UNIVERZITA KARLOVA

Právnická fakulta

Jan Kubica

Vybrané problémy technologické realizace evropské ochrany osobních údajů

Diplomová práce

Vedoucí diplomové práce: doc. Dr. iur. Harald Christian Scheu, Mag. phil., Ph.D.

Katedra: Katedra evropského práva

Datum vypracování práce (uzavření rukopisu): 29.3.2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 240 224 znaků včetně mezer.

V Praze dne _____ _____

Jan Kubica

Poděkování

Na tomto místě bych chtěl poděkovat doc. Dr. iur. Haraldovi Christianovi Scheuovi, Mag. phil., Ph.D. za odborné vedení práce a řadu cenných podnětů.
Dále bych rád poděkoval svým blízkým za podporu během studia.

Seznam zkratek:

AI	*Artificial Intelligence*, umělá inteligence
API	*Application programming interface,* rozhraní pro programování aplikací
čl.	článek
DPIA	*Data Protection Impact Assessment*, Posouzení vlivu na ochranu osobních údajů
EK	Evropská komise
EDPB	*European Data Protection Board,* Evropský sbor pro ochranu osobních údajů
ESD	Evropský soudní dvůr
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
Evropská úmluva	Úmluva o ochraně lidských práv a základních svobod
GDPR	*General Data Protection Regulation,* Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
ICO	*Information Commissioner's Office,* britský dozorový úřad
IoT	*Internet of Things,* Internet věcí
Listina	Listina základních práv Evropské unie (Charta základních práv EU)
ML	*Machine learning*, strojové učení
Nařízení	vizte *GDPR*
Obecné nařízení	vizte *GDPR*
OECD	*Organisation for Economic Co-operation and Development,* Organizace pro hospodářskou spolupráci a rozvoj

RFID	*Radio Frequency Identification,* radiofrekvenční identifikace
Sbor	vizte *EDPB*
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
Směrnice	Směrnice 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
Unie	Evropská unie
ÚOOÚ	Úřad pro ochranu osobních údajů
Úřad	vizte *ÚOOÚ*
ÚS	Ústavní soud
WP29	*Article 29 Working Party,* Pracovní skupina pro ochranu údajů zřízená podle článku 29

Obsah

1 Úvod

„Právo být nechán na pokoji je skutečným počátkem veškeré svobody.“[1]

Moderní technologie staví před právo mnohé výzvy. Jednou z největších výzev současnosti je pak nepochybně úprava ochrany osobních údajů, a to v důsledku nebývalého technologického rozvoje.[2] *Data mining*, rozmach a dostupnost internetu věcí (*Internet of Things)* a tzv. nositelné elektroniky (*wearables)*, *cloud computing, big data* a následné zpracování dat pomocí strojového učení (*machine learning)* jsou různorodé technologie či postupy, které ovšem mají jednu důležitou vlastnost společnou – přináší dosud nevídané možnosti jak získávání, tak následné analýzy osobních údajů. Netřeba dodávat, že tento rozvoj s sebou nese nejen příležitosti, ale též hrozby. Zároveň se většina Evropanů domnívá, že nad údaji, které poskytují online, nemají úplnou kontrolu[3], což také negativně ovlivňuje rozvoj jednotného trhu v digitálním světě.[4] Nejen možnosti zneužití, ale také praktická využitelnost zpracování osobních údajů spolu s možností jejich monetizace (kdy se data stávají *„ropou nové ekonomiky“)*[5] mají za následek vzrůstající důležitost odpovídající právní úpravy. Nové technologie ovšem nepřinášejí jen větší rozsah zpracovávaných dat, ale také zcela nové problémy, se kterými se musí právo vyrovnat. Namátkou může jít o posouzení vztahu mezi zálohováním systému a právem být zapomenut, o „otravu“ blockchainu osobními údaji, předávání osobních údajů do zahraničí, personalizované určení cen, algoritmickou diskriminaci, či obecněji o problematiku cloudu, cookies, nebo technologie RFID. Setkávání nových technologií s právem na ochranu osobních údajů přináší pestré, aktuální, a přitom praktické otázky, jejichž regulace musí jednak udržet vysoký standard ochrany lidských práv a jednak zabezpečit budoucí směr inovací v evropském prostoru. Z množiny otázek s tímto

