digitální stopu, a to v podobě osobních údajů.

V současné době se v oboru nových médií hovoří o big data, ačkoliv jednotná definice pojmu big data neexistuje.[12] Oxfordský slovník tento pojem definuje jako:

„*Extrémně velký soubor dat, který může být analyzován pomocí počítačů a zároveň má potenciál odhalit vzory, trendy and spojitosti týkající se především lidského chování a komunikace.*“ [13]

---

[8] O'REILLY, Tim. *What Is Web 2.0 - O'Reilly Media:* [online]. O'Reilly Media, 2005 [cit. 2017-03-06]. Dostupné z: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

[9] FUCHS, Christian, Anders ALBRECHTSLUND a Marisol SANDOVAL, ed. *Internet and surveillance: the challenges of Web 2.0 and social media*. Abingdon, Oxon: Routledge, 2012. Routledge studies in science, technology and society, 16. ISBN 978-0-415-89160-8. Str. 3-6.

[10] Nebýt toto diplomová práce, hodilo by se slovo „geekové“.

[11] JENSEN, Klaus, ed. *A handbook of media and communication research: qualitative and quantitative methodologies*. Oxon: Routledge, 2012. ISBN 978-0-415-60965-4. Str. 77, 100-101.

[12] DUTCHER, Jennifer. *What Is Big Data? - Blog:* [online]. Vyd. 2014-09-03 [cit. 2017-03-05]. Dostupné z: https://datascience.berkeley.edu/what-is-big-data/

[13] *Big data - definition of big data in English | Oxford Dictionaries:* [online]. [cit. 2017-03-05]. Dostupné z: https://en.oxforddictionaries.com/definition/big_data

Big data souvisí nejen s tím, že každý může tvořit obsah na internetu, s rozvojem sociálních sítí, ale především s rozmachem použití počítačů na denní bázi čím dál tím více lidmi. Toto vše má za následek exponenciální přibývání dat.[14] Big data mohou být vnímána pozitivně i negativně. Existuje nespočetně možností pozitivních aplikací big data, od zdravotnictví[15], přes ochranu životního prostředí[16], po zvyšování efektivity společností.[17] Stinnou stránkou získávání a využívání big data je, mimo jiné, potenciál omezit osobních svobody, především ve formě zásahu do soukromí ze strany veřejných i soukromých organizací.[18]

Odborníci využívající big data komerčně, poukazují nejen na množství dat, ale i na nutnost použití analytických nástrojů k jejich interpretaci, na rozmanitost zdrojů, odkud data pochází a na širokou paletu možností a otázek, pro které lze big data použít. Společnosti sbírají velké množství dat o svých zákaznících a produktech, aniž by je v současné době potřebovali. Avšak počítají s tím, že všechna data mohou nalézt uplatnění v budoucnu[19], pokud by se vyskytly otázky, které nejsou v současnosti myslitelné. Ačkoliv ne všechny big data obsahují osobní údaje, přináší současná doba nejvíce otázek a problémů spojených s ochranou osobních informací v historii lidstva.

---

[14] BOYD, Danah a Kate CRAWFORD. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication, & Society* [online]. **15**(5), 32 s. [cit. 2017-03-06]. Dostupné z: www.danah.org/papers/2012/BigData-ICS-Draft.pdf. Str. 2-6.

[15] ALTMAN, Russ. What really happens when you mix medications? *TED.com* [online]. [cit. 2017-03-07]. Dostupné z: https://www.ted.com/talks/russ_altman_what_really_happens_when_you_mix_medications

[16] BREGGIN, Linda a Judith AMSALEM. Big Data and Environmental Protection: An Initial Survey of Public and Private Initiatives [online]. Washington, 2014, 1-32 [cit. 2017-03-07]. Dostupné z: https://www.eli.org/sites/default/files/eli-pubs/big-data-and-environmental-protection.pdf. Str. 31.

[17] Autor neuveden. *Big data, artificial intelligence, machine learning and data protection* [online]. Information Commissioner's Office, 2014 [cit. 2017-03-07]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Str. 16.

[18] BOYD, Danah a Kate CRAWFORD. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication, & Society* [online]. 15(5), 32 s. [cit. 2017-03-06]. Dostupné z: www.danah.org/papers/2012/BigData-ICS-Draft.pdf. Str. 3, 15.

[19] DUTCHER, Jennifer. *What Is Big Data? - Blog:* [online]. Vyd. 2014-09-03 [cit. 2017-03-05]. Dostupné z: https://datascience.berkeley.edu/what-is-big-data/

2. Rizika při obchodování s osobními údaji

Pomineme-li nepříjemný pocit, který může být spojen se sběrem osobních informací, existují i objektivní rizika spojená s použitím personálních informací.

Tato rizika mohou mít negativní ekonomické nebo reputační následky. Mezi ekonomické patří, ku příkladu, praxe některých internetových obchodů rozlišovat klienty na základě osobních informacích a podle jejich ekonomických profilů jim stejné produkty nabízet za různé ceny.[20] Ve spojených státech je také praxí tvořit tzv. „*bad-tenant lists*, tedy seznamy „špatných nájemců nemovitostí“. Společnosti, které tyto seznamy provozují, pak umožní za poplatek pronajímatelům přístup do své databáze, ve které může být např. informace o ekonomické situaci, počtu dětí, rase nebo trestní historii nájemců.[21] Na základě toho si může pronajímatel vybrat „vhodného“ nájemníka. Negativní stránkou pro nájemce je však ztížená situace při hledání pronájmu, patří-li do skupiny, se kterou pronajímatele neradi uzavírají smlouvy. Tímto může samozřejmě dojít i k prodražení bydlení.[22] Jiným příkladem negativních ekonomických následků, zná-li obchodník příliš mnoho osobních informací, je vyšší cena letenek pro stálé zákazníky (frequent flyers) letecké společnosti Delta[23], nebo vyšší ceny za ubytování

[20] VALENTINO-DEVRIES, Jennifer; et al. Websites Vary Prices, Deals Based on Users' Information. *The Wall Street Journal* [online]. Vyd. 2012-12-24 [cit. 2016-08-23]. Dostupné z: http://www.wsj.com/news/articles/SB10001424127887323777204578189391813881534

[21] *PIPEDA Report of Findings #2016-002: Property management company agrees to scrap "bad tenant list"* [online]. 2016 [cit. 2016-08-29]. Dostupné z: https://www.priv.gc.ca/cf-dc/2016/2016_002_0219_e.asp

[22] Jedná se o zajímavý příklad rozporu práva na ochranu oprávněných zájmů pronajímatelů vybrat si vhodného nájemce a práva nájemců na bydlení za nediskriminačních podmínek.. V Kanadě jsou bad-tenants lists ilegální.

[23] SANBURN, Josh. *Delta Appeared to Overcharge Frequent Flyers for Weeks – Was That Legal?*. Time Inc. [online]. Vyd. 2012-05-21 [cit. 2017-04-08]. Dostupné z: http://business.time.com/2012/05/21/delta-overcharged-frequent-flyers-for-weeks-was-that-legal/

v hotelech na portálu Orbitz.com pro uživatele počítačů Apple ve srovnání s „chudšími“ uživateli Windows. [24]

Reputační riziko představuje použití soukromých informací a osobních detailů pro účely, které mají negativní následky, primárně společenské, ty se ale mohou sekundárně přenést i do ekonomické sféry. Příkladem může být neprodloužení pracovní smlouvy, dozví-li se zaměstnavatel o chorobě nebo militantních názorech zaměstnance, či ku příkladu negativní odezva komunity, dozví-li se o milostném poměru vdané ženy. Pomocí analytických nástrojů je možné tyto informace o osobě zjistit, aniž by samotná osoba informaci zveřejnila. Americký maloobchodní řetězec Target využívá statistickou analýzu chování zákazníku tak, že dokáže rozpoznat nastávající matky a inzerovat jim dětské zboží ještě před narozením potomka.[25] Pomocí digitálních medií se informace mající potenciál způsobit finanční nebo reputační riziko mohou šířit velmi rychle a je velmi obtížné jednou vypuštěnou informaci zcela odstranit.

Nebezpečím pro uživatele internetu je nejen použití jejich informací pro netransparentní účely neidentifikovanými společnostmi, ale i praktická nemožnost samotných uživatelů tyto informace obdržet nebo měnit. V důsledku je tedy velmi obtížné se bránit proti nežádoucím aktivitám těchto společností. Data traders působící ve Spojených státech se liší rozsahem, ve kterém lidem umožnují přístup k jejich informacím. Někteří[26] neposkytují přístup žádný s odůvodněním, že data nejsou přiřaditelná ke konkrétní osobě. Některé[27] poskytují přístup a možnost změnit jen ta data, která pocházejí z jejich vlastní činnosti (tedy nevztahuje se na data získaná od třetích stran). Některé[28] poskytují přístup i možnost změnit informace o své osobě, po zadání šesti „autentifikačních“

[24] WHITE, Martha. *Orbitz Shows Higher Prices to Mac Users*. Time Inc. [online]. Vyd. 2012-06-26 [cit. 2017-04-08]. Dostupné z: http://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/?iid=pf-main-mostpop1/

[25] DUHIGG, Charles. *The power of habit: why we do what we do in life and business*. New York: Random House, 2012. 353 s. ISBN 978-1-4000-6928-6. Str. 193-197. Kniha pokračuje příběhem, ve kterém se otec středoškolačky dotazuje společnosti Target, proč byla adresátkou inzerce pro nastávající matky. Až později se otec dozvěděl, že dcera byla opravdu těhotná.

[26] Experian, Equifax

[27] Rapleaf

[28] Acxiom

osobních informací[29], přičemž vymazat lze jen některá data. Číst, ani měnit však nelze informace odvozené z fakt, například informace, že osoba je rodič a zaměstnanec lze číst i měnit, nelze však získat přístup k odvozené informaci, že osoba je pracující rodič.[30] Tímto tedy reálná možnost ovlivnit jaké osobní informace jsou zpřístupňované je mizivá, zvláště s přihlédnutím k faktu, že data traders osoby, resp. jejich informace zařazují do různých seznamů podle charakteristik, které vznikly syntézou osobních údajů. Některé[31] společnosti nabízejí možnost opt-out, tedy zažádat o vyřazení z databáze. Tyto společnosti však uvedly, že všechna data o lidech vymazána nebudou, jelikož by tyto osoby nemohly být v budoucnu identifikovány, a tedy ani dodrženo jejich přání opt-out.[32] Jedná se proto spíše o zákaz dalšího nakládání s údaji.

S tímto lze identifikovat několik rizik:

- člověk musí aktivně zjišťovat u jakých společností jsou jeho data spravována a není zde jistota, že obsáhl veškeré data traders
- prakticky nelze zkontrolovat, jak je s daty nakládáno, tedy jestli byla vymazána, nebo zda nebyla po opt-out žádosti prodána či jinak poskytnuta jinému subjektu, který neuplatňuje opt-out politiku
- není jasné, zda je opt-out účinný pro všechny účely nebo jen pro nějaké

Někteří obchodníci s osobními údaji řadí svou populaci do segmentů podle ekonomické výkonnosti. To umožňuje marketingovým společnostem přesnější zaměření nabízených

[29] Lze pochybovat, že zadání jména, příjmení, adresy, data narození, e-mailové adresy a čtyř čísel ze social security number (zjednodušeně řečeno se jedná o obdobu rodného čísla) slouží jen pro autentifikaci osob.

[30] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 39-40.

[31] Acxiom, Epsilon, Experian

[32] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 41.

výrobků relevantním zákazníkům. Segmenty jsou v některých případech velmi expresivně označeny podle charakteristik a finanční situace jejich členů, například *Rocky Road* (Kamenitá cesta), *Rural and Barely Making It* (Vesničani, co to sotva zvládají), *Hard Times* (Težký časy) nebo *Small Town Shallow Pockets* (Malé město, malá kapsa).[33]

Data lze samozřejmě archivovat a kdykoliv použít. S tím se pojí riziko, že osoby, kterých se data týkají, budou v budoucnosti vystaveny negativním následkům během aktivit, které dnes ani neexistují.

Z výše uvedeného vyplývá, že hromadné sbírání osobních údajů vystavuje osoby finančnímu a reputačnímu riziku. Vzhledem k technologickému pokroku nelze ignorovat ani budoucí rizika spojená se sběrem „dnešních" informací, která budou použita v budoucnosti. Uživatelé internetu však mají značně omezené možnosti zjistit rozsah osobních informací, které jsou dostupné třetím osobám, natož se bránit transakcím s těmito daty.

[33] Tamtéž str. 30.

3. Obchodníci s osobními údaji

3.1. *Jaké údaje jsou sbírány*

Doposud nejpodrobnější publikace mapující praxi data brokers v USA uvádí přes 250 kategorií[34] osobních údajů, které jsou sbírány a dále využívány. Jedná se o velmi konkrétní údaje, které zahrnují:

- demografické údaje, mj. jméno, věk, pohlaví, místo bydliště, telefonní čísla, emailové adresy, počet a věk dětí, rodinný stav, vzdělání, profese, příjem, politické názory
- zdravotní stav, mj. zda osoba trpí jednou ze 44 chorob, včetně roztroušené sklerózy, rakoviny, deprese, cukrovky, vysokého krevního tlaku aj.[35]; zda používá projímadla či prostředky proti kvasinkové infekci[36]
- informace o nákupech a provedených transakcích, mj. zda byl nákup proveden online či v obchodě, jak často osoba nakupuje, zda zakoupila konkrétní výrobek v minulosti, jakou značku automobilu vlastní, jakou kartou platí a kdy byla karta vydána[37]
- popis chování osob, mj. jak často a jak daleko cestují, zda kouří, jak často pili konkrétní whisky v posledních 30 dnech, zda vlastní domácí zvířata, zda přispívají na charitu, jaké mají pojištění, kolik přátel mají na sociálních sítích, zda sledují Youtube videa či raději čtou romány[38]

---

[34] Viz Příloha 1 této práce. EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Str. 97-100.

[35] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 19-20.

[36] Tamtéž str. 20.

[37] Tamtéž str. 19-20.

[38] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18].

Data brokers využívají data dostupná online i offline.[39] Zároveň dokáží sjednotit různé online zdroje do jedné databáze.[40] Tímto dojde ke spojení původně oddělených informací, s čímž subjekt údajů nemusí být vždy srozuměn a souhlasit.

Obchodníci s osobními údaji využívají pro svůj business tři druhy informací, a to fakta, která sesbírají od svých zdrojů, informace odvozené od těchto fakt a na základě fakt vykonstruované domněnky. Do druhé kategorie lze zařadit se známými fakty pravděpodobně korelující neznámá fakta. Příkladem může být situace, kdy respondent vybere, že chce být oslovován „slečna“, pak je vysoce pravděpodobné, že se jedná o ženu, a navíc svobodnou. Třetí kategorie je vytvořená na základě fakty podložených domněnek[41], například z faktu, že osoba je starší než 65 let, se na základě průměrné populace lze odůvodněně domnívat, že nekupuje hormonální antikoncepci nebo snowboardové vybavení. Tyto domněnky jsou však podložené statistickými modely a psychologickými studiemi, dokáží proto osoby charakterizovat na základě jejich chování a do jisté míry dokonce predikovat jejich chování i v budoucnu.[42]

3.2. *Jak jsou údaje sbírány*

Existuje několik zdrojů osobních údajů. Jedním z nich jsou veřejně dostupné databáze a rejstříky. Ve Spojených státech lze získat data mj. ze sčítání obyvatel, katastrálního úřadu, soudních dokumentů, insolvenčního rejstříku, registru řidičů, přihlášky voličů[43], telefonních seznamů, matrik. O lékařích, advokátech, notářích, účetních a realitních makléřích lze získat cenné údaje z jejich licencí, které jsou veřejně dostupné

Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 20-21.

[39] Tamtéž str. 36.

[40] Tamtéž str. 37.

[41] Tamtéž str. 28.

[42] DUHIGG, Charles. *The power of habit: why we do what we do in life and business*. New York: Random House, 2012. 353 s. ISBN 978-1-4000-6928-6. Str. 182-197.

[43] V některých státech USA se voliči musí před volbami zaregistrovat; obdobně tomu je i ve Spojeném království. Více na https://www.usa.gov/register-to-vote resp. na http://www.aboutmyvote.co.uk/register-to-vote/why-should-i-register-to-vote

v licenčních rejstřících. Další informace lze získat z pilotních, rybářských či loveckých oprávnění.[44] Získávání dat (data mining) na internetu samozřejmě neprobíhá manuálně. Existují sofistikované programy a analytické prostředky, které automaticky tyto zdroje prohledávají, kategorizují a ukládají data v nich obsažená.[45]

V českém online prostředí je možné získat informace o dlužících klientech například Všeobecné zdravotní pojišťovny[46] nebo Zdravotní pojišťovny ministerstva vnitra ČR.[47] V insolvenčním rejstříku lze vyhledat dlužníky, proti kterým bylo zahájeno insolvenční řízení.[48] Zde lze najít nejen samotný záznam o dlužníkovi, ale i množství příloh, které se týkají insolvenčního řízení a které mohou dost podrobně ilustrovat dlužníkovy finanční i rodinné poměry. Mimo jiné zde lze, v závislosti na případu, najít adresu bydliště, místo a datum narození, rodné číslo dlužníka i manžela či manželky, seznam movitého a nemovitého majetku včetně jeho pořizovací ceny, finanční závazky (například úvěrové smlouvy, jejich subjekty, výši a den uzavření), vyživovací povinnost, zaměstnavatele včetně aktuální výše mzdy a příjmů za poslední 3 roky, dodavatele služeb, kterým nebylo zaplaceno či podpis dotčených osob.

V obchodním rejstříku a související sbírce listin[49] lze najít informace o právnických osobách a některých podnikajících fyzických osobách. Existence právnických společností je samozřejmě založena na existenci osob fyzických, o kterých lze v této databázi najít několik druhů informací. Kromě jména a adresy bydliště statutárních zástupců lze z účetních závěrek zjistit průměrnou mzdu zaměstnanců nebo členů orgánů

---

[44] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 21.

[45] *Data mining techniques:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.ibm.com/developerworks/library/ba-data-mining-techniques

[46] *Dlužníci - VZP ČR:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.vzp.cz/platci/dluznici

[47] Dlužníci - VZP ČR. *Dlužníci - Pojistovna 211:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.vzp.cz/platci/dluznici

[48] *Formulář pro lustraci - ISIR - Insolvenční rejstřík (U1.0.0.20A):* [online]. [cit. 2016-11-25]. Dostupné z: https://isir.justice.cz/isir/common/index.do

[49] *Veřejný rejstřík a Sbírka listin - Ministerstvo spravedlnosti České republiky:* [online]. [cit. 2016-11-25]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik

společnosti a celkovou finanční výkonnost právnické osoby, což v případě malých společností lze přímo převést na fyzické osoby figurující v těchto společnostech.

Základní informace včetně kontaktních údajů jsou online dostupné o notářích[50], advokátech a advokátních koncipientech[51], soudcích[52], insolvenčních správcích[53], daňových poradcích[54], soudních překladatelích[55] a lékařích[56]. Informace o jménech vlastníků a popřípadě spoluvlastníků nemovitostí lze online dohledat v katastru nemovitostí.[57] Placená verze dálkového přístupu do katastru nemovitostí nabízí přístup k velkému množství dalších údajů, například k cenám nemovitostí nebo vyhledávání všech nemovitostí vlastněných konkrétní osobou.[58] Existuje však mnoho dalších veřejných[59] i soukromých databází, ze kterých mohou být automatizovaně získávány osobní údaje.