[1] Komise pro veřejné služby v. Pollak, 343 U.S. 451, 467 (1952) (soudce William O. Douglas, separátní votum). Dostupné z: https://supreme.justia.com/cases/federal/us/343/451/

[2] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 12, ISBN 978-80-7554-097-3.

[3] EUROPEAN COMMISSION. *Special Eurobarometer 431 - Data protection*, s. 6 [online]. [cit. 2018-11-05].

[4] Vytvoření „evropské datové ekonomiky“ je pak jedním z dílčích cílů tvorby jednotného digitálního trhu. Dle: EVROPSKÁ KOMISE. *Jednotný digitální trh* [online]. [cit. 2018-11-18]. Dostupné z: https://ec.europa.eu/commission/priorities/digital-single-market_cs

[5] Např. TOONDERS, Joris. Data is the new oil of the digital economy. *Wired* [online]. [cit. 2018-10-27]. Dostupné z: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/

tématem spojených je v této práci blíže řešena problematika hmotněprávní úpravy *big data* a automatizovaného individuálního rozhodování, které s *big data* úzce souvisí a tvoří tak kompaktní celek pro bližší zkoumání.

Centrálním předpisem pro tuto práci je již účinné Obecné nařízení o ochraně osobních údajů (GDPR)[6], které je některými označováno za *„jeden z nejvýznamnějších legislativních počinů Evropské unie posledních let"*[7] a mělo by být základem evropské regulace po další desítky let[8], když má být navrženo jako změnám odolné (*futureproof).*[9] Z důvodu technologické neutrality neobsahuje předpis výslovnou úpravu pro konkrétní technologie[10], ale obsahuje úpravu obecnou, jejíž aplikace na konkrétní technologie a postupy má být v problematických bodech osvětlena ze strany Sboru, dozorových úřadů či skrze judikaturu ESD. Této charakteristice právní úpravy odpovídá i struktura práce, kdy je pro obě vybrané oblasti poměřována jejich slučitelnost s obecnými zásadami ochrany osobních údajů. Důraz je kladen na problematická místa.

Cílem práce je zhodnotit funkčnost a perspektivy evropské ochrany osobních údajů pro vybrané technologické fenomény a představit několik úvah *de lege ferenda*. Pro naplnění výše zmíněného cíle slouží metody deskripce (zejména pro technický úvod), komparace (v menší míře pro porovnání s minulou úpravou) a kritické analýzy. Práce vychází zejména z dokumentů vypracovaných jednotlivými dozorovými úřady (a to zvlášť ze strany britského a norského

[6] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[7] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 7, ISBN 978-80-7502-288-2.

[8] RHOEN, Michiel a Qing Yi FENG. Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science. *International Data Privacy Law*. 2018, **8**(2), 140-159. DOI: 10.1093/idpl/ipy005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article/8/2/140/5045225

[9] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). [cit. 2018-10-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011

[10] Z tohoto důvodu je lichá následující námitka: *„GDPR's prescriptive nature means it was outdated before the ink even dried. It deals with the world as it is, not as it is likely to be in the next 20 years."* Dle: RASMUSSEN, Anders Fogh. The West's dangerous lack of tech strategy. *Politico* [online]. [cit. 2019-03-22]. Dostupné z: https://www.politico.eu/article/opinion-the-wests-dangerous-lack-of-tech-strategy/