Sociální sítě jsou důležitým a často používaným zdrojem osobních informací. Automatizovaný software dokáže procházet profily na sociálních sítích LinkedIn,

[50] *Seznam notářů:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.nkcr.cz/seznam-notaru

[51] *ČAK - Vyhledávání advokátů a koncipientů:* [online]. [cit. 2016-11-25]. Dostupné z: http://vyhledavac.cak.cz/Units/_Search/search.aspx

[52] *Prehled soudcu:* [online]. [cit. 2016-11-25]. Dostupné z: http://portal.justice.cz/Justice2/Soudci/soudci.html#002

[53] *Seznam insolvenčních správců - přehled:* [online]. [cit. 2016-11-25]. Dostupné z: https://isir.justice.cz/InsSpravci/public/seznamFiltr.do

[54] *Seznam daňových poradců - Komora daňových poradců ČR:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.kdpcr.cz/seznam-danovych-poradcu?from=1370

[55] *KST ČR - Komora soudních tlumočníků:* [online]. [cit. 2016-11-25]. Dostupné z: http://www.kstcr.cz/cz

[56] *ČLK > / Pro veřejnost / Seznam lékařů:* [online]. [cit. 2016-11-25]. Dostupné z: http://www.lkcr.cz/seznam-lekaru-426.html

[57] *Nahlížení do katastru nemovitostí:* [online]. [cit. 2016-11-25]. Dostupné z: http://nahlizenidokn.cuzk.cz/

[58] *ČÚZK - Výstupy z KN poskytované prostřednictvím DP:* [online]. [cit. 2016-11-25]. Dostupné z: http://www.cuzk.cz/Katastr-nemovitosti/Poskytovani-udaju-z-KN/Dalkovy-pristup/Vystupy-z-KN-poskytovane-prostrednictvim-DP.aspx

[59] *Rejstříky a registry - statnisprava.cz:* [online]. [cit. 2016-11-25]. Dostupné z: https://www.statnisprava.cz/rstsp/redakce.nsf/i/rejstriky

Facebook či Twitter a ukládat do databází jednotlivá data o osobách, které je zveřejňují.[60]

Obchodníci s osobními údaji také skupují nebo na základě licenčních smluv získávají přístup k osobním údajům získanými maloobchodníky, finančními institucemi nebo jinými obchodníky s osobními údaji.
Zajímavou obchodní symbiózou je koncept založený na smlouvách o vzájemné spolupráci, kdy společnosti vlastnící data o svých klientech poskytují tato data obchodníkům s údaji, kteří na oplátku společnostem dodávají obohacené seznamy stávajících i potenciálně nových zákazníků.[61] Pro výše uvedené společnosti se jedná o win-win business model, kdy s minimálními náklady získávají přidanou hodnotu. V praxi mají data brokers a jejich klienti smluvně ujednáno[62], že třetím stranám nebudou poskytovat žádné údaje o druhé straně a o obsahu jejich vztahů.[63] Samotné osoby, s jejichž údaji je nakládáno, o tomto předávání jen zřídkakdy vědí[64], a lze proto pochybovat, že z toho jakkoliv profitují.

Dalším využívaným způsobem získávání klientských údajů online jsou webové dotazníky. V tomto případě uživatelé webových stránek vyplňují informace o sobě

[60] EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Str. 31.

[61] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 22-27.

[62] Pomocí tzv. non-disclosure agreements (NDA), které mohou obsahovat velké sankce za jakékoliv porušení. Informace o smluvním vztahu však mohou (resp. musí) být prozrazeny na základě rozhodnutí soudu či jiného kompetentního orgánu.

[63] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 39.

[64] Tamtéž *s*tr. 18.

samých. Otázkou zůstává, zda jsou tyto osoby řádně informovány, co se s jejich údaji stane následně. Informování probíhá nejčastěji „odclicknutím checkboxu“, což simuluje právní jednání, kterým osoba stvrzuje, že četla pravidla nakládání s osobními údaji a souhlasí s nimi. V praxi však bývají tato pravidla extrémně nečtivá, ať už svou délkou či složitým jazykem. Lze proto pochybovat, že je někdo opravdu čte. Respondenti bývají motivováni různými slosováními o výhry či možností získat slevové kupóny. Pomocí dotazníků data traders získávají citlivé údaje, včetně odpovědí na otázky týkající se zdravotního stavu nejen svého, ale i osob žijících ve společné domácnosti.[65] Takto může být zasaženo i do soukromí osob, které s poskytnutím svých údajů nesouhlasily, či ani nevěděly. Osobní informace lze získávat i pomocí webových stránek, které se jeví, že návštěvníkovi poskytují zdarma nějakou službu, typicky srovnávače cen energií[66] nebo pojištění. Pro poskytnutí služby však musí nejprve návštěvník vyplnit informace o sobě, aby mu byla poskytnuta služba. Tyto dotazníky bývají koncipovány tak, že začínají velmi obecnými dotazy, postupně se však dotazy soustřeďují na konkrétnější osobní údaje. Respondentovi je s postupujícím množstvím odpovědí již nepříjemné dotazník ukončit bez úspěšného uložení, čímž by ztratil investovaný čas a také přišel o možnost výhry. Často se proto na poslední stránce dotazníku objeví nepříjemně citlivé otázky.

Informace o chování osob získávají data brokers také ze souborů cookies[67], což jsou textové soubory, které se ukládají do složky webového prohlížeče během prohlížení internetu. Bez těchto souborů by se stránky jevily, tak jako když na ně uživatel přišel poprvé, tedy musely by se načíst kompletně všechny informace, prohlížeč by si nepamatoval hesla ani přístupová jména, preferovaný jazyk či místo, ze kterého se

[65] Tamtéž str. 24-25.

[66] Českým příkladem je stránka http://www.energie123.cz/kalkulacka-elektriny/#zadani, jež má v podmínkách, mimo jiné, že zadané údaje budou „…zpracovávány primárně za účelem přípravy nabídky služeb a návrhů smluv pro klienta, za účelem marketingu tj. zasílání informací o stávajících i nových produktech společnosti, počátku různých promo akcí, soutěží apod….“

[67] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 37.

uživatel připojuje. Cookies tedy sloužily primárně pro zvýšení komfortu surfování. Existence cookies si lze snadno všimnout například v okamžiku, kdy se uživateli na cizojazyčných stránkách zobrazí reklama v jeho jazyce. Pozornější uživatelé si mohou všimnout, že postupem času se mu zobrazují reklamy, které tematicky souvisí s jeho předchozími návštěvami a nezobrazují se reklamy, které se dříve zobrazovaly.[68][69] Vzhledem k faktu, že pomocí cookies mohou být ukládány osobní údaje, včetně jména, emailové adresy, či bydliště[70], využívají se v současné době také pro identifikaci uživatelů pro reklamní účely.[71] Problematické z pohledu ochrany osobních údajů je možnost číst obsah ostatních cookies těmi, kdo je do počítače ukládají. Existuje více druhů cookies s odlišnými vlastnostmi a také novější a pokročilejší metody, před kterými je složitější se bránit. Patří mezi ně mimo jiné cookie syncing (někdy označováno jako cookie matching), tedy předávání identifikačních informací o uživateli mezi různými doménami [72]; canvas fingerprinting, tedy vytvoření malého grafického souboru, ve kterém se promítnou charakteristiky použitého software i hardware, čímž vznikne identifikující prvek uživatele, respektive jeho hardware[73]; nebo používání

[68] Ačkoliv toto může být způsobeno i tím, že zadavatel reklamy již dále reklamu nevyužívá.

[69] Podobným způsobem vytváří Facebook, Google a další mediální giganti informační bubliny, na které ve svém Ted videu upozorňuje Eli Paliser, např. ukazuje, jak na stejný vyhledávací dotaz „Egypt“ ve stejném okamžiku v roce 2011 zobrazil Google dvěma různým osobám na jejich počítačích zobrazily naprosto odlišné výsledky; jednomu popis politické situace v Egyptě v souvislosti s arabským jarem, druhému nabídku zájezdů do Egypta. Více na: Eli Pariser: Beware online "filter bubbles". *TED.com: TED Talk* [online]. 2011 [cit. 2016-08-15]. Dostupné z: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en

[70] *Cookies - Information that websites store on your computer | Firefox Help:* [online]. [cit. 2016-08-15]. Dostupné z: https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer#w_what-is-a-cookie

[71] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 37.

[72] ACAR, Gunes; et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild* [online]. 2015 [cit. 2016-08-15]. Dostupné z: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf. Str. 8-9.

[73] Tamtéž str. 4-7.

evercookies (zvaných i supercookies či flash cookies[74]), tedy malých textových souborů, které zůstanou v prohlížeči i po vymazání standardních cookies a které standardní prostředky (např. AdBlock) nedokáží účinně blokovat.[75] Použitím více sledovacích metod je možné dosáhnout kumulace množství informací i o uživatelích, kteří dbají na ochranu svých osobních údajů. Jediná neopatrnost v online světě pak umožní spojení izolovaných údajů do jediného, ke konkrétní osobě přiřazeného, souboru.[76]

Dalším příkladem, jak lze získat osobní informace a zároveň příkladem, kdy technologie předstihla regulaci, je sledování uživatelů napříč několika jeho zdánlivě neprovázanými přístroji (cross-device tracking). Základní metodou je analýza chování online, konkrétně jaká témata, v jakém čase a na jakém místě uživatel online vyhledává. Tímto lze vypozorovat vzorce chování na jednotlivých přístrojích. Pokud vzorce chování na sobě navazují, lze provázat všechny přístroje a přiřadit je k jedné konkrétní osobě.[77] Typickým případem je osoba doma používající soukromý počítač, v práci pracovní počítač a v obou lokalitách mobilní telefon. Mobilní telefon v tomto případě může sloužit jako pojítko mezi prostředími, a to díky IP adrese domácí i pracovní wifi sítě, do kterých se připojuje mobilní telefon. Tímto lze spárovat oba samostatné počítače a s vysokou pravděpodobností přiřadit oba počítače i telefon k jedné osobě. Další indicií je čas připojování, tedy ráno a večer v pracovní dny bude osoba většinou doma; v průběhu dne v práci. Jinou indicií mohou být navštěvované webové stránky. Pokud se z obou počítačů připojí na nějaké méně navštěvované a tedy unikátnější stránky, je

[74] CALABRESE, Chris; et al. *Comments for November 2015 Workshop on Cross - Device Tracking. Microsoft Word - FTC Cross-Device Draft v14.docx - 10.16.15-CDT-Cross-Device-Comments.pdf:* [online]. 2015 [cit. 2016-08-25]. S. 3. Dostupné z: https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf

[75] ACAR, Gunes; et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild* [online]. 2015 [cit. 2016-08-15]. Dostupné z: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf. Str. 7-8.

[76] Tamtéž str. 1.

[77] BROOKMAN, Justin. *What is Cross-Device Tracking?* [online]. In: FTC - Office of Technology Research and Investigation, 2015 [cit. 2016-08-25]. Dostupné z: https://www.ftc.gov/system/files/documents/public_events/630761/cross-device_tracking_workshop_deck.pptx

možné, že tato návštěva přispěje k identifikaci fyzickou osobu[78] Čím více údajů, tím samozřejmě přesnější profil uživatele.
Ačkoliv tato metoda není ve všech případech použitelná, jedná se o další možnost, jak zefektivnit zaměření reklamy online a zároveň jak získat ještě větší kontrolu nad soukromím nic netušících osob.

V roce 2014 vzbudila mediální nevoli odlišná metoda cross-device tracking[79], vyvinutá společností SilverPush a posléze použita i do aplikací jiných výrobců. Mobilní aplikace, do kterých byl SilverPush kód implementován, umožnily zachycení lidským sluchem neidentifikovatelného audio signálu v televizních reklamách pomocí mikrofonu mobilních telefonů a tabletů. Pokud byl přístroj v doslechu televize, mohl sledovat a následně odeslat data o tom, zda osoba reklamu viděla, jak dlouho sledovala televizní vysílání a další údaje. To vše bez jejího vědomí dané osoby. Funkce SilverPush byla aktivní i pokud samotná aplikace byla vypnutá.[80] Společnost SilverPush odmítla zveřejnit aplikace, které jejího kódu využívaly, neexistovala proto možnost, že by se uživatel těchto aplikací vyvaroval.[81]

Všechny výše uvedené metody získávání dat mají potenciál přinést mnoho informací, avšak kombinací těchto metod lze v době big data získat unikátní data set a velmi přesný profil uživatelů internetu.[82]

---

[78] Například návštěva nepřehledné univerzitní webové stránky s informacemi o náležitostech diplomové práce může sloužit jako unikátní identifikátor.

[79] HA, Anthony. *SilverPush Says It's Using "Audio Beacons" For An Unusual Approach To Cross-Device Ad Targeting* [online]. TechCrunch, vyd. 2014-7-24 [cit. 2016-08-26]. Dostupné z: https://techcrunch.com/2014/07/24/silverpush-audio-beacons/

[80] MITHAL, Maneesha. Vzor dopisu odeslaný výrobcům aplikací obsahující SilverPush. *160317samplesilverpushltr.pdf:* [online]. FTC - Bureau of Consumer Protection, 2016 [cit. 2016-08-25]. Dostupné z: https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-silverpush-code/160317samplesilverpushltr.pdf. Str. 1.

[81] CALABRESE, Chris; et al. *Comments for November 2015 Workshop on Cross - Device Tracking. Microsoft Word - FTC Cross-Device Draft v14.docx - 10.16.15-CDT-Cross-Device-Comments.pdf:* [online]. 2015 [cit. 2016-08-25]. Dostupné z: https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf. Str. 4-5.

[82] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18].

Existuje několik možností obrany proti sledovacím mechanismům. V prohlížeči lze tradiční cookies lze odstranit po každém použití nebo zamezit jejich používání. Podobně lze zablokovat, resp. nepovolit prozrazovaní polohy na základě IP adresy. Pokročilejší metody sledování lze omezit pomocí různých doplňků do prohlížečů, mezi nejznámější patří již zmiňovaný AdBlock nebo Ghostery. Dalším stupněm ochrany soukromí může být používání čím dál známějšího prohlížeče anonymního Tor.[83] Důsledné používaní rozdílných webových prohlížečů, např. pro pracovní a soukromé účely, zamezí získání komplexních informací o uživateli.[84] Otázkou zůstává, zda má toto rozdělování v současné době vůbec smysl. Existuje důvodná obava, že jediné zaváhání, například přihlášení do stejné emailové schránky z obou prohlížečů, funguje jako cross-device tracking mechanismus, kterým dojde ke spojení obou data setů do jednoho.

Nevýhodou obezřetného používání výše uvedených nástrojů je zpravidla snížení komfortu a rychlosti surfovaní po internetu. Použití doplňků typu Ghostery mírně, ale přesto znatelně, zpomalí načítání obsahu. Pomalejší surfování lze očekávat i v případě používání browseru Tor. Některé webové stránky nezobrazí svůj obsah, pokud detekují použití AdBlock a podobného software.[85] Některé stránky dobrovolně implementovaly službu Do Not Track, která umožňuje uživatelům jednoduše zvolit v prohlížeči

---

Str. 31. Také v *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. Dostupné z: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf*. Str. 44.

[83] *Tor Project: Overview:* [online]. [cit. 2017-02-07]. Dostupné z: https://www.torproject.org/about/overview.html.en

[84] ACAR, Gunes; et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild* [online]. 2015 [cit. 2016-08-15]. Dostupné z: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf. S.12-13

[85] Což jak se zdá způsobuje úbytek návštěvníků, tedy menší zájem reklamních zadavatelů, a tedy nižší příjmy z reklamy. Více např. v ANDERSON, Martin. Sites that block adblockers seem to be suffering. *The Stack* [online]. Vyd. 2016-04-21 [cit. 2016-08-25]. Dostupné z: https://thestack.com/world/2016/04/21/sites-that-block-adblockers-seem-to-be-suffering/

možnost, aby jejich prohlížeč vyslal signál indikující stránkám, že si uživatel nepřeje být sledován.[86]

Právní kancelář Winston Law Firm, LLC. na svých stránkách uveřejnila 50 odkazů[87] na opt-out formuláře, přes které lze vyjádřit nesouhlas se zpracováním osobních údajů různými data brokers. Osoba, která by si nepřála zpracovávání svých dat, bude muset podstoupit vyplňování těchto 50 dotazníků, nebo může využít placenou službu a nechat si opt-out formuláře vyplnit.[88] Obojí však bez garance, že její data nebyla zpřístupněna před vyjádřením nesouhlasu jiným subjektům. Dalším rizikem je, že osobní data nebudou zcela vymazána, jak je popsáno výše v textu.[89]

Ochrana osobních dat v době sociálních sítí není snadnou záležitostí. Zveřejňování informací online o sobě i o blízkých osobách z každé společenské akce spolu s trendem být vidět a slyšet na internetu je neodmyslitelnou součástí života digitálních občanů. Sociální tlak na osoby, které tak nečiní, může být pro mnohé důvodem proč raději zvolit konformní cestu společenské interakce, a to i přes uvědomění, že využití poskytnutých informací je netransparentní. Opatrnost v online světě s sebou nese i jistý stupeň paranoi a v určitých momentech i pocit bezmoci, zda vůbec lze neprohrát tento soukromý boj proti korporacím hladových po soukromých datech.

3.3. *Využití údajů od data brokers*

Subjekty, které osobní data nakupují, mají možnost vybrat si typicky ze dvou produktů:

- seznamy osob, které splňují určitá kritéria, například potenciální klienti, mající vybrané demografické nebo zájmové charakteristiky

---

[86] *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. Dostupné z*:* *https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf*. Str. 42-43.

[87] *Master List of Data Broker Opt-Out Links* - [online]. Winston Law Firm, LLC., 2015 [cit. 2016-08-29]. Dostupné z: http://www.stopdatamining.me/opt-out-list/

[88] Společnosti Abine, Inc. Nabízí službu DeleteMe za 129 dolarů na rok, pouze pro americké občany. *DeleteMe - Protect Your Personal Data And Reputation Online:* [online]. [cit. 2017-04-09]. Dostupné z: https://abine.com/deleteme/landing.php

[89] Viz kapitola 3.

- doplnění informací o svých stávajících klientech[90], například mobilní operátor, který si nechá doplnit informace o finančním příjmu svých klientů a rychlosti internetového připojení v místě bydliště, tak aby mohl těmto klientům nabídnout vlastní internetové připojení

Americká Committee on Commerce, Science, and Transportation analyzovala i zákazníky obchodníků s osobními údaji. Obchodníci však, paradoxně, nechtěli poskytovat příliš informací o svých klientech, kteří osobní data nakupují a využívají pro své obchodní aktivity. Z reportu vyplývá, že mezi klienty patří mj. 47 společností z Fortune 100[91], a tedy patří mezi ně ty nejznámější banky, hotelové řetězce, telekomunikační společností, pojišťovny, aerolinky a další korporace. Report dále zmiňuje obchodníky s cennými papíry, univerzity i střední školy, realitní makléře, státní instituce, politiky a samozřejmě různé druhy reklamních společností[92]. Jiný zdroj uvádí navíc i advokáty a vyšetřovatele, jiné data brokers, farmaceutické společnosti nebo technologické společnosti.[93]

Mezi uváděné využití produktů data brokers patří:

- přímý marketing
- online marketing

---

[90] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 28.

[91] Žebříček 100 amerických společností s nejvyšším hrubým obratem. Více na http://beta.fortune.com/fortune500

[92] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 35.

[93] EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Str. 57-58.

- marketingová analýza
- ověření identity
- rozpoznávání podvodů
- hledání osob[94]
- hledání nových zaměstnanců[95]

Jedním z dobře dokumentovaných případů je použití údajů ze zdravotních záznamů pacientů, lékařských předpisů, záznamů pojišťoven nebo laboratorních testů. Tato data jsou kupována farmaceutickými společnostmi, například pro účely lepšího cílení reklamních kampaní. Data jsou před prodejem poskytnutím zbavena údajů, které by mohly přímo identifikovat konkrétního člověka, tedy jeho jméno, adresu a číslo sociálního pojištění, (které v USA slouží jako unikátní identifikátor osoby). Data brokers však po této anonymizaci k profilu přiřadí unikátní číslo. Použitím analytických metod, spolu s kombinací jiných databází, lze i po anonymizaci zjistit opravdovou identitu osob. Vedoucí data broker se zdravotními informacemi IMS Health[96] dosáhl v roce 2014 obratu 2,6 miliardy dolarů[97] (65 miliard korun); v roce 2016, po spojení se společností Quintiles, to bylo 7,8 miliardy dolarů (195 miliard korun). Společnost ve své výroční zprávě za rok 2016 uvádí, že data čerpá z více než 100 000 zdrojů po celém světě a disponuje informacemi o více než 85 % světových transakcích zahrnující

[94] EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Str. 57.

[95] *PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION on What Information Do Data Brokers Have On Consumers, And How Do They Use It* [online]. Washington, D.C., 2013 [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf. Str. 5.

[96] https://www.quintilesims.com/. Společnost má pobočku i v České republice

[97] TANNER, Adam. *How Data Brokers Make Money Off Your Medical Records: Data brokers legally buy, sell and trade health information, but the practice risks undermining public confidence.* Scientific American [online]. Scientific American, a Division of Nature America, vyd. 2016-02-01 [cit. 2017-04-17]. Dostupné z: https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

léčiva.[98] Farmaceutický gigant Pfizer investuje do dat od data brokers přes 12 milionů dolarů ročně (cca 300 milionů korun).[99]

[98] *Výroční zpráva společnosti QuintilesIMS* 2016 [online]. [cit. 2017-04-17]. Dostupné z: http://s21.q4cdn.com/395013450/files/doc_financials/2016/QuintilesIMS_2016_Annual-Report_Final-%281%29.pdf. Str. 2-3.

[99] TANNER, Adam. *How Data Brokers Make Money Off Your Medical Records: Data brokers legally buy, sell and trade health information, but the practice risks undermining public confidence.* Scientific American [online]. Scientific American, a Division of Nature America, vyd. 2016-02-01 [cit. 2017-04-17]. Dostupné z: https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

4. Právní regulace obchodu s osobními údaji

4.1. *Právní regulace v Severní Americe*

4.1.1. USA

Vzhledem ke globální povaze internetu je nutné i regulaci obchodování s osobními údaji řešit globálně, tedy za použití mezinárodních právních instrumentů nebo za použití norem z více legislativních prostředí. V současném světě není zásadním problémem založit společnost na druhé straně světa, a to i bez fyzické přítomnosti zakladatele. Je proto možné, a v praxi i běžné, přemisťovat společnosti na základě vhodného legislativního nebo daňového prostředí pro konkrétní podnikatelskou aktivitu. Data trading je zcela jistě obchodní aktivitou, kterou lze provádět odkudkoliv na světě, jelikož ke své činnosti vyžaduje pouze datové uložiště a přístupový bod k internetu.

Na základě analýzy geografického rozložení data brokers je nutné zaměřit se na regulaci ve Spojených státech, protože představují klíčový trh s touto komoditou. Určitá nejistota však panuje v opravdovém rozsahu tohoto businessu v jiných místech planety, jelikož relevantní publikace dokumentující obchod s osobními údaji jsou, na rozdíl od USA, na internetu dostupné v mnohem menší míře, pokud vůbec. Spojené státy také již desetiletí hrají klíčovou roli v technologických inovacích, je proto pravděpodobné, že právě zde vznikl business model obchodování se soukromými daty.

Ve Spojených státech jednotná definice pojmu *osobní údaj* neexistuje, jelikož zde neexistuje jednotná právní úprava chránící osobní údaje. Ochrana některých informací (např. o zdravotním stavu, finanční výkonnosti fyzických osob) je roztříštěna mezi více zákonů.[100] Ačkoliv i v USA existuje zákon o ochraně osobních údajů (Privacy Act of 1974), dopadá pouze na zpracování osobních údajů federálními úřady, nikoliv na

[100] Tzv. patchwork system (záplatový systém).
Citováno z: JOLLY, Ieuan. *Data protection in the United States: overview | Practical Law:* [online]. [cit. 2017-04-15]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/6-502-0467?__lrTS=20170415143511897&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1

zpracování údajů společnostmi nebo jinými osobami.[101] Zákon označuje osobní informace jako záznamy o osobách (*records*), které se překrývají s evropským pojetím osobní informace.[102] Neosobní označení *záznam* lze také považovat za odlišující přístup evropské a americké legislativy k ochraně soukromých informací.

V USA je komerční použití osobních údajů upraveno především v zákoně Fair Credit Reporting Act[103] (dále jen FCRA), který se primárně vztahuje na subjekty označované jako consumer reporting agencies, které shromažďují o lidech osobní údaje především pro účely vytvoření reportu, který slouží k ohodnocení kredibility například při poskytnutí půjčky, zaměstnání, pojištění nebo bydlení. Shromažďování údajů však probíhá se souhlasem subjektů údajů, kteří mají ke zpracovávaným údajům přístup a mohou údaje opravovat, jsou-li nepřesné. Consumer reporting agencies nemohou poskytnout osobní údaje k jiným, než výše uvedeným účelům. Společnosti poskytující služby na základě reportů mají povinnost informovat osobu, která na základě reportu bude čelit negativním následkům, například horšími podmínkami pro poskytnutí úvěru nebo zamítnutí jeho poskytnutí. V případě porušení může dohlížející orgán, kterým je Federal Trade Commission, uložit peněžité sankce.[104] Tento zákon však dopadá jen na výše uvedené situace a nelze jej, ve většině případů, použít na aktivitu data brokers.[105]

---

[101] BIGNAMI, Francesca. *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* [online]. Brussels: European Union, 2015 [cit. 2017-04-27]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf . Str. 10-11.

[102] Mezi tyto záznamy patří například, vzdělání, finanční transakce, zdravotní, trestní a pracovní historie, jméno nebo identifikační číslo nebo jiný identifikátor osoby, jako je otisk prstu, záznam hlasu nebo fotografie. Citováno z: Privacy Act of 1974 5 U.S.C. § 552a(a)(4).

[103] V češtině znamenajíc zhruba „zákon o spravedlivém úvěrovém reportu".

[104] RAMIREZ, Edith. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues: FTC Report* [online]. 2016 [cit. 2017-04-14]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Str. 25-29.

[105] EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Str. 25-26.

Existuje však velké množství zákonů, ať už federálních, či státních, které okrajově dopadají na činnost data brokers. Účelem těchto zákonů však primárně není ochrana osobních údajů.

Jsou jimi, ku příkladu, zákony zakazující diskriminaci na základě rasy, barvy, pohlaví, náboženství, věku, postižení, původu, rodinného stavu nebo genetické informace[106], což jsou také informace obchodované data brokers.[107] Pokud by se subjekt údajů dozvěděl, že mu byla způsobena újma kvůli nestejnému jednání jiného subjektu, založeném na znalosti těchto citlivých údajů, mohla by se tato osoba bránit civilní žalobou. Navíc v tomto případě hrozí společnostem, které se dopustily diskriminačního jednání správní sankce.[108] Dalšími zákon obsahující roztříštěná ustanovení o ochraně osobních údajů jsou the Gramm Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) nebo the Health Information Technology for Economic and Clinical Health Act (HITECH).[109] Některé zákony byly přijaty dokonce jako reakce na negativně vnímané medializované příběhy jednotlivců, které byly zapříčiněny nedostatečnou ochranou některých informací.[110]

Další nespecializovanou normou je The Federal Trade Commission Act (FTCA)[111], která chrání práva spotřebitele, jakožto slabší smluvní strany v transakcích s podnikateli. Norma mimo jiné zakazuje podvodné nebo nespravedlivé jednání

[106] Těmito zákony jsou the Equal Credit Opportunity Act ("ECOA"), Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act ("ADEA"), the Fair Housing Act ("FHA") a the Genetic Information Nondiscrimination Act ("GINA"). Někdy také souhrnně označované Equal Opportunity Laws.

[107] Toto téma je detailně zpracováno v kapitole 4.

[108] RAMIREZ, Edith. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues: FTC Report* [online]. 2016 [cit. 2017-04-14]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Str. 29-33.

[109] *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 2.

[110] Jedná se například o the Driver's Privacy Protection Act (DPPA) nebo o the Video Privacy Protection Act (VPPA). K tomu více viz KUEMPEL, Ashley. The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* [online]. 2016, 36(1), 207-234 [cit. 2016-07-22]. Dostupné z: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1795&context=njilb. Str. 216.

[111] V češtině znamenajíce zhruba „zákon o federální obchodní komisi".

a praktiky, jež se mohou samozřejmě týkat i společností obchodujících s osobními informacemi.[112]

Ústava USA výslovně nezaručuje ochranu soukromí; z rozsudku Nejvyššího soudu vyplývá ochrana občanů před obtěžujícími aktivitami státu, nikoliv však před aktivitami ze strany soukromých společností.[113] Ve Spojených státech je také velmi silně chráněna svoboda projevu, což může kolidovat s právy na ochranu soukromí.[114]

Legislativní rámec ochrany osobních informací je ve Spojených státech poněkud roztříštěný a ne zcela přehledný. V současnosti neexistuje federální zákon, který by obchodníkům s osobními údaji ukládal povinnost informovat subjekty údajů, jaké osobní údaje jsou o nich shromažďovány.[115] Existuje zde však množství norem, které se liší svou lokální působností i cílem. Některé z nich se totiž vztahují na celé území a některé jen na určité státy; některé se dotýkají jen specializovaných témat, jakým je například zákon FCRA regulující úvěrový report (credit report), jiné se týkají obecnějších kategorií, které částečně zasahují i do oblasti osobních údajů, jako třeba normy chránící spotřebitele. Přičemž ne vždy se tyto normy logicky a funkčně doplňují.[116]

---

[112] RAMIREZ, Edith. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues: FTC Report* [online]. 2016 [cit. 2017-04-14]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Str. 33-35

[113] KUEMPEL, Ashley. The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* [online]. 2016, 36(1), 207-234 [cit. 2016-07-22]. Dostupné z: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1795&context=njilb. Str. 214.

[114] *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 3.

[115] KUEMPEL, Ashley. The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* [online]. 2016, 36(1), 207-234 [cit. 2016-07-22]. Dostupné z: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1795&context=njilb. Str. 210.

[116] KUEMPEL, Ashley. The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* [online]. 2016, 36(1), 207-234 [cit. 2016-07-22]. Str. 214-215 nebo *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014.

V USA se vyskytly pokusy regulovat data brokers komplexní legislativou, tyto pokusy však nikdy nebyly dotaženy do konce. Jedním z uváděných důvodů je silná ochrana svobody slova plynoucí z Prvního dodatku americké ústavy. Podle interpretace tohoto dodatku Nejvyšším soudu USA nelze omezovat předávání či prodej informací, vše však závisí na posouzení konkrétní situace[117]. Podle dostupných informací neexistuje jiná judikatura řešící legitimitu data brokers, nelze proto s jistotou posoudit ani další směr vývoje.

Na základě výše uvedené analýzy normativního rámce se zdá, že data traders na území USA provozují svojí činnost v souladu s platnými právními akty. Vzhledem k absenci povinnosti poskytovat o své činnosti mnoho detailů, ať už subjektům údajů nebo státním institucím, nelze s určitostí říci, zda jejich veškeré aktivity jsou v souladu s právním řádem.

S jistotou však lze pochybovat o výroku kanceláře prezidenta USA, že

> „*Spojené státy jsou připravené lépe, než kterýkoliv jiný národ na světě, i nadále využívat digitální revoluci pro posílení svých občanů a veřejného dobra.*“[118]

4.1.2. Kanada

I přes kulturní a geografickou blízkost se Spojenými státy je situace v Kanadě značně odlišná. Existuje zde zákon o ochraně osobních údajů a elektronických dokumentech, Personal Information Protection and Electronic Documents Act (PIPEDA)[119], který

[cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 2-3.

[117] *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 3.

[118] „The United States is better suited than any nation on earth to ensure the digital revolution continues to work for individual empowerment and social good.“ In *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. Dostupné z: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. Str. 3.

[119] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), účinný ke dni 2015-06-23 [online]. [cit. 2016-08-29]. Dostupné z: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

svou působností dopadá na všechny seskupení sbírající, používající nebo zpřístupňující osobní údaje. Zákon také platí ve stejném rozsahu i pro subjekty, jež kupují produkty data brokerů. Ačkoliv se v některých provinciích tento zákon nepoužije v celém rozsahu (za předpokladu, že provincie přijala „v *zásadě obdobnou legislativu*"[120]), vždy se uplatní jeho ustanovení pro přeshraniční výměnu dat. Kanaďané musí poskytnout souhlas se zpracováním svých osobních údajů,[121] a to i když jsou veřejně dostupné online nebo offline.[122] Z tohoto důvodu nelze proto provádět například data mining osobních údajů například na sociálních sítích nebo z veřejně dostupných databází jiným subjektem, než který k tomu získal souhlas (typicky provozovatel sociální sítě nebo databáze). Odlišná legislativa přináší i jinou praxi data brokerů, a to i přes fakt, že některé společnosti působí v obou zemích.[123] Tyto společnosti, že provozují svou činnost jen v omezeném měřítku, a to v souladu s kanadskou legislativou.[124]

Tímto jsou kanadští rezidenti chráněni i před aktivitami data brokers svého jižního souseda. Právní úprava ochrany osobních informací se tedy podobá spíše evropské regulaci.

4.2. *Právní regulace v EU*

Evropská unie je dobrovolný spolek států, které se dohodly vzdát se některých svých kompetencí ve prospěch nadnárodního celku. Evropská unie má tak pravomoc svými vlastními právními akty, tedy bez předchozího souhlasu zákonodárných celků jejích členů, rozhodovat o některých otázkách v rámci tzv. *výlučné pravomoci*. V některých otázkách mohou členské státy rozhodovat a vydávat normy, jen pokud EU nevyužije své tzv. *sdílené pravomoci* na úpravu těchto otázek. Třetí kategorií je tzv. *koordinační*

[120] Přehled speciální provinční legislativy, která se použije místo PIPEDA je dostupný v *Substantially Similar Legislation - Legal information related to PIPEDA* [online]. 2013 [cit. 2016-08-29]. Dostupné z: https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp

[121] PIPEDA čl. 6.1

[122] *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 5-8

[123] Např. Acxiom, Equifax, TransUnion

[124] *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf. Str. 10.

pravomoc, v rámci níž EU nemá pravomoc vydávat právně závazné akty, ale koordinuje a podporuje členské státy v dosažení nějakého společného cíle.[125] Ochrana osobních údajů patří do sdílené pravomoci[126] a vzhledem k existenci unijního práva harmonizujícího, resp. unifikujícího regulaci obchodu s osobními údaji, mají členské státy povinnost dodržovat de facto stejné právo. Z tohoto důvodu nemá smysl analyzovat zvlášť například české právo a zvlášť unijní právo týkající se data brokers.[127]

Státy EU mají obecnou povinnost udržovat svůj právní řád v souladu s právem EU, které lze rozčlenit na dvě oblasti podle toho, kdo schvaluje právní normy EU. Primární právo EU je soubor norem, které schválily členské státy; jedná se především o zakládací smlouvy.[128] Sekundární právo EU je soubor norem EU, které schválily orgány Evropské unie.[129]

Sekundární unijní právo se dále dělí na dva druhy závazných právních aktů, a to směrnice (directive) a nařízení (regulation). V případě směrnic musí členské státy, respektive jejich zákonodárné sbory, harmonizovat národní právní akty s obsahem směrnic tak, aby obsahovaly stejná práva a povinnosti jako směrnice. Implementace může být docílena buď doslovným převzetím textu směrnice do národního právního aktu, nebo použitím jiného textu se stejným významem.[130] V některých případech představují směrnice prostředek k dosažení minimálního standardu, což znamená, že státy se mohou odchýlit od tohoto minimálního standardu a zavést například přísnější regulaci ve prospěch občanů.[131]

---

[125] Časté otázky týkající se pravomocí EU a Evropské komise – Evropská občanská iniciativa - Evropská komise: [online]. [cit. 2016-07-11]. Dostupné z: http://ec.europa.eu/citizens-initiative/public/competences/faq?lg=cs#q1

[126] Čl. 4 Smlouvy o fungování EU

[127] Sankce za porušení norem EU na ochranu osobních údajů jsou upraveny národní legislativou, což je popsáno níže v textu.

[128] Smlouva o EU a Smlouva o fungování EU

[129] *EUR-Lex - l14534 - EN - EUR-Lex: Prameny práva Evropské unie* [online]. [cit. 2017-02-07]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=URISERV:l14534

[130] BARNARD, Catherine a Steve PEERS. *European Union law*. 1. Oxford: Oxford University Press, 2014. ISBN 9780199686117. Str. 100-101.

[131] Tento minimální standard lze najít například v mnoha článcích SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2012/29/EU, kterou se zavádí minimální pravidla pro práva, podporu a ochranu obětí trestného činu a kterou se nahrazuje rámcové rozhodnutí Rady 2001/220/SVV.

Některé záležitosti týkající se justiční spolupráce byly dříve upravovány dalším, třetím druhem právních aktů tzv. rámcovými rozhodnutími (framework decision), které mají podobné rysy jako dnešní směrnice. Tento druh však není od přijetí Lisabonské smlouvy v 2009 vydáván.[132]

V případě nařízení EU nemusí státy vydávat ani přizpůsobovat právní akty, pokud nejsou v rozporu s nařízením, jelikož nařízení mají přímou účinnost vůči státům i všem fyzickým i právnickým osobám v EU, a to bez ohledu na legislativní procesy členských států. Nařízení tedy unifikují právo Evropské unie, jelikož ve všech státech platí naprosto totožný předpis, zatímco směrnice evropské právo harmonizují.[133]

Pro praktické použití evropského práva je důležité pochopit předchozí rozdělení, které umožnuje fyzickým i právnickým osobám (i z nečlenských států) řešícím obchodování s osobními údaji vyhledat relevantní národní nebo evropský právní akt.

Ochranu osobních údajů garantuje Listina základních práv Evropské unie, která ve článku 7 zaručuje všem lidem na území EU právo na respektování osobního života a komunikace (ve smyslu dopisů, emailů, telefonátů apod.).[134] Článek 8 pak konkretizuje právo každého člověka na ochranu svých osobních údajů a definuje zásady na zpracovávání těchto údajů, mezi něž patří:

- férovost zpracování
- použití údajů jen pro konkrétní účel
- použití jen na základě souhlasu osoby, jíž se údaje týkají nebo na základě jiného, právem definovaného legitimního důvodu
- garance přístupu ke svým vlastním údajům
- možnost opravit a zpřesnit vlastní osobní údaje
- kontrola těchto pravidel podléhá kontrole nezávislého orgánu[135]

[132] *Portál evropské e-Justice - Právo EU* [online]. [cit. 2016-07-12]. Dostupné z: https://e-justice.europa.eu/content_eu_law-3-cs.do

[133] BARNARD, Catherine a Steve PEERS. *European Union law*. 1. Oxford: Oxford University Press, 2014. ISBN 9780199686117. Str. 99-100.