úřadu, které považuji vzhledem ke své propracovanosti za nejinspirativnější) a WP29[11], stejně jako z odborných periodik. Ve vědeckých periodicích je patrný zvýšený zájem o toto téma, výsledky právního výzkumu v této oblasti mají znatelný dopad na aplikaci práva a chování správců i subjektů osobních údajů, jak je patrné na případě srovnávacích vysvětlení. Práce pak vychází v menší míře z komentářové literatury, která je použita spíše pro popis základních principů GDPR, když v práci řešené problematice se žádný ze současných komentářů dostatečně nevěnuje.[12] Judikatura ESD, ESLP a národních soudů členských států je použita k ilustraci některých dílčích problémů, ovšem širší rozhodovací praxe vztahující se bezprostředně k řešeným otázkám prozatím chybí. Technický popis je na mnoha místech proložen skutečnými příklady, které ukazují možnosti a hrozby popisovaných technologií a ilustrují tak výzvy, které stojí před regulátorem a správci osobních údajů. Zahrnutí technického popisu do práce odpovídá přesvědčení, že právní problémy spojené s novými technologiemi je třeba posuzovat v jejich celkovém společenském a technickém kontextu.[13] Popisované koncepty či postupy jsou tam, kde je to účelné, doplněny grafickým znázorněním, které se nachází v příloze.

Konkrétně je v první části práce, po stručné úvodní kapitole, řešena problematika *big data* a souladu s tím spojených způsobů zpracování s evropskou úpravou, kdy soulad je, jak již bylo zmíněno, poměřován vůči vybraným principům ochrany osobních údajů, které jsou v GDPR zakotveny. V podbodu věnovaném anonymizaci je pak posuzována možnost využití anonymizačních technik pro naplnění požadavků GDPR, stejně jako je upozorněno na možné nebezpečí, které nedostatečná anonymizace skýtá.

V druhé části je pak blíže řešeno příbuzné téma automatizovaného individuálního rozhodování, které nejčastěji vzhledem ke způsobu „trénování“ či „učení“ algoritmu vychází

[11] „Pracovní skupina pro ochranu údajů zřízená podle článku 29“ se s účinností GDPR přejmenovala na Evropský sbor pro ochranu osobních údajů, v textu je pro přehlednost používán původní název tam, kde daný dokument byl vydán ještě skrze „Pracovní skupinu“.

[12] Výslovně k problematice *big data* se vyjadřují, v patrně nejkvalitnějším současném komentáři, Voigt a von dem Bussche jen na třech stranách. Vizte VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017. ISBN 978-3-319-57959-7.

[13] Obdobně MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, s. 25, ISBN 978-80-904248-7-6.

právě ze širokých datových setů (*big data*). Mezi prvním a druhým tématem je tedy úzký vztah, když z hlediska transparentnosti nejproblémovější současné algoritmy vycházejí z *big data*. Dále jsou řešena dílčí témata vlastní pouze tomuto rozhodování, jmenovitě jde o naplnění zásady přesnosti v tréninkových datech pro zabránění vzniku diskriminačního algoritmu, stejně jako je řešena, pro ochranu subjektů údajů nesmírně důležitá, otázka existence a charakteru práva na vysvětlení.

V závěru práce je zhodnoceno Nařízení[14] nejen v těchto dvou bodech, ale i ve své celistvosti.

[14] V textu je *promiscue* používáno výrazů Nařízení, Obecné nařízení a GDPR. Pro vysvětlení všech zkratek užitých v práci vizte Seznam zkratek. Pro přehlednost textu se tam, kde jsou bez dalšího zmiňovány články a recitály, jedná o odkaz na GDPR.

2 Úvodní poznámky k unijní ochraně osobních údajů

V této kapitole je stručně představena systematika unijního systému ochrany osobních údajů, která představuje právní rámec pro posuzování následujících kapitol.