[134] Čl. 7 Listiny základních práv EU

[135] Čl. 8 Listiny základních práv EU

Garance ochrany jsou obdobně uvedeny i v článku 16 Smlouvy o fungování EU, ve kterém se dále specifikují pravidla pro nakládání s osobními údaji orgány a institucemi EU i jejími členskými státy.[136]

V rámci strategie Digital Single Market[137] schválily orgány Evropské unie v roce 2015 reformu ochrany osobních dat. Tato reforma se legislativně promítla do dvou nových právních aktů, které vstoupí v účinnost v květnu 2018. Prvním z aktů je směrnice (EU) 2016/680 [138] nahrazující doposud účinné rámcové rozhodnutí Rady č. 2008/977/JHA[139]; tato dvojice se věnuje zpracování osobních údajů vyšetřovacími orgány v jiných členských státech v trestních věcech, avšak tato problematika nespadá pod téma této diplomové práce.
Druhým z nových aktů je nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které se i v české praxi označuje jako GDPR podle anglického *General Data Protection Regulation* (dále tedy jen „GDPR"). GDPR nahradí doposud účinnou směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice o ochraně údajů").

Pro plnohodnotné posouzení právního stavu je proto nutné analyzovat jak současnou směrnici, tak i budoucí právní úpravu dle GDPR. Analýza bude založena především na porovnání ustanovení v obou dokumentech relevantních pro data brokers. Vedle těchto klíčových dokumentů, existují i jiné, speciálnější normy týkající se obchodování s osobními údaji, které jsou pro přehlednost uvedeny až v následujících kapitolách.

---

[136] Čl. 16 Smlouvy o fungování EU

[137] *Reform of EU data protection rules - European Commission* [online]. [cit. 2016-06-30]. Dostupné z: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[138] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV

[139] RÁMCOVÉ ROZHODNUTÍ RADY 2008/977/JHA, o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech

Účinnost směrnice o ochraně osobních údajů skončí dnem 24. května 2018, ode dne následujícího vstoupí v účinnost GDPR.

4.2.1. Definice osobních údajů

Definovat pojem *osobní údaj* je klíčové pro jakoukoliv další analýzu obchodování s těmito údaji.

Českým zákonem o ochraně osobních údajů[140] splnila Česká republika svou povinnost implementovat evropskou směrnici[141]; tento zákon tedy zrcadlí téměř totožnou evropskou definici. Podle této definice se za osobní údaj pokládá jakákoliv informace týkající se určené či určitelné fyzické osoby, kterou lze přímo či nepřímo identifikovat tímto osobním údajem. Demonstrativním výčtem pak zákon uvádí několik příkladů, jak lze osobu identifikovat: jedná se o jakékoliv číslo, kód nebo jeden či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[142] V budoucí evropské úpravě přibyly do demonstrativního výčtu i lokační údaje, síťové identifikátory a genetické informace.[143] Vzhledem k tomu, že v současně platné směrnici se jedná taktéž o demonstrativní výčet, nelze, podle mého názoru, říci, že by se současná a budoucí definice osobního údaje v evropském právu zásadně lišila.

Soudní dvůr Evropské Unie (SDEU), jako nejvyšší interpretační orgán legislativy Evropské unie, však rozšířil pojetí osobních údajů i o IP adresu, pokud umožní nebo přispěje k identifikaci konkrétní osoby.[144] V preambuli GDPR, která vysvětluje

[140] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů v aktuálním znění (dále jen „zákon o ochraně osobních údajů“)

[141] Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[142] § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, resp. čl. 2 odst. 1 směrnice o ochraně osobních údajů.

[143] Čl. 9 odst. 1 GDPR

[144] Bod 65 Rozsudku SDEU č. C-582/14. *In CURIA - Dokumenty: Rozsudek SDEU č. C-582/14 ze dne 19 října 2016, ve věci Patrick Breyer proti Bundesrepublik Deutschland* [online]. [cit. 2017-04-15]. Dostupné z:

a upřesňuje jednotlivé články i cíle nařízení, jsou mezi síťovými identifikátory zmíněny právě IP adresa a cookies.[145]

Ochrana osobních údajů se v každém případě týká jen fyzických osob[146], právnických osob se týká především ochrana dobré pověsti.

Zákon o ochraně osobních údajů definuje dále podmnožinu osobních údajů, a to *citlivé údaje*. V současné i budoucí evropské legislativě jsou citlivé údaje označené jako „*zvláštní kategorie údajů*“.[147]

Těmito údaji jsou informace vypovídající o:

- národnostním, rasovém nebo etnickém původu,
- politických postojích a členství v odborových organizacích,
- náboženském a filozofickém přesvědčení,
- odsouzení za trestný čin,
- zdravotním stavu,
- sexuálním životě a orientaci[148], a
- genetickém a biometrickém údaji, který umožňuje přímou identifikaci nebo autentizaci[149]

Citlivé údaje, jak už jejich samotné označení napovídá, jsou údaje ještě důvěrnější než osobní údaje. Jejich zpracování je, až na taxativně uvedené výjimky, zakázáno.[150] Pokud zpracování této kategorie údajů je předmětem výjimky, jsou na zpracovatele kladeny přísnější nároky[151] a také za případné prohřešky hrozí alespoň v ČR vyšší sankce.[152]

---

http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945

[145] Bod 30 preambule GDPR

[146] § 4 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů; čl. 2 písm. a); čl. 4 odst. 1 GDPR

[147] Čl. 8 odst. 1 směrnice o ochraně osobních údajů resp. čl. 9 odst. 1 GDPR

[148] Sexuální orientace je jako citlivý údaj explicitně uvedena jen v GDPR, nicméně se domnívám, že pod kategorii sexuální život (uvedeno v obou předpisech) lze zahrnout i sexuální orientaci.

[149] § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů. Genetické a biometrické údaje nejsou uvedeny v aktuálně účinné směrnici o ochraně osobních údajů, ale jsou uvedeny v budoucím nařízení GDPR i v českém zákoně na ochranu osobních údajů.

[150] Čl. 8 odst. 1 směrnice o ochraně osobních údajů resp. čl. 9 odst. 1 GDPR

[151] § 9 zákona č. 101/2000 Sb., o ochraně osobních údajů

[152] § 44 písm. odst.6 zákona č. 101/2000 Sb., o ochraně osobních údajů

Za osobní údaj lze považovat i podobu člověka zachycenou například na fotografii či videu, která je navíc chráněna i českým občanským zákoníkem. Dále jsou chráněny i písemnosti osobní povahy, které mohou být, v závislosti na obsahu, taktéž chráněny i podle zákona o ochraně osobních údajů.[153] Občanský zákoník představuje nástroj, díky němuž se proti zásahu do osobnostních práv mohou civilní žalobou bránit samotné dotčené osoby. Uvedené normy Evropské unie, respektive národní zákony o ochraně osobních údajů, představují veřejnoprávní nástroj, díky němuž dozorové orgány mohou (a zároveň musí) dohlížet na činnost zpracovatelů osobních údajů, případně je, v rámci správního soudnictví trestat za porušení.

Speciálním zákonem je zákon o elektronických komunikacích[154], kterým byla implementována směrnice o soukromí a elektronických komunikacích.[155] V těchto dokumentech se jen zpřesňují některé povinnosti vyplývající z obecnějších právních předpisů. Zavazuje jen subjekty činné v oblasti služeb elektronických komunikací ve veřejných elektronických sítích, typicky poskytovatele komunikačních služeb na internetové síti.[156] Samotná definice osobních údajů ani další regulace činnosti data brokers zde regulována není, některé ustanovení se však budou muset posuzovat společně s ustanoveními zákona o ochraně osobních údajů, resp. směrnicí o ochraně osobních údajů.

V praxi však nestačí spoléhat jen na legislativní akty, ale je nutné brát v potaz i rozhodovací praxi soudů a výkladová stanoviska dozorových orgánů na ochranu osobních údajů.

Z výše uvedeného vyplývá, že definice osobního údaje je relativně široká, jelikož zahrnuje informace, které přímo identifikují konkrétního člověka a zároveň, které mají

[153] § 84 a násl. zákona č. 89/2012 Sb., v aktuálním znění (dále jen „občanský zákoník“)

[154] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „zákon o elektronických komunikacích“. Relevantní ustanovení jsou především §87-97.

[155] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „směrnice o soukromí a elektronických komunikacích“)

[156] Čl. 3 směrnice o soukromí a elektronických komunikacích

pouze potenciál osobu identifikovat. V hraničních případech záleží i na konkrétní situaci, zda má informace potenciál být spojená s konkrétní fyzickou osobou. S postupným technologickým rozvojem, lze pozorovat rozšiřování definice i na technologické identifikátory, které úzce souvisí s fyzickými osobami.

Na základě komparace výše uvedených definice a informací, které sbírají američtí data brokers, se jeví, že většina těchto informací je ve členských státech považována za osobní informaci. Mnohé z těchto informací spadají do zvláštní kategorie údajů (v české terminologii *citlivé údaje*).

4.2.2. Současná regulace v EU

Současná evropská právní úprava obchodování s osobními údaji spočívá, spolu s výše uvedenou Listinou základních práv Evropské unie, ve dvou směrnicích: konkrétně v již zmíněné směrnici o ochraně osobních údajů a směrnici Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „směrnice o soukromí a elektronických komunikacích“). Tato směrnice byla přijata v souvislosti s rozvojem internetu, nedostatečností původní úpravy regulující osobní údaje v oblasti telekomunikací[157] a snahou zpřesnit právní úpravu směrnice o ochraně osobních údajů.[158]

Směrnice o soukromí a elektronických komunikacích je speciálním právním předpisem (*lex specialis*), a použije se tedy jen ve specifických situacích. Konkrétně v případě zpracování osobních údajů v odvětví elektronických zařízeních a elektronické komunikace, kdy je nutné řídit se speciální úpravou. Směrnice o ochraně osobních údajů je naopak obecným právním předpisem (*lex generalis*), použije se tedy ve všech případech, na něž se nevztahuje speciální úprava. Cílem speciální směrnice je reagovat na technický pokrok, především v rozvoji internetu[159], a zpřesnit úpravu v obecnější směrnici.[160] V praxi bude nutné aplikovat obě uvedené směrnice, respektive národní právní akty, které směrnice implementují.

[157] Body 4-8 preambule směrnice o soukromí a elektronických komunikacích

[158] Čl. 1 odst. 2 směrnice o soukromí a elektronických komunikacích

[159] Body 4-6 preambule směrnice o soukromí a elektronických komunikacích

[160] Čl. 1 odst. 2 směrnice o soukromí a elektronických komunikacích

Směrnice o soukromí a elektronických komunikacích oproti obecnější směrnici na ochranu osobních údajů mimo jiné:

- nařizuje ochranu důvěrnosti sdělení během elektronické komunikace, včetně obsahu a údajů vztahujících se k takovým sdělením,[161]
- poskytuje ochranu oprávněných zájmů i právnických osob,[162]
- zakazuje neoprávněný přístup ke sdělením přenášených prostřednictvím veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací,[163]
- nařizuje povinnost informovat dotčené osoby a regulační orgány v případě ohrožení bezpečnosti osobních údajů,[164]
- nařizuje vymazat či anonymizovat nepotřebné údaje o účastnících komunikace,[165]
- upravuje podstatu provozních a lokalizačních údajů, postup a povinnosti při nakládání s těmito údaji,[166]
- reguluje zasílání nevyžádaných reklamních sdělení pomocí elektronických sítí.[167]

Na činnost subjektů, které obchodují s osobními údaji, dopadá primárně obecnější směrnice o ochraně osobních údajů.

Pro jakékoliv komerční zpracování osobních údajů je nutné splnit kritéria evropských směrnic, které však představují minimální standard, což znamená, že v některých případech lze v jednotlivých státech implementovat přísnější legislativu.

Osobní údaje osob v Evropské unii je nutné:

- zpracovávat korektně

[161] Čl. 1 směrnice o soukromí a elektronických komunikacích

[162] Čl. 1 odst. 2 směrnice o soukromí a elektronických komunikacích

[163] Čl. 4 odst. 1a směrnice o soukromí a elektronických komunikacích

[164] Čl. 4/ odst. 2-3 směrnice o soukromí a elektronických komunikacích

[165] Čl. 6 směrnice o soukromí a elektronických komunikacích

[166] Čl. 6 a 9 směrnice o soukromí a elektronických komunikacích

- shromažďovat jen pro výslovně a legitimně stanovené účely
- shromažďovat a zpracovávat přiměřeně s ohledem na stanovený účel
- mít možnost opravit či vymazat
- neuchovávat po dobu delší než je nutné pro splnění účelu, pro který jsou shromažďovány a zpracovávány[168]

Data brokers by pro použití osobních údajů museli dále splnit alespoň jednu z následujících zásad pro oprávněné zpracování osobních údajů:

- získat nezpochybnitelné udělení souhlasu[169], který je svobodný, výslovný a vědomý[170]
- zpracování je nutné pro splnění smlouvy, přičemž osoba je jednou ze stran smlouvy[171]
- zpracování je nezbytné pro realizaci oprávněných zájmů správce nebo třetí osoby, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody osob[172]

Tyto dva sety obecných pravidel a zásad představují základní právní rámec pro činnost data brokers a společností, které obchodníkům cizí osobní údaje poskytují.

Zpracovávat osobní údaje lze jen za předpokladu, že osoba, jíž se údaje týkají, nezpochybnitelně udělila svobodný, výslovný a vědomý souhlas se zpracováním svých údajů.[173] Existují i možnosti, kdy osoba, jíž se údaje týkají, nemusí souhlasit se zpracováním svých údajů, nicméně z povahy obchodování s osobními údaji se ty mody spíše nevyužijí.[174]

---

[167] Čl. 13 směrnice o soukromí a elektronických komunikacích

[168] Čl. 6 směrnice o ochraně osobních údajů

[169] Čl. 7 písm. a) směrnice o ochraně osobních údajů

[170] Čl. 2 písm. h) směrnice o ochraně osobních údajů

[171] Čl. 7 písm. b) směrnice o ochraně osobních údajů

[172] Čl. 7 písm. f) směrnice o ochraně osobních údajů

[173] Čl. 2 písm. h) a čl. 7 písm. a) směrnice o ochraně osobních údajů

[174] Čl. 7 písm. b-f) směrnice o ochraně osobních údajů

Existují dvě možnosti, jak data broker údaje získá. Sám přímo od osoby, jejíž osobní údaje budou shromažďovány nebo zpracovávány (tzv. subjekt údajů), nebo od třetí strany, která údaje od subjektu údajů získala. Subjekt údajů musí být informován v obou případech o totožnosti toho, kdo údaje zpracovává nebo shromažďuje a pro jaké účely, komu budou údaje poskytovány (tzv. příjemce) a o možnosti přístupu ke svým údajům.
V prvním případě, pokud broker získává údaje přímo od subjektu údajů, musí navíc informovat, zda je zadání osobních údajů povinné nebo dobrovolné a uvést případné následky neposkytnutí údajů (například neposkytnutí služby).
V druhém případě, pokud broker získává údaje od třetích stran, musí tyto třetí strany již před prvním získáním informovat subjekt údajů o výše uvedených skutečnostech, spolu s uvedením, jaké osobní údaje budou dále předávány.[175]

Každý členský stát je povinen mít alespoň jeden nezávislý úřad[176] věnující se dohledu nad dodržováním těchto pravidel v oblasti ochrany osobních údajů.[177] Tyto úřady jsou také kontaktními místy pro občany, s jejichž daty bylo nelegálně nakládáno i pro organizace, které obchodují s osobními údaji. V případě porušení národní legislativy v oblasti osobních údajů jsou tyto orgány oprávněné k udělování správních sankcí za delikty v oblasti ochrany osobních údajů.

Současná právní legislativa Evropské unie neupravuje výši sankcí za porušení směrnic, v tomto případě je nutné sankce hledat již v legislativě toho státu, ve kterém k porušení došlo. V České republice může Úřad pro ochranu osobních údajů právnickým osobám a podnikajícím fyzickým osobám udělit pokutu do 5 000 000 Kč, a v případě ohrožení většího počtu osob neoprávněným zasahováním do soukromého a osobního života nebo porušením povinností při zpracování citlivých údajů je možné udělit pokutu až do výše 10 000 000 Kč. Pro fyzické osoby je tato pokuta nižší, nicméně je pravděpodobné, že data brokers budou svou činnost vykonávat jako právnické osoby.

[175] Čl. 10-11 směrnice o ochraně osobních údajů

[176] Seznam úřadů v jednotlivých státech lze nalézt na http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

[177] Čl. 28 směrnice o ochraně osobních údajů

Pro porovnání, ve Spolkové republice Německo je možné uložit pokutu v maximální výši 50 000 Euro (cca 1,35 milionu Kč), respektive 300 000 Euro (cca 8,1 milionu Kč), jedná-li se o závažnější porušení německého zákona na ochranu osobních údajů.[178] V případě ekonomického obohacení je navíc možné uvedené limity překročit, tak aby výše trestu vyvážila případné zisky z nelegální činnosti.[179] Nejsou zde rozděleny pokuty podle subjektů jako v ČR, nicméně lze předpokládat, že reálná výše pokuty bude vyšší u právnických osob. Ve Spojeném království Velké Británie a Severního Irska není maximální výše pokuty stanovena samotným zákonem. Zákon však zmocňuje Komisaře pro informace (Information Commissioner) k vydání metodiky na vymáhání norem na ochranu osobních údajů.[180] Tato metodika také určila maximální výši pokuty na 500 000 liber[181] (cca 15,9 milionu Kč). Z výše uvedeného vyplývá, že případná porušení norem budou řešit úřady jednotlivých států, a ty mohou ukládat pokuty v různých výších. Vzhledem k mezinárodní povaze internetu, a tedy i obchodu s osobními údaji, je nutné rozlišit lokální působnost národních úřadů, tedy určit úřad kterého státu bude porušení směrnic (resp. národních zákonů, pomocí kterých byly směrnice implementovány) sankcionovat. Pravidlo[182], podle kterého lze určit příslušnost místní úřadu, je místo, kde má společnost spravující osobní údaje sídlo nebo provozovnu. Není-li správce usazen na území EU, ale používá pro zpracování osobních údajů prostředky umístěné na území Unie (například servery), je rozlišovacím znakem stát, ve kterém jsou tyto prostředky umístěny.[183]

Každý správce údajů má povinnost ohlásit zpracovávání osobních údajů dozorovému orgánu (v České republice Úřad pro ochranu osobních údajů). V tomto ohlášení musí

[178] Do této kategorie spadá například neoprávněné (automatizované i ruční) zpracování a sběr neveřejných osobních údajů, nedovolené poskytnutí údajů jiným osobám, nedovolené použití údajů pro marketingové účely, aj.

[179] § 43 Bundesdatenschutzgesetz. Citováno z: *BDSG - Bundesdatenschutzgesetz:* [online]. [cit. 2017-01-26]. Dostupné z: https://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html

[180] Čl. 55C Data Protection Act 1998. Citováno z: *Data Protection Act 1998:* [online]. [cit. 2017-01-26]. Dostupné z: http://www.legislation.gov.uk/ukpga/1998/29/section/55C

[181] *Ico-guidance-on-monetary-penalties.pdf* [online]. 36 s. [cit. 2017-01-26]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf. Str. 10.

[182] V právní terminologii se používá pojem *hraniční určovatel*.

[183] Čl. 4 směrnice o ochraně osobních údajů

být obdobné informace jako při informování subjektů údajů[184] spolu s uvedením předpokládaného zpřístupnění do států mimo Evropskou unii a s uvedením obecného popisu přijatých technických a organizačních opatření, které mají sloužit bezpečnému zpracování.[185] Tato ohlášení jsou pak uvedena ve veřejném registru u každého správce údajů.[186] Smysl těchto ohlášení spočívá ve zvýšení transparentnosti nakládání s osobními informacemi, a tím i k jednoduššímu procesu kontroly ze strany státního orgánu. V registru jsou uvedeny mimo jiné kontaktní adresy, na kterých lze od správců (včetně data brokerů) žádat informace, opravu údajů a případně odebrat souhlas se zpracováním údajů. V praxi však přínos pro fyzické osoby považuji za malý, jelikož v typickém případě dotčený člověk neví jméno data brokera, který má jeho osobní údaje k dispozici.

Osobní údaje mohou být uchovávány jen po nezbytnou dobu s ohledem na cíle, pro které byly zpracovány.[187] Toto ustanovení by mělo zabránit uchování osobních údajů na zbytečně dlouhou dobu, pokud k tomu není legitimní důvod, což představuje další překážku v dlouhodobém sběru informací o určitých osobách a vytváření databází s jejich profily. Nezbytná délka uložení nebo zpracovávání se bude posuzovat individuálně pro každý případ.[188]

Z výše uvedeného vyplývá, že evropská regulace klade na data brokers přísné požadavky. Zpracovávat osobní údaje lze jen za předpokladu, že osoba, jíž se údaje týkají, nezpochybnitelně udělila svobodný, výslovný a vědomý souhlas se zpracováním svých údajů. Existují i možnosti, kdy osoba, jíž se údaje týkají, nemusí souhlasit se zpracováním svých údajů. V případě navštěvování internetových stránek a s tím

[184] Nemusí zde být informace o existenci práva na přístup a opravu osobních údajů.

[185] Čl. 18-19 směrnice o ochraně osobních údajů

[186] Například Karlova univerzita ke dni citace měla 64 ohlášení, lišíce se lokalitou, zdrojem osobních údajů (např. kamerový systém, přímo od osob), subjektem údajů (studenti, zaměstnanci, návštěvníci) Citováno z: *Správci osobních údajů: zaregistrovaná zpracování:* [online]. [cit. 2017-01-26]. Dostupné z: https://forms.uoou.cz/registration.aspx?id=191313

[187] Čl. 6 odst. 1 písm. e) směrnice o ochraně osobních údajů

[188] Obdobné ustanovení je i v GDPR (čl. 5 odst. 1 písm. e), ale navíc obsahuje povinnost informovat subjekt údajů o předpokládané délce zpracování, resp. o kritériích, které délku určí (čl. 15 odst. 1 písm. d).

souvisejícím sběrem informací se však tyto mody nevyužijí. Pokud souhlas subjektů údajů nesplní všechny požadavky, je možné správce nebo zpracovatele pokutovat podle národních norem.

Z tohoto důvodu se domnívám, že ve členských státech existuje jen velmi malý prostor pro legální činnost data traders v takovém rozsahu, jež je zdokumentován v USA.

4.2.3. Regulace v EU od května 2018

Od 25. května 2018 vstoupí v účinnost obecné nařízení o ochraně osobních údajů (GDPR), které, mimo jiné, zruší směrnici o ochraně osobních údajů. Ačkoliv cíle a zásady směrnice a nařízení jsou stejné[189], přináší GDPR některé změny. Už jen samotný typ normy (tedy nařízení) je značnou změnou vedoucí k jednotnému vnímání ochrany osobních údajů v celé Evropské unii. Každý členský stát bude mít identický text nařízení, čímž se odstraní odlišnosti v národních normách, které směrnice připouštěla. Tím se usnadní a zpřehlední regulace osobních údajů pří transakcích mezi členskými i nečlenskými státy.

Potřeba nové právní normy je spojována s technologickým pokrokem v posledních 20 letech[190], pokračující globalizací, zvýšenou výměnou informací.[191]

Nové nařízení o ochraně osobních údajů poskytuje odlišnou formulaci zásad[192] nakládání s osobními údaji. Jsou jimi:

- zákonnost, korektnost a transparentnost
- účelové omezení (určité a legitimní)
- minimalizace údajů
- přesnost (a možnost opravy a výmazu nepřesných údajů)
- omezení uložení (jen na nutnou dobu)

[189] Bod 9 preambule GDPR

[190] Současná směrnice musela být implementována do 24 října 1998. Čl. 32/1 směrnice o ochraně osobních údajů

[191] Body 5, 6 preambule GDPR

- integrita a důvěrnost (zajištění zabezpečení údajů)
- odpovědnost (správce) [193]

GDPR sjednocuje výši pokut za porušení tohoto nařízení pro všechny členské státy do maximální možné výše 20 000 000 milionů eur (přes 500 milionů korun) nebo 4 % celosvětového ročního obratu podniku, podle toho, která částka je vyšší.[194] Právě výše pokut je jednou z velkých změn a zároveň motivací pro důslednou přípravu společností na vstup GDPR v účinnost, jelikož pokuty podle doposud platné úpravy jsou řádově nižší, například v ČR 50x nižší. Zmíněná 4 procenta z celosvětového ročního obratu mohou dosáhnout u největších evropských společností hodnot miliard eur.

Společnosti, jejichž hlavní činností je zpracovávání osobních údajů nebo rozsáhlé, pravidelné a systematické monitorování občanů, budou muset nově jmenovat pověřence pro ochranu osobních údajů (*data protection officer*). Tato osoba bude muset disponovat některými profesními kvalitami, musí mít zejména adekvátní znalosti práva a praxi v oblasti osobních údajů.[195] Pověřenec bude mít povinnosti interní a externí. Mezi interní úkoly patří poskytování poradenství správcům a zpracovatelům osobních údajů, jako i jejich zaměstnancům. Dále bude muset monitorovat dodržování předpisů a zvyšovat erudici osob, které osobní data spravují[196] a vydávat posudky při zavádění nových technologií nebo postupů, které by mohly mít vliv na bezpečí osobních údajů.[197] Mezi externí úkoly patří především spolupráce a komunikace s dozorovým orgánem.[198]

Toto nařízení se bude přímo vztahovat na všechny fyzické i právnické osoby přítomné nebo usazené na území členských států. Novinkou je povinnost řídit se tímto nařízením i pro subjekty neusazené v EU, jejichž činnost souvisí s monitorováním chování lidí nebo s nabízením služeb subjektům v EU.[199]

---

[192] Obdobné zásady jsou obsaženy v čl. 6 a 7 současné směrnice.

[193] Čl. 5 GDPR

[194] Čl. 83 GDPR

[195] Čl. 37 GDPR

[196] Čl. 37 písm. a-b) GDPR

[197] Čl. 35 GDPR

[198] Čl. 37 písm. d-e) GDPR

[199] Čl. 3 odst. 2 GDPR

Toto nové ustanovení tedy přímo dopadá i na data brokers z nečlenských států, kteří by monitorovali kohokoliv na území státu EU. Dochází zde tedy možné extrateritorialitě nařízení, což jistě koreluje s rostoucí globalizovaností datových toků, včetně toku osobních údajů za hranice Evropské unie. V extrémním případě si lze představit situaci, kdy data broker z nečlenského státu bude evropským orgánem dozoru potrestán za monitorování příslušníka nečlenského státu při jeho pobytu v EU. Otázkou zůstává vymahatelnost případných nápravných opatření a sankcí udělených orgánem na ochranu osobních údajů jednoho ze členských států společnosti, která nemá v EU místo výkonu činnosti.

Novinkou je také přísnější posuzování, zda subjekt údajů udělil souhlas se zpracováním svých údajů. Podle GDPR musí být souhlas udělen aktivně (prohlášením nebo jiným zjevným potvrzením), ne jen předvyplněným checkboxem nebo mlčením.[200] Má-li být udělený souhlas platný, musí být žádost srozumitelná, stručná a jasně oddělená od ostatních podmínek.[201] Subjekt údajů zároveň musí mít objektivní možnost rozhodnout se neudělit souhlas, aniž by bylo omezeno poskytnutí služby, pokud tyto údaje nejsou nezbytné pro poskytnutí služby.[202] Zpracovatel údajů bude povinen i v ostatní komunikaci jednat transparentním, srozumitelným a stručným způsobem.[203] Bude-li poskytnutí souhlasu se zpracováním osobních údajů založeno na jasné nerovnováze ve vztahu zpracovatele a subjektu údajů, neměl by být souhlas platný, a tedy zpracování bude nezákonné, nebude-li existovat jiný právní důvod.[204]

V současné praxi je běžné, že do smluvních podmínek online služeb a programů je zakomponován souhlas s použitím osobních údajů pro marketingové účely. Tyto podmínky bývají často pro průměrného uživatele příliš dlouhé. Od května 2018 bude muset být tento souhlas oddělen od ostatních smluvních podmínek, dále bude muset být stručný, srozumitelný a nesmí jim být podmíněno použití produktu.[205]

---

[200] Čl. 4 odst. 11 GDPR; Bod 32 preambule GDPR

[201] Čl. 7 odst. 2 GDPR; Bod 32 preambule GDPR

[202] Čl. 7 odst. 4 GDPR; Bod 32 preambule GDPR

[203] Čl. 5 odst. 1 písm. a), čl. 12 GDPR

[204] Bod 43 preambule GDPR

[205] Například při upgrade Windows 8 na Windows 10 bylo nutné souhlasit se zpracováním osobních údajů i pro marketingové účely a pro „zlepšení produktů společnosti Microsoft“. Bez udělení souhlasu

Zásada minimalizace údajů představuje další krok ve snaze ochránit osobní údaje občanů EU. V současné směrnici je zakotvena povinnost, že zpracování údajů nesmí přesáhnout míru s ohledem na účel zpracování a shromažďování a toto musí být přiměřené.[206] Podle GDPR bude nakládání s osobními údaji omezené na nezbytný rozsah ve vztahu k účelu[207], což ještě více omezí možnost uchování pro transakci nerelevantních dat.

Nově je formulováno ustanovení ohledně práva být zapomenut (*right to be forgotten, right to erasure*). Nyní platí, že občan má poměrně široce artikulované právo na výmaz informací, které nejsou zpracovány v souladu se směrnicí.[208] Výklad tohoto ustanovení byl upřesněn judikaturou Soudního dvora Evropské unie.[209] Podle nové formulace bude existovat šest okolností, které zapříčiní vznik práva na výmaz údajů.[210] Obdobně jsou nově precizněji formulovány okolnosti, za nichž mohou subjekty údajů žádat omezení zpracování.[211] Stejně jako dříve, i v budoucnu bude správce povinen žádost o vymazání nebo omezení zpracování oznámit všem dalším subjektům, kterým osobní informace poskytl, není-li to nemožné nebo nevyžaduje-li to nepřiměřené úsilí. Nově si však bude mít subjekt údajů právo si také v této souvislost vyžádat informaci, kterým dalším subjektům byla jeho data poskytnuta.[212]

V nařízení je implicitní výzva k zavedení pečetí a známek dokládající soulad aktivit správců a zpracovatelů údajů s GDPR.[213] Lze si představit tuto známku na první stránce

---

nešlo v upgrade pokračovat. Prohlášení společnosti Microsoft o zásadách ochrany osobních údajů mělo 60 stránek (vel.písma 12, řádkování 1,5). In: *Prohlášení společnosti Microsoft o zásadách ochrany osobních údajů – Microsoft a ochrana osobních údajů:* Verze Leden 2016 [online]. [cit. 2017-02-10]. Dostupné z: https://privacy.microsoft.com/cs-cz/privacystatement?PrintView=true

[206] Čl. 6 odst. 1 písm. c) směrnice o ochraně osobních údajů

[207] Čl. 5 odst. 1 písm. b) GDPR

[208] Čl. 12 písm. b) směrnice o ochraně osobních údajů

[209] Především rozsudkem SDEU č. C-131/12 ze dne 13. května 2014, ve věci Google Spain SL,Google Inc. Proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

[210] Čl. 17 GDPR

[211] Čl. 18 GDPR

[212] Čl. 12 písm. c) směrnice o ochraně osobních údajů a čl. 19 GDPR

[213] Čl. 42 GDPR

webů nebo v místě, kde uživatel internetu uděluje souhlas se zpracováním svých osobních údajů, tak aby uživatel služby mohl na první pohled identifikovat úroveň ochrany údajů.[214] Podobná označení sloužící k poskytnutí informace o důvěryhodnosti webu jsou v současné době často přítomna například při online platbě kartou nebo jako důkaz, že e-shop splňuje podmínky nějaké organizace.

Výše uvedený rozbor obsahuje především zpřesnění aktuální legislativy. V některých případech však zavádí do ochrany osobních údajů nové prvky. Existují desítky rozdílů mezi současnou a budoucí úpravou, v každém případě lze shrnout, že i s účinností GDPR bude legislativní rámec pro činnost data traders velmi přísný. Lze pozorovat snahu upřednostnit právo na soukromí fyzických osob před komerčním použitím jejich osobních údajů. Lze si proto jen těžko představit, že by ve členských státech mohlo probíhat získávání osobních údajů bez vědomosti samotných osob, kterých se týkají. Pokud by tomu tak bylo, sankce za porušení nového nařízení jsou, natolik přísné, že by případného data brokera mohly finančně zlikvidovat. Ačkoliv smysl sankcí je spíše preventivní, pokuta ve výši 20 000 000 eur nebo 4 % hrubého konsolidovaného ročního obratu může působit likvidačně.

[214] Příkladem takové známky poukazující na soulad činnosti provozovatele webové stránky se zákonem, jenž řeší i ochranu některých osobních údajů, lze nalézt na konci www.reputation.com. Zde je pečeť HIPAA odkazující na informace o *Health Insurance Portability and Accountability Act.*

5. Legitimita obchodování s osobními údaji

5.1. *Etika v době nových médií*

Podle názoru evropského inspektora ochrany údajů[215] je nutné i v době digitální revoluce a big data dodržovat zásady ochrany soukromí a důstojnosti člověka. Důraz klade také na dodržování etických pravidel, která by i nadále měla fungovat jako primární korelativ této digitální doby.[216]

Etika a nové moderní technologie je téma objevující se stále častěji. Vzhledem k rychlému rozvoji nových médií nestačí regulace včas reagovat na objevující se negativní jevy. Často tak nezbývá použít sociální normy a etická pravidla pro posouzení toho, co je správné a co není. Tato pravidla však nejsou zcela přesně určená a zpravidla ani vymahatelná. Zároveň se v různých kulturách liší. Podle mého názoru však na internetu existují etická pravidla globální. Zároveň pociťuji, že popsaná praxe data brokers není s touto etikou zcela v souladu, a to ani v případě, kdy je tato obchodní aktivita v některém státě legální.

Jako neetické vnímám především netransparentnost celého businessu. Tím, že američtí data traders odmítají prozradit své zdroje informací[217], zde dochází k asymetrickému postavení, kdy občané nemají dostatek informací a oproti tomu data brokers jich mají

[215] V rámci EU existuje nezávislý inspektor ochrany, jenž dohlíží na dodržování právních norem a standardů na ochranu osobních údajů v jednotlivých orgánech a institucích EU, také je poradním orgánem Soudního dvora EU či monitoruje technologický vývoj mající vliv na soukromí Evropanů. Citováno z:.*About - European Data Protection Supervisor:* [online]. [cit. 2017-05-08]. Dostupné z: https://edps.europa.eu/about-edps_en

[216] *Shrnutí stanoviska č. 4/2015 evropského inspektora ochrany údajů, „Směrem k nové digitální etice: Data, důstojnost a technologie" (2015/C 392/08)* [online]. 2015 [cit. 2017-05-08]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=uriserv:OJ.C_.2015.392.01.0009.01.CES

[217] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str.18, 27, 39.

příliš mnoho. Američtí občané zároveň nemají plnou kontrolu nad svými údaji. I v případě, pokud by věděli, jaké jejich osobní údaje jsou zužitkovávány třetími stranami, lze se z těchto transakcí vyvázat jen s velkými obtížemi a úsilím, pokud vůbec. V rozporu s digitální etikou se také jeví fakt, že fyzické osoby nemají z obchodování se svými údaji žádný přínos.
Skutečnost, že některá osobní data, jsou veřejně dostupná online, neopravňuje ostatní subjekty tato data bez souhlasu použít pro svůj vlastní zisk.[218]

Předpokládám proto, že čím dál častěji se bude hovořit o nutnosti zvýšit transparentnost data traders a vylepšit pozici fyzických osob, tak aby došlo ke spravedlivému trhu.

5.2. *Konflikt práva na svobodu podnikání a práva na ochranu soukromí*

Stejně jako jsou v moderních státech chráněna osobnostní práva, je v moderních státech dbáno i na ochranu práva podnikání.[219] Tato práva však nemusí být vždy v symbióze. Obchodování s osobními údaji je dobrým příkladem tohoto konfliktu, Je častým úkazem, že podniky a podnikatelé jsou omezováni rozličnými zákony, ať už například se jedná o stanovení minimální mzdy či omezení délky pracovní doby zaměstnanců nebo o zákaz vypouštět nebezpečné látky do okolí. Kdyby tato omezení neexistovala, docházelo by k negativním společenským jevům. Pro podnikatele to však přináší povinnost nutných investic, které nemají návratnost. Bez základních právních omezení ve prospěch, například zaměstnanců či životního prostředí, lze pochybovat, o tom, že by

[218] BOYD, Danah a Kate CRAWFORD. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication, & Society.* [online]. **15**(5), 32. s [cit. 2017-03-06]. Dostupné z: www.danah.org/papers/2012/BigData-ICS-Draft.pdf. Str. 18-21

[219] Bod 4 preambule GDPR „Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy. Toto nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou, jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost.“

podnikatelé dobrovolně začali uplatňovat nějaká omezující opatření ve prospěch občanů či veřejných statků. Jak situace v zemi vypadá, když minimální standardy chybí, lze pozorovat v rozvojových státech.

Vývoj společnosti je úzce spojen s objevováním nových věcí a nových podnikatelských nápadů. Tyto novinky jsou mnohdy zpočátku neregulované, pokud se ale časem ukáže, že s sebou přináší negativní konsekvence, jsou dříve či později regulovány. Postupným společenským vývojem dochází v právním státě, podle mého názoru, ke stálé prohlubujícímu se omezování existujících podnikatelských aktivit ve prospěch blahobytů občanů.

Stejně jako nulová regulace ekonomických subjektů není pro společnost žádoucí ani přílišná regulace. Ne vždy je snadné tyto protipóly vybalancovat ke spokojenosti celé komunity. Společnost navíc není rigidní, ale velmi dynamická. To, co mohlo být považováno za optimální řešení před pěti lety, nemusí být optimálním řešením dnes.

Zdá se ale, že současná evropská společnost dosáhla takového stupně rozvoje, že jedním z aktuálních témat je právě ochrana osobních údajů. Soukromí osob je, z pohledu celé společnosti, důležitější než profit data brokers. Proto existují, alespoň na území Evropské unie, přísné normy ukládající správcům osobních údajů povinnosti, které jim přináší zvýšené náklady. Je však pravděpodobné, že v budoucnu bude tato regulace tak přirozená, jako je dnes omezení pracovní doby nebo ochrana životního prostředí.

5.3. *Konflikt informačních práv a práva na ochranu osobnosti*

Problematika data brokers také naráží na konflikt práva na ochranu soukromí a práva na svobodu projevu spolu s právem na svobodný přístup k informacím.
Soudní dvůr Evropské unie posuzoval v roce 2014 ve známém případu Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González konflikt práva svobodný přístup k informacím a práva na ochranu soukromí. Žalobce se domáhal výmazu z vyhledávácích výsledků Google, který to však odmítal mj. s poukazem na právo ostatních získat objektivní informace o žalobci. SDEU se

přiklonil právě k ochraně soukromí, jež považuje za důležitější než obchodní aktivitu vyhledávače, a za některých okolností i než právo ke svobodnému přístupu k informacím.[220] Toto rozhodnutí tak tvoří základ relativně nového práva občanů EU, práva být zapomenut, a tedy i nebýt zobrazován ve výsledcích online vyhledávacích nástrojů.

Jak je uvedeno výše[221], například v USA toto právo není zakotveno, jelikož zde naopak převažuje silná ochrana práva na svobodu projevu, která může být interpretována i jako právo vyhledávače zveřejňovat široké spektrum vyhledávacích výsledků.
Omezování svobody projevu je však, i vzhledem k historickým zkušenostem evropských států, citlivé téma. Existuje jen tenká hranice mezi legitimním omezením přístupu k informacím a cenzurou. Jak také konstatuje SDEU je nutné nalézt spravedlivou rovnováhu mezi těmito právy.[222]

[220] Např. body 81 a 97 rozsudku. Citováno z: *CURIA - Dokumenty: Rozsudek SDEU č.* C-131/12 *ze dne 13. května 2014, ve věci Google Spain SL,Google Inc. Proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [online]. [cit. 2017-04-15]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=118910

[221] Viz kapitola 4.2.3.

[222] Bod 81 rozsudku. Citováno z: *CURIA - Dokumenty: Rozsudek SDEU č.* C-131/12 *ze dne 13. května 2014, ve věci Google Spain SL,Google Inc. Proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [online]. [cit. 2017-04-15]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=118910

6. Alternativní a budoucí trendy

6.1. *Rozšíření definice osobní informace*

V reportu pro bývalého senátora Rockefellera je uvedena i obhajoba společností, které obchodují s daty internetových uživatelů. Společnosti mj. uvedly, že jejich digitální produkty zabezpečují lidem větší míru soukromí, protože tyto informace nejsou přiřaditelné ke konkrétní osobě, ale tyto „neosobní osobní" údaje se přiřazují pouze ke kódu namísto jména. Tímto se dostáváme k limitu definice osobních údajů, jelikož data mohou být vztažena jen k počítači či mobilnímu telefonu, ne ke konkrétní osobě.

Jak je uvedeno výše[223], pro naplnění evropské definice osobního údaje musí podle tohoto údaje být identifikovaná nebo identifikovatelná konkrétní fyzická osoba. Nabízí se otázka, zda i v Evropské unii neexistují případy, kdy údaj nelze považovat za osobní, protože nelze přiřadit k osobě, ale lze jej přiřadit ke konkrétnímu zařízení, například počítači nebo mobilnímu telefonu, nebo ke konkrétnímu software, například internetovému prohlížeči. V současné marketingové praxi nejsou jméno, adresa, věk ani jiné „klasické" osobní údaje konkrétní osoby tak podstatné, jako dříve, jelikož zákazníka lze zacílit i bez těchto údajů. V Evropské unii lze pozorovat trend rozšiřování chápání toho, co je osobní údaj. V novém nařízení jsou přidány i biometrické a genetické údaje a také síťové identifikátory.[224] Soudní dvůr EU však již i podle současné směrnice v závislosti na dalších okolnostech považuje IP adresu za údaj, který může osobu identifikovat.[225] Jaké informace jsou považovány za osobní je uvedeno ve směrnici o ochraně osobních údajů i GDPR jen demonstrativním výčtem, což umožnuje použití norem i pro údaje, které nejsou v právních aktech výslovně uvedené.

---

[223] Viz kapitola 4.2.1

[224] Bod 30 preambule GDPR

[225] Bod 65 Rozsudku SDEU č. C-582/14. *In CURIA - Dokumenty: Rozsudek SDEU č. C-582/14 ze dne 19. října 2016, ve věci Patrick Breyer proti Bundesrepublik Deutschland* [online]. [cit. 2017-04-15]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945

Hranice, kdy lze na základě nějakých dat potenciálně identifikovat konkrétní osobu není jasná, ale záleží právě na konkrétních okolnostech, které bude posuzovat relevantní správní orgán, respektive soud konkrétního státu. A v případě nenalezení koncensu na národní úrovni posoudí situaci v poslední instanci SDEU. Pokud by však nějaká společnost dokázala zacílit přístroje bez použití osobních identifikátorů, dalo by se uvažovat o legitimním využití tohoto zaměření. Podle dostupných informací se však zdá, že v současnosti není této regulatorní *šedé zóny* využíváno.

Pokud by se v budoucnu vyskytl problém s výše uvedeným, lze, podle mého názoru využít i samotných zásad uvedených v regulaci EU. Konkrétně zásady korektnosti, přiměřenosti a transparentnosti by pravděpodobně zamezila použití osobních dat, které by byly používány proti smyslu norem na ochranu soukromí fyzických osob.
Předpokládám, že s dalším vývojem technologií se bude dále vyvíjet i pojetí osobního údaje.

6.2. *Samoregulace*

Američtí data brokers v současnosti vlastní samoregulační spolek nemají[226], někteří však avizují, že jejich interní pravidla jsou v souladu s Guidelines for Ethical Business Practices, která vydala Direct Marketing Association.[227] Existují i další samoregulační spolky sdružující společnosti činné v reklamním průmyslu, jejichž některé regulační mechanismy zasahují i do aktivit data brokers. Mezi nejvýznamnější působící v USA

[226] V roce 1997 proběhl pokus o vytvoření samoregulační organizace Individual References Services Group (IRSG), jejímiž členy měly být velké americké společnosti. Tehdy byla ochrana osobních údajů na internetu pouze sekundárním cílem této organizace; primárně cílila na offline sféru. Organizace byla ukončena v roce 2001 bez zanechání známek úspěšných výsledků. Více v PLESSER, Ronald a CIVIDANES, Emilio. *COMMENTS OF THE INDIVIDUAL REFERENCE SERVICES GROUP ON ELEMENTS OF EFFECTIVE SELF REGULATION FOR THE PROTECTION OF PRIVACY AND QUESTIONS RELATED TO ONLINE PRIVACY* [online]. 1998 [cit. 2016-08-26]. Dostupné z: https://www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/irsgcom.html

[227] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 38-39.

patří Digital Advertising Alliance, poskytující pravidla upravující cross-device tracking nebo online behaviorální reklamu. Digital Advertising Alliance zároveň zastřešuje i další organizace, které se věnují propagaci práv spotřebitelů, zvýšení transparentnosti online reklamy.[228]

Podle dostupných informací neexistují samoregulační asociace data brokers ani v evropském měřítku. Domnívám se, že je to zapříčiněno poměrně přísnou veřejnou regulací, díky níž není důvod pro existenci těchto asociací.

Samoregulace však může být vhodnou alternativou k regulaci zákonné, pokud tato ve státě chybí. Problémem je, že záleží jen na rozhodnutí samotných společností pro vstup do samoregulační instituce. Společnosti však logicky mají jen malou motivaci samy sebe omezovat. Motivací by mohlo být větší mediální pokrytí tohoto businessu a následná odmítavá reakce většího množství lidí.

Jiným impulsem by mohla být zvýšená iniciativa státních úřadů kontrolovat data brokers, přičemž vznik, respektive vstup do samoregulatorní organizace by mohl sloužit jako dostatečný nápravný argument pro dodržování best practice, a tedy i vyhnutí se negativní pozornosti státních institucí. Na základě výše uvedené právní analýzy[229] se však zdá, že američtí data traders neporušují státní regulaci. Nelze proto ani data brokers za tuto obchodní aktivitu postihovat.

Pro vznik samoregulační platformy by se, podobně jako se to stalo v mnoha jiných oborech, spojilo několik vedoucích společností na relevantním trhu do nějaké asociace či spolku, který postupem času začne propagovat samoregulaci jako optimální cestu, a to na základě jejich zavedené praxe s občasným korelativem veřejných institucí nebo veřejného mínění. Spolupráce konkurentů přináší minimálně čtyři výhody: tyto asociace působí solidnějším dojmem pro zákazníky, mají větší vyjednávací sílu vůči státním úřadům, v mnoha případech představují překážku pro vznik nebo rozmach konkurence a jsou platformou pro sdílení best practice a know-how (a tedy snížení výdajů).

[228] *DigitalAdvertisingAlliance.org* [online]. [cit. 2017-04-27]. Dostupné z: http://digitaladvertisingalliance.org/principles

[229] Viz kapitola 4.1.1.

Domnívám se proto, že jednou z možných budoucích cest, jak posílit práva Američanů na ochranu soukromí, je vznik samoregulační instituce i v oblasti obchodu s osobními údaji, podobně jako například v oblasti regulace dostupnosti audiovizuálních děl nezletilému publiku, kde v USA vnikla samoregulační asociace Motion Picture Association of America (MPAA).[230]

6.3. *Odměna za poskytnutí osobních údajů*

Osoby, které své údaje poskytnou prostřednictvím dotazníků na internetu, mohou v některých případech získat přímou odměnu v podobě slevových kuponů nebo mají šanci získat odměnu v podobě zařazení do slosování o peněžní a jiné výhry.[231]

Objevují se také názory, že provozovatelé sociálních sítí a jiní shromažďovatelé osobních údajů by mohli platit subjektům údajů za používání sociálních sítí nebo za získávání informací o nich.[232] Ačkoliv může tato myšlenka z dnešního pohledu vypadat nereálně, v USA již existuje společnost platící lidem za jejich údaje. Jedná se o společnost DataCoup, Inc,[233] která platí řádově dolary měsíčně za data o využívání platebních karet a sociálních sítí.[234] Podle dostupných informací se jedná o první službu platící zákazníkům penězi za poskytnutí jejich údajů.

---

[230] POVEJŠIL, Tomáš. *Právní regulace dostupnosti digitálního obsahu mladistvým*. Brno, 2014. Diplomová práce. Masarykova univerzita. Vedoucí práce Radim Polčák. Str. 36-38.

[231] *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013, 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Str. 25, 26.

[232] SIMON, Phil. Facebook: The New King of Data Brokers? In: *Wired.com* [online]. [cit. 2016-06-30]. Dostupné z: http://www.wired.com/insights/2014/10/facebook-king-data-brokers/

[233] *Datacoup - Reclaim your personal data:* [online]. [cit. 2017-05-06]. Dostupné z: https://datacoup.com/docs#connecting-data

[234] SIMONITE, Tom. *Sell Your Personal Data for $8 a Month: Would you let a startup track your social media accounts and credit-card transactions in exchange for cash?* [online]. MIT Technology Review [cit. 2017-05-06]. Dostupné z: https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/

Dnes již standardním modelem je poskytování internetové služby zákazníkům výměnou za jejich osobní informace. Nejznámějším příkladem je společnost Alphabet provozující služby Google, která kromě v současnosti pravděpodobně nejlepšího vyhledávání na internetu nabízí *zdarma* i řadu dalších kvalitních služeb, například email, cloudové úložiště, online kalendář, překladač nebo mapy. Tyto služby jsou taktéž pokládány za vysoce kvalitní a zdatně konkurují placeným alternativám. Mnohdy jsou to právě služby Google, jež určují trend dalšího vývoje nových médií. Bez jakýchkoliv poplatků jsou tyto služby dostupné lidem téměř na celé planetě. Jediným přispěním uživatelů je poskytování rozličných dat, včetně těch, která spadají do kategorie osobní údaje. Google umí tyto informace zpracovat a komerčně velmi úspěšně nabídnout dalším společnostem. I přesto, že za služby uživatelé nic neplatí, patří společnost Alphabet mezi světově nejúspěšnější společnosti.[235] Je proto nepopiratelné, že údaje uživatelů mají v současné digitální ekonomice vysokou hodnotu.[236]
V porovnání s výše uvedeným modelem nenabízejí data brokers subjektům údajů žádnou protislužbu nebo výhodu.

I přes možnost odměňování pomocí společnosti DataCoup, neexistuje v současnosti obecně přijímaná metoda určení hodnoty osobních údajů. Data traders však své služby poskytují komerčně, obdobně jako komoditu, je tedy jisté, že nějaké metody oceňování osobních údajů používají. Domnívám se proto, že v příštích letech se bude stále častěji mluvit o hodnotě našich osobních údajů a dost možná získáme možnost tuto hodnotu získávat i pro sebe.

Předpokládám také, že i v zemích mimo EU bude docházet ke spravedlivějšímu rozdělení pozic mezi komerčními zpracovateli osobních údajů a lidmi, jejichž osobní údaje jsou používány. Nemusí se přímo jednat o služby typu DataCoup, vyplácející

[235] *Global 500 - Fortune:* [online]. [cit. 2017-05-06]. Dostupné z: http://fortune.com/global500/2015/

[236] Magazín The Economist označil data (tedy nejen osobní údaje) za nejcennější komoditu současnosti. Dříve byla touto komoditou ropa. Citováno z: Autor neuveden. *Regulating the internet giants: The world's most valuable resource is no longer oil, but data | The Economist:* [online]. The Economist Newspaper Limited, vyd. Vyd. 2017-05-06 [cit. 2017-05-16]. Dostupné z: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

přímé odměny za poskytnutá data, ale alespoň k většímu rozkvětu služeb, ze kterých by lidé měli přímý užitek. Zdá se, že i na internetu se začíná prosazovat zásada transparentnosti zpracování údajů, díky níž by mohli i občané mimo EU získat opravdovou kontrolu nad svými osobními informacemi.

Závěr

V práci je představena jedna z externalit nových médií, totiž trh s osobními údaji. S rozvojem v oblasti online médií došlo ke změně chování uživatelů internetu, někdy označované také jako přechod z Webu 1.0 k Webu 2.0. Tento pojem označuje dobu, kdy uživatel internetu není již jen konzument obsahu provozovatele internetových stránek, ale stává se také autorem mediálních obsahů. Tím dochází k silnější expozici fyzických osob na internetu, především na sociálních sítích, a také k zanechávání čím dál tím většího množství digitálních stop, které lze přiřadit ke konkrétní fyzické osobě. V dnešní digitální ekonomice je velmi obtížné vyhnout se zanechávaní digitálních stop, a to i pro osoby, které nejsou aktivní na sociálních sítích, protože současné technologie automaticky zaznamenávají o lidech množství dat. Vzniká tak velké množství informací, která jsou ukládány a mohou být dále použity pro rozličné účely. Současná doba se proto někdy označuje jako doba big data. Existuje tisíce praktických a pro lidstvo přínosných použití big data, jednou ze stinných stránek je však hrozba pro soukromí.

Každý člověk má jinou toleranci k poodkrývání svého soukromí. Ačkoliv někteří tvrdí, že je ochrana osobních údajů v online prostředí nezajímá nebo jim nepřijde důležitá, jelikož na internetu nedělají nic špatného, lze si jen těžko představit, že by duševně zdravé osobě v reálném světě nevadilo dlouhodobé sledování a analyzování svých osobních údajů v takovém měřítku, v jakém to provádějí data brokers v online prostředí. Vzhledem k faktu, že ve vyspělých státech člověk požívá internet jak pro soukromý, tak pracovní život několik hodin denně, má toto médium unikátní postavení pro současnou společnost. Zároveň však umožňuje zásah i do těch nejsoukromějších oblastí člověka.

Kromě zásahu do soukromí, tedy jedné ze základních lidských potřeb, existují i další rizika spojená s činností data brokers. Nevhodným použitím osobních údajů může dojít k reputačnímu riziku, například když bude osoba společensky znevýhodněna kvůli utajovaným neobvyklým zájmům nebo chování, které není úplně v souladu se společenskými normami dané společnosti. Zneužití soukromých informací může přinést

i riziko finanční, kdy na základě osobních údajů o osobě dojde ke znevýhodnění osoby, například protože patří do kategorie, o které poskytovatelé produktu a zboží vědí, že si mohou dovolit zaplatit více, jak se tomu stalo v případě prodeje letenek nebo rezervací hotelů. Dále je zdokumentována praxe pronajímatelů nemovitostí, které si kupují tzv. seznamy nevhodných nájemců (*bad-tenants lists)*, díky nimž může dojít ke znevýhodnění osob s kriminální historií nebo osob s „nevhodným“ původem a následným neuzavřením nájemní smlouvy, což vede nejen ke ztížení nalezení ubytování, ale i k jeho zdražení. Ačkoliv výše uvedené rozlišování klientů se jeví jako diskriminační a potenciálně zakázané, je velmi obtížné ho v praxi prokázat. Reputační a finanční riziko nejsou oddělené kategorie, jelikož jedno s sebou může snadno přinést i to druhé.

Na základě dostupných informací je evidentní, že ve Spojených státech je obchodování s osobními údaji rozsáhlý business v hodnotě miliard dolarů ročně, živící jen v USA tisíce společností.
Jedná se však o podnikatelskou aktivitu, jejíž existence není veřejnosti obecně známá a ani úplný rozsah zpracovávání informací není z veřejně dostupných informací patrný. Dostupné zdroje však naznačují, že existují velmi podrobné databáze obsahující profily téměř celé americké populace. Tyto profily obsahují stovky kategorií osobních údajů, přičemž některé údaje mohou být i velmi citlivé. Mezi sbíraná data patří například jméno, adresa, emailová adresa, číslo zdravotního pojištění, číslo řidičského průkazu, detailní informace o zdravotních problémech, vzhledu, původu, rodinné situaci, zaměstnání, kriminální historii nebo okruhu přátel. Data brokers dále shromažďují data o zájmech, politických a náboženských názorech, finanční situaci, aktivitě na sociálních sítích, o provedených nákupech nebo třeba o oblíbených značkách oblečení.
Jako problematické se jeví, že tato obchodní činnost probíhá bez vědomosti samotných lidí, jichž se osobní údaje týkají. Společnosti tak dosahují značných příjmů s komoditou odvozenou od lidí, kteří se bez znalosti existence této komodity logicky nebudou bránit. Osoby jsou tak postaveny do nevýhodné pozice, jelikož z aktivit data traders nemají žádný užitek.

Data brokers dokáží shromažďovat osobní informace z mnoha online i offline zdrojů. Mezi uváděné online zdroje patří především sociální sítě, veřejně dostupné rejstříky

a databáze, soudní a správní rozhodnutí, informace z cookies, data od provozovatelů e-shopů nebo z dotazníků vyplněných samotnými lidmi. Mezi uváděné offline zdroje patří informace od lékařů a prodejců léčiv nebo informace získané z věrnostních karet maloobchodníků. Samotná hranice mezi online a offline zdroji však v současné době není natolik důležitá, jelikož mnohé offline údaje lze poměrně snadno digitalizovat a zpřístupnit online. Data brokers kombinují informace z mnoha oddělených zdrojů, čímž dosáhnou přesnějších profilů osob, a tedy i hodnotnějšího produktu. Informace jsou sbírány dlouhodobě, lze tedy vypozorovat vzorce chování i důležité události v životech sledovaných osob. Jednotliví data traders si mezi sebou data vyměňují, dochází tak relativně snadno k rozrůstání databází s minimálními náklady. Z hlediska ochrany soukromí subjektů údajů však může být spojování informačních zdrojů a dlouhodobé pozorování problematické, jelikož občané si nemusí uvědomit, že informace, kterou poskytli před několika lety, může být spojena s informací, kterou poskytnou dnes, a navíc jinému zpracovateli osobních údajů.
Pomocí automatizovaných analytických nástrojů lze navíc na základě množství dat poměrně přesně predikovat i budoucí chování osob.

Data brokers nabízí své produkty širokému spektru společností, primárně pro lepší cílení potenciálních zákazníků. Pokud má společnost přesný profil zákazníků, o kterých ví, co si v minulosti zakoupili, jaké mají zájmy, či jaká je jejich finanční situace, je pro společnost snadnější nabídnout zákazníkům vhodný produkt. Kromě marketingových účelů, slouží produkty data brokers k ověřování finanční situace žadatelů o bankovní služby, k prověření potenciálních zaměstnanců, k ověření identity a pro účely předcházení podvodům a také ke hledání konkrétních osob. Mezi klienty data traders patří mimo jiné i známé společnosti z žebříčku Fortune 100.

Ačkoliv existují i legitimní možnosti použití osobních údajů, chybějící veřejná regulace a transparentnost data traders v USA vyvolává otázky o legitimním použití osobních údajů.

Na základě provedené analýzy se však nezdá, že je tato činnost v USA nelegální. Ačkoliv to může být pro evropského čtenáře překvapivé, v USA neexistuje legislativa, která by uceleně regulovala data brokers nebo ochranu osobních údajů ve vztahu

k soukromým společnostem. Federální zákon Privacy Act of 1974 reguluje pouze zpracování osobních údajů státními úřady. Existuje však množství zákonů vydaných jednotlivými státy a v některých případech i federálním zákonodárným sborem regulující některé aspekty ochrany osobních údajů a obchodních aktivit společností obchodujícím s osobními daty. Jedná se například zákon regulující použití osobních údajů při použití tzv. úvěrového reportu při sjednávání půjček, zákon regulující poskytování některých zdravotních dat pacientů, zákon o ochraně spotřebitele v transakcích s podnikateli nebo zákony zakazující diskriminaci. Tento systém je v odborné literatuře označován jako záplatový systém (*patchwork system*). V USA je ústavou silně chráněná svoboda slova a projevu, a to i na úkor ochrany soukromí, což v souvislosti s data brokers potvrdil i Nejvyšší soud, když judikoval, že v zásadě nelze omezovat předávání či prodej informací, a to na základě Prvního dodatku americké ústavy chránící svobodu projevu.

Ani použité odborné články a stanoviska veřejných orgánů neobsahují názor, že by američtí data brokers porušovali platné zákony. Tyto zdroje však také neobsahují informaci zda, a případně v jakém rozsahu, musí data traders reportovat svoji činnost dozorovým orgánům nebo zda existuje efektivní správní kontrola tohoto odvětví. Federal Trade Commission sama přiznává, že tyto společnosti provozují činnost skrytě před zraky spotřebitelů a údaje, které si FTC vyžádala, byly poskytnuty na základě dobrovolného rozhodnutí společností. Je proto, podle mého názoru, problematické kategoricky tvrdit, že veškerá použití osobních údajů je v souladu s právem, pokud chybí kontrolní mechanismus. Zákony zakazující diskriminaci poskytují možnost poškozené straně bránit se civilní žalobou u soudu proti zásahu do svých práv. V případě sporu s data brokers by mohlo být však velmi problematické prokázat, že došlo k diskriminaci na základě zpracovaných osobních údajů, když samotný rozsah zpracování není osobám znám.

Odlišný přístup k ochraně osobních údaj je jasně patrný v Kanadě, kde je regulace podobná té evropské, jelikož zde existuje zákon chránící soukromí kanadských občanů, což podle dostupných informací znemožnilo aktivitu amerických data brokers na území Kanady a ve vztahu k jejím obyvatelům.

Ochrana osobních údajů je v EU, v porovnání s USA, naprosto odlišná, což pravděpodobně reflektuje i odlišné historické okolnosti ve Spojených státech a Evropě.[237]

Ochrana soukromí je pro státy Evropské Unii zakotvena v Listině základních práv Evropské unie, tedy považuje jej za základní lidské právo, které může být omezeno jen ve výjimečných případech. Již samotná evropská definice osobního údaje je značně expanzivní a mimo běžně chápané osobní údaje zahrnuje i různé síťové identifikátory nebo kódy, které mohou přispět k identifikaci konkrétní osoby. Osobní údaje mají i podkategorii, tzv. *zvláštní kategorii údajů*, které se někdy označují jako *citlivé údaje,* jejichž zpracování je v zásadě zapovězeno.
Obdobně jako v Kanadě, také v EU platí, že i v případě, že jsou osobní údaje veřejně dostupné, je nutné poskytnout jim zákonnou ochranu.

Regulace ochrany osobních údajů projde v EU v roce 2018 reformou, nicméně na základě analýzy současné směrnice řešící ochranu osobních údajů se jeví činnost data brokers v americkém rozsahu zaměřená na občany EU nebo prováděná společnostmi na území EU jako nepravděpodobná nebo nelegální. Budoucí regulace, nařízení GDPR, poskytuje fyzickým osobám ochranu ještě lepší.

Současná směrnice o ochraně osobních údajů byla transponována zákonodárnými orgány jednotlivých členských států do národních právních řádů. Mezi členskými státy se mohou vyskytovat odlišnosti, jelikož směrnice v některých ustanoveních umožnila jistou diskreci států. Z tohoto důvodů se liší například výše správní sankce v různých členských státech. Většina pravidel je však ve státech EU totožná.
Pro jakékoliv zpracování osobních údajů je nutné splnit alespoň jeden z důvodů zpracování, přičemž pro činnost data brokers je v praxi použitelný pravděpodobně

[237] Existuje domněnka, že mnohem přísnější ochrana osobních údajů na evropském kontinentě úzce souvisí s negativními následky uchovávání osobních informací během druhé světové války a v době komunistických režimů, což mnohdy vedlo k perzekucím sledovaných osob. V USA tuto zkušenost nemají, a není proto tak silný tlak na ochranu osobních údajů, který by donutil zákonodárce podle toho jednat. Např. v FREUDE, Alvar, FREUDE Trixy. *Echos of History* [online]. [cit. 2017-05-07]. Dostupné z: http://www.bfna.org/publication/newpolitik/echos-of-history-understanding-german-data-protection

pouze jeden důvod, totiž získání souhlasu osoby, jejíž údaje mají být zpracovávány. Platný souhlas musí splňovat relativně přísná měřítka, jelikož musí být svobodný, výslovný, vědomý a nezpochybnitelný.
Zpracování musí také probíhat v souladu se zásadami, které samotné se jeví jako dostatečné pro znemožnění činnosti data brokers v EU, jelikož zpracování musí být jen pro stanovené účely, legitimní, přiměřené a jen po omezenou dobu, což je, podle mého názoru, v rozporu s popsanou praxí v USA.
Na rozdíl od USA, má každý členský stát EU také specializovaný správní orgán chránící osobní údaje, který také může, v případě porušení norem, udělit správní sankci. Tomuto úřadu musí správce údajů před započetím zpracovávání oznámit svůj záměr. Existuje zde tedy poměrně efektivní možnost kontroly a v krajním případě i sankční intervence veřejného orgánu.

Všechny tyto okolnosti směřují k závěru, že data brokers v EU mají značně omezené možnosti pro svoji aktivitu. V rozsahu, jaký je provozován na území USA, by byl považován za ilegální. Na základě současné regulace si lze představit jejich činnost omezenou na poskytování agregovaných dat, tedy bez možnosti rozlišit jednotlivé fyzické osoby. Pro získání těchto dat, by však i přesto data brokers musely získat souhlas konkrétní osoby, která by v agregovaných datech figurovala, nebo jiný právní důvod pro zpracování jejích údajů.

Z veřejně dostupných zdrojů, ani na základě několika rozhovorů s osobami zasvěcenými do marketingových praktik známých společností fungujících v ČR se mi nepodařilo v evropském měřítku identifikovat data brokers, tak jak jsou popsaní v americkém kontextu. Domnívám se proto, že je nepravděpodobné, že by ve členských státech docházelo k obchodování s velmi přesnými profily jednotlivých občanů v masovém měřítku.

Od 25. května 2018 vstupuje v účinnost nové nařízení GDPR, které ještě více zdůrazňuje právo osob na ochranu jejich osobních informací. Navíc klade na subjekty zpracovávající údaje přísnější nároky. Patrně nejdůležitější novinkou bude změna druhu normy, jelikož budoucí norma je nařízením, které platí na území států bez nutnosti transpozice do národních právních řádů. Z tohoto důvodu bude stejný text na celém

území EU. Druhou podstatnou změnou je výše sankce za porušení GDPR, jelikož bude sankce v EU sjednocena, s maximální výší 20 miliónů euro nebo 4 % celosvětového ročního obratu podniku, podle toho, která částka je vyšší. Tato sankce je natolik vysoká, že lze pochybovat, že by některá ze společností podnikající na území EU riskovala takto materiální sankci pro použití osobních údajů, které byly zpracovány v rozporu s nařízením. Domnívám se proto, že i pokud by v současnosti existoval ve větším měřítku v EU utajovaný trh s osobními údaji, bude mít GDPR odstrašující účinek i pro klienty data brokers, v důsledku čehož by došlo k zániku tohoto trhu. Další novinkou pro společnosti obchodující s osobními údaji bude povinnost zřídit pozici pověřence pro ochranu osobních údajů (*data protection officer*), který bude kontaktním bodem mezi danou společností a národním úřadem na ochranu osobních údajů.

Nové nařízení bude dopadat i na subjekty ze států mimo Evropskou unii, pokud se jejich činnost týká monitorování osob přítomných v EU. Tímto může dojít k rozšíření dosahu evropského nařízení i mimo Evropu. Zůstává však otázka, jak bude případné porušení nařízení společnostmi usazenými mimo EU vymáháno.

S dalším technologickým pokrokem je pravděpodobné, že bude pokračovat i evoluce chápání osobních údajů. V budoucnu by se mohla ochrana vztahovat například na situace, kdy informace nebude přiřaditelná ke konkrétní osobě, ale například pouze ke konkrétnímu mobilnímu telefonu nebo jinému zařízení.

Další z možných budoucích cest vývoje businessu data brokers v USA je vznik samoregulačního subjektu, jehož členové by dobrovolně garantovali alespoň nějaký standard ochrany soukromí fyzických osob. V současné době sice existuje několik samoregulačních organizací, ale zaměřují se spíše na různé elementy digitálního marketingu, komplexněji zaměřený subjekt neexistuje. V EU tato samoregulace není, vzhledem k dostatečné přísné veřejné regulaci, nutná.

Stále sílícím trendem je snaha evropských legislativců a některých zpracovatelů osobních údajů minimalizovat rozsah zpracovávaných osobních údajů, tedy trend poskytovat digitální služby i bez znalosti kdo je klientem. V případě, že nelze již při

samotném poskytování služeb minimalizovat rozsah, jeví se budoucí praxí anonymizace nebo co nejdřívější vymazání získaných údajů.

Big data je big business. Z komerčního využití osobních údajů nyní občané většinou nic nemají. Existují však platformy, které přímo i nepřímo fyzické osoby za poskytování osobních údajů odměňují. Lze však pochybovat o spravedlivě rozdělených pozicích ve vztahu k data traders. Doufám, že jednoho dne bude hodnota soukromí brána dostatečně vážně.

Další výzkum navazující na tuto práci by se mohl zabývat připravovaným evropským nařízením ePrivacy, které je nyní v pokročilé fázi legislativního procesu. Vztah tohoto nařízení a na řízení GDPR není ještě zcela jasný, nicméně se bude zabývat tématy obsaženými v této práci.
Práce se zcela záměrně nezabývá přeshraniční výměnou osobních údajů mezi veřejnými orgány Evropské unie a jiných států. Toto téma v nedávné minulosti, i vzhledem k zásadnímu rozhodnutí SDEU, získalo pozornost i mimo odborné kruhy. Pro pochopení všech rozměrů transferu osobních informací by však bylo zajímavé také analyzovat současnou teoretickou i praktickou stránku tohoto zpřístupňování osobních údajů.
Z použitých zdrojů vyplývá, že data brokers v současnosti čerpají informace primárně ze strukturovaných dat. Technologický pokrok však umožňuje stále kvalitnější analýzu nestrukturovaných dat, například emailů, příspěvků na sociálních sítích nebo obrázků. Podle dostupných informací je právě komerční data mining nestrukturovaných dat v počátcích, nicméně je evidentní, že se jedná o budoucí trend digitální ekonomiky.

Summary

In today's digital economy our personal data may be treated as valuable commodity even without our knowledge. In the USA, there are thousands of companies secretly processing personal information of millions of American citizens. By using sophisticated automated software tools they search for data from numerous sources including social media, web cookies, various public databases, retail transactions, loyalty cards and many more. Data collection is being done continuously over years on a large scale. Personal information databases are merged together which allows data brokers to create extremely descriptive profiles containing information about health conditions, financial and family status, interests, political preferences, racial or criminal background.

The goals of the thesis are to present this little-known business and to cast light on the data brokers outside of the US. For this reason, the thesis contains an analysis of the data brokers legislation in the US, Canada and the European Union. The thesis also includes an outline of trends relating to commercial use of personal data and explanation of risks related to personal information processing in our digital economy. The lack of digital privacy may lead to reputational and financial risk, as demonstrated on real events.

The US regulation consists of a number of topic-related laws which stipulate personal data trading inconsistently, also known as the *patchwork system*. However, the above described practice of data brokers seems compliant with current legislation.
On the other hand, in Canada and the EU there is a regulation protecting privacy against both private and public subjects. These laws empower citizens with a right to decide whether and how their personal data may be used.

Notable is a different attitude of the US and European society, as there is a preference of the freedom of speech and the right to information access notion over the right to privacy in the US. On the other hand, in the EU the protection of citizens' privacy is strongly preferred. The current EU directive on personal data protection is strict enough

to make data broker industry in member states practically illegal. Moreover, on April 25, 2018 a new EU privacy regulation enters into force, which is considered to be another privacy rights milestone. In the EU the following principles of personal data processing have to be followed: fairness, transparency, adequacy or legality. The EU regulation, as well as the European Court of Justice, provides the Europeans with the right to be forgotten and right to access/edit their own personal data; rights not present in the US legal system.

In conclusion, it seems very unlikely that the data trading industry is present in the EU states or Canada.

For this thesis, mainly literature in the English language was used. The key source for this work was the report of the US Federal Trade Commission on data broker market; this report is the most comprehensive publicly available information source on data traders. The other bibliography I used consists mostly of peer-reviewed articles, standpoints of state authorities and laws of the EU, the US, the Czech Republic, Canada, Germany and the UK.

Bibliografie

Právní normy

- *BDSG - Bundesdatenschutzgesetz [online]*. [cit. 2017-01-26]. Dostupné z: https://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html
- *Data Protection Act 1998* [online]. [cit. 2017-01-26]. Dostupné z: http://www.legislation.gov.uk/ukpga/1998/29/section/55C
- Charter of Fundamental Rights of the European Union [online]. [cit. 2016-07-12]. Dostupné z: http://www.europarl.europa.eu/charter/pdf/text_en.pdf
- Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), účinný ke dni 2015-06-23 [online]. [cit. 2016-08-29]. Dostupné z: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
- Privacy Act of 1974, 5 U.S.Code § 552a [online]. [cit. 2017-01-26]. Dostupné z: https://www.gpo.gov/fdsys/pkg/CPRT-110HPRT38035/pdf/CPRT-110HPRT38035.pdf
- Směrnice Evropského parlamentu a Rady 2012/29/EU, kterou se zavádí minimální pravidla pro práva, podporu a ochranu obětí trestného činu a kterou se nahrazuje rámcové rozhodnutí Rady 2001/220/SVV. In: *EUR-Lex* [právní informační systém]. [cit. 2016-06-26]
- 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: *EUR-Lex* [právní informační systém]. [cit. 2016-06-26]
- Smlouva o fungování Evropské unie (konsolidované znění). In: *EUR-Lex* [právní informační systém]. [cit. 2016-06-26]
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v aktuálním znění. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [cit. 2016-06-26]
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů v aktuálním znění. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [cit. 2016-06-26]
- Zákon č. 2/1993 Sb., Listina základních práv a svobod, v aktuálním znění. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [cit. 2016-06-26]

- Zákon č. 89/2012 Sb., občanský zákoník v aktuálním znění.
- Zákon č. 89/2012 Sb., občanský zákoník v aktuálním znění. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [cit. 2016-06-26]

Použitá literatura

- *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes: STAFF REPORT FOR CHAIRMAN ROCKEFELLER* [online]. 2013. 42 s. [cit. 2016-07-18]. Dostupné z: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- *About - European Data Protection Supervisor [online]*. [cit. 2017-05-08]. Dostupné z: https://edps.europa.eu/about-edps_en
- ACAR, Gunes; et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild* [online]. 2015 [cit. 2016-08-15]. Dostupné z: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf.
- ALTMAN, Russ. What really happens when you mix medications? *TED.com* [online]. [cit. 2017-03-07]. Dostupné z: https://www.ted.com/talks/russ_altman_what_really_happens_when_you_mix_medications
- ANDERSON, Martin. Sites that block adblockers seem to be suffering. *The Stack* [online]. Vyd. 2016-04-21 [cit. 2016-08-25]. Dostupné z: https://thestack.com/world/2016/04/21/sites-that-block-adblockers-seem-to-be-suffering/
- Autor neuveden. *Big data, artificial intelligence, machine learning and data protection* [online]. Information Commissioner's Office, 2014 [cit. 2017-03-07]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
- Autor neuveden. *Regulating the internet giants: The world's most valuable resource is no longer oil, but data | The Economist:* [online]. The Economist Newspaper Limited, vyd. 2017-05-06 [cit. 2017-05-16]. Dostupné z:

http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

- BARNARD, Catherine a Steve PEERS. *European Union law*. 1. Oxford: Oxford University Press, 2014. 928 s. ISBN 9780199686117
- *Big data - definition of big data in English | Oxford Dictionaries* [online]. [cit. 2017-03-05]. Dostupné z: https://en.oxforddictionaries.com/definition/big_data
- *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* [online]. Executive Office of the President, 2014 [cit. 2016-08-23]. 85 s. Dostupné z: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf
- BIGNAMI, Francesca. *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* [online]. Brussels: European Union, 2015 [cit. 2017-04-27]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf
- BOYD, Danah a Kate CRAWFORD. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication, & Society* [online]. 15(5), 662-679 [cit. 2017-03-06]. Dostupné z: www.danah.org/papers/2012/BigData-ICS-Draft.pdf
- BREGGIN, Linda a Judith AMSALEM. Big Data and Environmental Protection: An Initial Survey of Public and Private Initiatives. *ELI* [online]. Washington, 2014, 1-32 [cit. 2017-03-07]. Dostupné z: https://www.eli.org/sites/default/files/eli-pubs/big-data-and-environmental-protection.pdf
- BROOKMAN, Justin. *What is Cross-Device Tracking?* [online]. In: FTC - Office of Technology Research and Investigation, 2015 [cit. 2016-08-25]. Dostupné z: https://www.ftc.gov/system/files/documents/public_events/630761/cross-device_tracking_workshop_deck.pptx
- CALABRESE, Chris; et al. *Comments for November 2015 Workshop on Cross - Device Tracking*. *Microsoft Word - FTC Cross-Device Draft v14.docx - 10.16.15-CDT-Cross-Device-Comments.pdf [online]*. 2015 [cit. 2016-08-25]. 11

s. Dostupné z: https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf

- *Cookies - Information that websites store on your computer | Firefox Help [online]*. [cit. 2016-08-15]. Dostupné z: https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer#w_what-is-a-cookie
- *CURIA - Dokumenty: Rozsudek SDEU č.* C-131/12 *ze dne 13. května 2014, ve věci Google Spain SL,Google Inc. Proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [online]. [cit. 2017-04-15]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=118910
- *CURIA - Dokumenty: Rozsudek SDEU č. C-582/14 ze dne 19. října 2016, ve věci Patrick Breyer proti Bundesrepublik Deutschland* [online]. [cit. 2017-04-15]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945
- ČAK - Vyhledávání advokátů a koncipientů [online]. [cit. 2016-11-25]. Dostupné z: http://vyhledavac.cak.cz/Units/_Search/search.aspx
- *Časté otázky týkající se pravomocí EU a Evropské komise – Evropská občanská iniciativa - Evropská komise [online]*. [cit. 2016-07-11]. Dostupné z: http://ec.europa.eu/citizens-initiative/public/competences/faq?lg=cs#q1
- ČLK > / Pro veřejnost / Seznam lékařů [online]. [cit. 2016-11-25]. Dostupné z: http://www.lkcr.cz/seznam-lekaru-426.html
- ČÚZK - Výstupy z KN poskytované prostřednictvím DP [online]. [cit. 2016-11-25]. Dostupné z: http://www.cuzk.cz/Katastr-nemovitosti/Poskytovani-udaju-z-KN/Dalkovy-pristup/Vystupy-z-KN-poskytovane-prostrednictvim-DP.aspx
- *Data Brokers: A Look at the Canadian and American Landscape Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada* [online]. 2014. [cit. 2016-08-19]. 13 s. Dostupné z: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf
- *Data mining techniques [online]*. [cit. 2016-11-25]. Dostupné z: https://www.ibm.com/developerworks/library/ba-data-mining-techniques

- *Datacoup - Reclaim your personal data [online]*. [cit. 2017-05-06]. Dostupné z: https://datacoup.com/docs#connecting-data
- *DeleteMe - Protect Your Personal Data And Reputation Online* [online]. [cit. 2017-04-09]. Dostupné z: https://abine.com/deleteme/landing.php
- Dlužníci - VZP ČR [online]. [cit. 2016-11-25]. Dostupné z: https://www.vzp.cz/platci/dluznici
- DUHIGG, Charles. *The power of habit: why we do what we do in life and business*. New York: Random House, 2012. 353 s. ISBN 978-1-4000-6928-6.
- DUTCHER, Jennifer. *What Is Big Data? - Blog [online]*. Vyd. 2014-09-03 [cit. 2017-03-05]. Dostupné z: https://datascience.berkeley.edu/what-is-big-data/
- EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability* [online]. Federal Trade Commission, 2014. 110 s. [cit. 2016-08-26]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
- Eli Pariser: Beware online "filter bubbles“. *TED.com: TED Talk* [online]. 2011 [cit. 2016-08-15]. Dostupné z: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en
- *EUR-Lex - l14534 - EN - EUR-Lex: Prameny práva Evropské unie* [online]. [cit. 2017-02-07]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=URISERV:l14534
- Formulář pro lustraci - ISIR - Insolvenční rejstřík (U1.0.0.20A) [online]. [cit. 2016-11-25]. Dostupné z: https://isir.justice.cz/isir/common/index.do
- FREUDE, Alvar, FREUDE Trixy. *Echos of History* [online]. [cit. 2017-05-07]. Dostupné z: http://www.bfna.org/publication/newpolitik/echos-of-history-understanding-german-data-protection
- FUCHS, Christian, Anders ALBRECHTSLUND a Marisol SANDOVAL, ed. *Internet and surveillance: the challenges of Web 2.0 and social media*. Abingdon, Oxon: Routledge, 2012. Routledge studies in science, technology and society, 16. 332 s. ISBN 978-0-415-89160-8
- *Global 500 - Fortune [online]*. [cit. 2017-05-06]. Dostupné z: http://fortune.com/global500/2015/

- HA, Anthony. *SilverPush Says It's Using "Audio Beacons" For An Unusual Approach To Cross-Device Ad Targeting* [online]. TechCrunch, vyd. 2014-07-24 [cit. 2016-08-26]. Dostupné z: https://techcrunch.com/2014/07/24/silverpush-audio-beacons/
- *Ico-guidance-on-monetary-penalties.pdf* [online]. 36 s. [cit. 2017-01-26]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf.
- JENSEN, Klaus, ed. *A handbook of media and communication research: qualitative and quantitative methodologies*. Oxon: Routledge, 2012. 448 s. ISBN 978-0-415-60965-4.
- *JOLLY, Ieuan. Data protection in the United States: overview | Practical Law [online]. [cit. 2017-04-15]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/6-502-0467?__lrTS=20170415143511897&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1*
- KROFT, Steve. *The Data Brokers: Selling your personal information* [online]. Vyd. 2014-08-24 [cit. 2016-08-26]. Dostupné z: http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/
- KST ČR - Komora soudních tlumočníků [online]. [cit. 2016-11-25]. Dostupné z: http://www.kstcr.cz/cz
- KUEMPEL, Ashley. The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* [online]. 2016, **36**(1), 207-234 [cit. 2016-07-22]. Dostupné z: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1795&context=njilb
- MANOVICH, Lev. *The language of new media*. [online]. MIT Press, 2001. 68 s. [cit. 2017-03-06]. Dostupné z: http://faculty.georgetown.edu/irvinem/theory/Manovich-LangNewMedia-excerpt.pdf
- *Master List of Data Broker Opt-Out Links* - [online]. Winston Law Firm, LLC., 2015 [cit. 2016-08-29]. Dostupné z: http://www.stopdatamining.me/opt-out-list/

- MITHAL, Maneesha. Vzor dopisu odeslaný výrobcům aplikací obsahující SilverPush. *160317samplesilverpushltr.pdf [online]*. FTC - Bureau of Consumer Protection, 2016 [cit. 2016-08-25]. Dostupné z: https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-silverpush-code/160317samplesilverpushltr.pdf
- Nahlížení do katastru nemovitostí | Nahlížení do katastru nemovitostí [online]. [cit. 2016-11-25]. Dostupné z: http://nahlizenidokn.cuzk.cz/
- O'REILLY, Tim. *What Is Web 2.0 - O'Reilly Media [online]*. O'Reilly Media, 2005 [cit. 2017-03-06]. Dostupné z: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html
- OTTO, Paul; ANTÓN Annie; BAUMER David. The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information. *North Carolina State University Technical Report* [online]. 2006, str. 1-13 [cit. 2017-04-09]. Dostupné z: https://pdfs.semanticscholar.org/4368/5dba37726d66a071d7844f9ab0b9057180bd.pdf
- *Personal data protection | EU fact sheets | European Parliament [online]*. [cit. 2016-07-12]. Dostupné z: http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.12.8.html
- PLESSER, Ronald a Emilio CIVIDANES. *COMMENTS OF THE INDIVIDUAL REFERENCE SERVICES GROUP ON ELEMENTS OF EFFECTIVE SELF REGULATION FOR THE PROTECTION OF PRIVACY AND QUESTIONS RELATED TO ONLINE PRIVACY* [online]. 1998 [cit. 2016-08-26]. Dostupné z: https://www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/irsgcom.html
- *Portál evropské e-Justice - Právo EU* [online]. [cit. 2016-07-12]. Dostupné z: https://e-justice.europa.eu/content_eu_law-3-cs.do
- POVEJŠIL, Tomáš. *Právní regulace dostupnosti digitálního obsahu mladistvým*. Brno, 2014. Diplomová práce. Masarykova univerzita. Vedoucí práce Radim Polčák.
- Prehled soudcu [online]. [cit. 2016-11-25]. Dostupné z: http://portal.justice.cz/Justice2/Soudci/soudci.html#002

- *PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION on What Information Do Data Brokers Have On Consumers, And How Do They Use It* [online]. Washington, D.C., 2013 [cit. 2016-08-26]. 10 s. Dostupné z: https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf
- *Prohlášení společnosti Microsoft o zásadách ochrany osobních údajů – Microsoft a ochrana osobních údajů:* Verze Leden 2016 [online]. [cit. 2017-02-10]. Dostupné z: https://privacy.microsoft.com/cs-cz/privacystatement?PrintView=true
- *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* [online]. FTC, 2012. upraveno 2012-3-16 [cit. 2016-08-19]. 112 s. Dostupné z: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
- RAMIREZ, Edith. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues: FTC Report* [online]. 2016. 50 s. [cit. 2017-04-14]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
- *Reform of EU data protection rules - European Commission* [online]. [cit. 2016-06-30]. Dostupné z: http://ec.europa.eu/justice/data-protection/reform/index_en.htm
- Rejstříky a registry - statnisprava.cz [online]. [cit. 2016-11-25]. Dostupné z: https://www.statnisprava.cz/rstsp/redakce.nsf/i/rejstriky
- SANBURN, Josh. *Delta Appeared to Overcharge Frequent Flyers for Weeks – Was That Legal?*. Time Inc. [online]. Vyd. 2012-05-21 [cit. 2017-04-08]. Dostupné z: http://business.time.com/2012/05/21/delta-overcharged-frequent-flyers-for-weeks-was-that-legal/
- Seznam daňových poradců - Komora daňových poradců ČR [online]. [cit. 2016-11-25]. Dostupné z: https://www.kdpcr.cz/seznam-danovych-poradcu?from=1370

- Seznam insolvenčních správců - přehled [online]. [cit. 2016-11-25]. Dostupné z: https://isir.justice.cz/InsSpravci/public/seznamFiltr.do
- Seznam notářů [online]. [cit. 2016-11-25]. Dostupné z: https://www.nkcr.cz/seznam-notaru
- *Shrnutí stanoviska č. 4/2015 evropského inspektora ochrany údajů, „Směrem k nové digitální etice: Data, důstojnost a technologie" (2015/C 392/08)* [online]. 2015 [cit. 2017-05-08]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=uriserv:OJ.C_.2015.392.01.0009.01.CES
- SIMON, Phil. Facebook: The New King of Data Brokers? In: *Wired.com* [online]. [cit. 2016-06-30]. Dostupné z: http://www.wired.com/insights/2014/10/facebook-king-data-brokers/
- SIMONITE, Tom. *Sell Your Personal Data for $8 a Month: Would you let a startup track your social media accounts and credit-card transactions in exchange for cash?* [online]. MIT Technology Review [cit. 2017-05-06]. Dostupné z: https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/
- *Správci osobních údajů: zaregistrovaná zpracování [online]*. [cit. 2017-01-26]. Dostupné z: https://forms.uoou.cz/registration.aspx?id=191313
- *Substantially Similar Legislation - Legal information related to PIPEDA* [online]. 2013 [cit. 2016-08-29]. Dostupné z: https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp
- TALEB, Nassim Nicholas. *The black swan: the impact of the highly improbable*. New York: Random House, 2007. 366 s. ISBN 978-140-0063-512.
- TANNER, Adam. *How Data Brokers Make Money Off Your Medical Records: Data brokers legally buy, sell and trade health information, but the practice risks undermining public confidence.* Scientific American [online]. Scientific American, a Division of Nature America, vyd. 2016-02-01 [cit. 2017-04-17]. Dostupné z: https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/
- *Tor Project: Overview [online]*. [cit. 2017-02-07]. Dostupné z: https://www.torproject.org/about/overview.html.en

- ULANOFF, Lance. *Tim Cook blasts Silicon Valley companies for 'gobbling up' your personal data [online]*. Vyd. 2016-06-03 [cit. 2017-05-13]. Dostupné z: http://mashable.com/2015/06/02/tim-cook-privacy/#M.Yx7bidfuqN
- VALENTINO-DEVRIES, Jennifer; et al. Websites Vary Prices, Deals Based on Users' Information. *The Wall Street Journal* [online]. Vyd. 2012-12-24 [cit. 2016-08-23]. Dostupné z: http://www.wsj.com/news/articles/SB10001424127887323777204578189391813881534
- Veřejný rejstřík a Sbírka listin - Ministerstvo spravedlnosti České republiky [online]. [cit. 2016-11-25]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik
- *Výroční zpráva společnosti QuintilesIMS* 2016 [online]. [cit. 2017-04-17]. Dostupné z: http://s21.q4cdn.com/395013450/files/doc_financials/2016/QuintilesIMS_2016_Annual-Report_Final-%281%29.pdf
- WHITE, Martha. *Orbitz Shows Higher Prices to Mac Users*. Time Inc. [online]. Vyd. 2012-06-26 [cit. 2017-04-08]. Dostupné z: http://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/?iid=pf-main-mostpop1/

Seznam příloh

Příloha č. 1: Ilustrativní seznam osobních údajů, které mají data brokers k dispozici (seznam)

Přílohy

Příloha č. 1: Ilustrativní seznam osobních údajů, které mají data brokers k dispozici (seznam)

Převzato z:
EDITH, Ramirez; et al. *DATA BROKERS: A Call for Transparency and Accountability*. str. 97-100

Identifying Data

- Name
- Previously Used Names
- Address
- Address History
- Longitude and Latitude
- Phone Numbers
- Email Address

Sensitive Identifying Data

- Social Security Number
- Driver's License Number
- Birth Date
- Birth Dates of Each Child in Household
- Birth Date of Family Members in Household

Demographic Data

- Age
- Height
- Weight
- Gender
- Race & Ethnicity
- Country of Origin
- Religion (by Surname at the Household Level)
- Language
- Marital Status
- Presence of Elderly Parent
- Presence of Children in Household
- Education Level
- Occupation
- Family Ties

• Demographic Characteristics of Family
Members in Household
• Number of Surnames in Household
• Veteran in Household
• Grandparent in House
• Spanish Speaker
• Foreign Language Household (e.g., Russian,
Hindi, Tagalog, Cantonese)
• Households with a Householder who is
Hispanic Origin or Latino
• Employed - White Collar Occupation
• Employed - Blue Collar Occupation
• Work at Home Flag
• Length of Residence
• Household Size
• Congressional District
• Single Parent with Children
• Ethnic and Religious Affiliations

Court and Public Record Data

• Bankruptcies
• Criminal Offenses and Convictions
• Judgments
• Liens
• Marriage Licenses
• State Licenses and Registrations (e.g., Hunting, Fishing, Professional)
• Voting Registration and Party Identification

Social Media and Technology Data

• Electronics Purchases
• Friend Connections
• Internet Connection Type
• Internet Provider
• Level of Usage
• Heavy Facebook User
• Heavy Twitter User
• Twitter User with 250+ Friends
• Is a Member of over 5 Social Networks
• Online Influence
• Operating System
• Software Purchases
• Type of Media Posted
• Uploaded Pictures
• Use of Long Distance Calling Services
• Presence of Computer Owner
• Use of Mobile Devices
• Social Media and Internet Accounts including: Digg, Facebook, Flickr, Flixster,
Friendster, hi5, Hotmail, LinkedIn, Live Journal, MySpace, Twitter, Amazon, Bebo, CafeMom, DailyMotion, Match, myYearbook, NBA.com, Pandora, Photobucket, WordPress, and Yahoo

Home and Neighborhood Data

• Census Tract Data
• Address Coded as Public/Government Housing

• Dwelling Type
• Heating and Cooling
• Home Equity
• Home Loan Amount and Interest Rate
• Home Size
• Lender Type
• Length of Residence
• Listing Price
• Market Value
• Move Date
• Neighborhood Criminal, Demographic, and Business Data
• Number of Baths
• Number of Rooms
• Number of Units
• Presence of Fireplace
• Presence of Garage
• Presence of Home Pool
• Rent Price
• Type of Owner
• Type of Roof
• Year Built

General Interest Data

• Apparel Preferences
• Attendance at Sporting Events
• Charitable Giving
• Gambling - Casinos
• Gambling - State Lotteries
• Thrifty Elders
• Life Events (e.g., Retirement, Newlywed, Expectant Parent)
• Magazine and Catalog Subscriptions
• Media Channels Used
• Participation in Outdoor Activities (e.g., Golf, Motorcycling, Skiing, Camping)
• Participation in Sweepstakes or Contests
• Pets
• Dog Owner
• Political Leanings
• Assimilation Code
• Preferred Celebrities
• Preferred Movie Genres
• Preferred Music Genres
• Reading and Listening Preferences
• Donor (e.g., Religious, Political, Health Causes)
• Financial Newsletter Subscriber
• Upscale Retail Card Holder
• Affluent Baby Boomer
• Working-Class Moms
• Working Woman
• African-American Professional
• Membership Clubs - Self-Help
• Membership Clubs - Wines
• Exercise - Sporty Living
• Winter Activity Enthusiast
• Participant - Motorcycling
• Outdoor/Hunting & Shooting
• Biker/Hell's Angels
• Santa Fe/Native American Lifestyle

• New Age/Organic Lifestyle
• Is a Member of over 5 Shopping Sites
• Media Channel Usage - Daytime TV
• Bible Lifestyle
• Leans Left
• Political Conservative
• Political Liberal
• Activism & Social Issues

Financial Data

• Ability to Afford Products
• Credit Card User
• Presence of Gold or Platinum Card
• Credit Worthiness
• Recent Mortgage Borrower
• Pennywise Mortgagee
• Financially Challenged
• Owns Stocks or Bonds
• Investment Interests
• Discretionary Income Level
• Credit Active
• Credit Relationship with Financial or Loan
Company
• Credit Relationship with Low-End Standalone Department Store
• Number of Investment Properties Owned
• Estimated Income
• Life Insurance
• Loans
• Net Worth Indicator
• Underbanked Indicator
• Tax Return Transcripts
• Type of Credit Cards

Vehicle Data

• Brand Preferences
• Insurance Renewal
• Make & Model
• Vehicles Owned
• Vehicle Identification Numbers
• Vehicle Value Index
• Propensity to Purchase a New or Used Vehicle
• Propensity to Purchase a Particular Vehicle
Type (e.g., SUV, Coupe, Sedan)
• Motor Cycle Owner (e.g., Harley, Off-Road
Trail Bike)
• Motor Cycle Purchased 0-6 Months Ago
• Boat Owner
• Purchase Date
• Purchase Information
• Intend to Purchase – Vehicle

Travel Data

• Read Books or Magazines About Travel
• Travel Purchase - Highest Price Paid
• Date of Last Travel Purchase
• Air Services - Frequent Flyer
• Vacation Property

• Vacation Type (e.g., Casino, Time Share,
Cruises, RV)
• Cruises Booked
• Preferred Vacation Destination
• Preferred Airline

Purchase Behavior Data

• Amount Spent on Goods
• Buying Activity
• Method of Payment
• Number of Orders
• Buying Channel Preference (e.g., Internet,
Mail, Phone)
• Types of Purchases
• Military Memorabilia/Weaponry
• Shooting Games
• Guns and Ammunition
• Christian Religious Products
• Jewish Holidays/Judaica Gifts
• Kwanzaa/African-Americana Gifts
• Type of Entertainment Purchased
• Type of Food Purchased
• Average Days Between Orders
• Last Online Order Date
• Last Offline Order Date
• Online Orders $500-$999.99 Range
• Offline Orders $1000+ Range
• Number of Orders - Low-Scale Catalogs
• Number of Orders - High-Scale Catalogs
• Retail Purchases - Most Frequent Category
• Mail Order Responder - Insurance
• Mailability Score
• Dollars - Apparel - Women's Plus Sizes
• Dollars - Apparel - Men's Big & Tall
• Books - Mind & Body/Self-Help
• Internet Shopper
• Novelty Elvis

Health Data

• Ailment and Prescription Online Search
Propensity
• Propensity to Order Prescriptions by Mail
• Smoker in Household
• Tobacco Usage
• Over the Counter Drug Purchases
• Geriatric Supplies
• Use of Corrective Lenses or Contacts
• Allergy Sufferer
• Have Individual Health Insurance Plan
• Buy Disability Insurance
• Buy Supplemental to Medicare/Medicaid
Individual Insurance
• Brand Name Medicine Preference
• Magazines - Health
• Weight Loss & Supplements
• Purchase History or Reported Interest in

Health Topics including: Allergies, Arthritis,
Medicine Preferences, Cholesterol, Diabetes,
Dieting, Body Shaping, Alternative Medicine, Beauty/Physical Enhancement,
Disabilities, Homeopathic Remedies,
Organic Focus, Orthopedics, and Senior Needs