2.1 Právo na soukromí a právo na ochranu osobních údajů

Koncepce práva na soukromí

Definovat soukromí a s tím spojené právo na soukromí, je neobyčejně složité. Důvody jsou nasnadě; jde zejména o dynamický vývoj technických možností a v důsledku i právní regulace, nejasný rozdíl mezi právem na soukromí a právem na ochranu osobních údajů, stejně jako o střet dvou různých pojetí soukromí, vycházejících ze dvou různých právních kultur.[15] Jak v angloamerickém právním prostředí, tak v prostředí kontinentálního práva je ochraně soukromí přikládán značný význam, důraz je ale kladen na odlišné prvky.[16] V rámci těchto dvou širších proudů lze rozlišit celou řadu dalších pojetí soukromí, např. Solove rozlišuje 6 různých typů.[17]

Kontinentální, evropská, právní kultura vnímá ochranu soukromí převážně jako formu ochrany důstojnosti, či jako právo na informační sebeurčení.[18] Obecně lze shrnout, že ochrana soukromí představuje v evropském kontextu možnost ovlivňovat svůj „veřejný obraz“, právo

[15] Odlišná pojetí soukromí jsou jistě vlastní celé řadě různých kultur, vzhledem k rozsahu práce a významu příslušných právních úprav jsou dále rozebírány jen zmíněné dvě právní kultury.

[16] Rozdílné představy, a v důsledku i rozdílná úroveň právní ochrany, ostatně vedou k mnohým právním úskalím přeshraničního předávání osobních údajů.

[17] SOLOVE, Daniel. *Understanding Privacy*. Harvard University Press, 2008, s. 10. ISBN 978-0674027725.

[18] Pro tento koncept je určující zejména německá doktrína (*informationelle Selbstbestimmung*). Ústavní soud ČR právo na informační sebeurčení dovozuje z čl. 10 (3) a čl. 13 Listiny základních práv a svobod, s tím že k charakteru tohoto práva se ÚS vyjádřil následovně: *„svou povahou i významem tak právo na informační sebeurčení spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní), svobodou komunikační a zajisté i dalšími ústavně garantovanými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec je nutno respektovat a důsledně chránit; zcela právem jsou proto respekt a ochrana této sféry garantovány ústavním pořádkem, neboť – posuzováno jen z poněkud jiného úhlu – je o výraz úcty k právům a svobodám člověka a občana (čl. 1 Ústavy České republiky).“* Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, 94/2011 Sb.

garantující, že člověk bude viděn tak, jak si přeje být viděn.[19] Je příznačné, že v tomto pojetí je řada *leading cases* spojena s aristokracií, či obecně se slavnými osobnostmi (za všechny zmiňme případ monacké princezny Caroline von Hannover[20]). Hodnota soukromí spočívá také v tom, že jednotlivci přináší prostor pro jeho rozvoj[21], což prospívá nejen mu, ale i rozvoji společnosti a demokracie.[22]

Americké pojetí soukromí oproti tomu vnímá soukromí jako vyjádření svobody, zejména ve smyslu (negativní) svobody od státu.[23] Nejvyšší soud Spojených států amerických se v jednom z klíčových případů, Planned Parenthood v. Casey, vyslovuje takto: „*At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State."*[24] Zatímco pro evropské pojetí soukromí je přirozenou hrozbou přílišná pozornost médií a jiných soukromých aktérů na život jednotlivce, pro americké pojetí je prvořadou hrozbou stát. Ostatně ochrana soukromí je dovozována ze čtvrtého dodatku americké ústavy[25], který chrání před nepřiměřenými prohlídkami a konfiskacemi[26], a jehož cílem bylo do budoucna zabránit nadměrnému využívání

[19] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law School Legal Scholarship Repository*, s. 1161 [online]. [cit. 2018-12-06]. Dostupné z: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.cz/&httpsredir=1&article=1647&context=fss_papers

[20] Rozsudek ESLP ze dne 24. 6. 2004 ve věci von Hannover v. SRN, stížnost č. 59320/00

[21] Toto pojetí vystihuje Čechov ve slavné povídce Dáma s psíčkem: „*Měl dva životy – jeden život zjevný a veřejný, který viděl každý, komu bylo libo, plný relativní pravdy a relativní lži, docela podobný životu všech jeho známých a přátel, a druhý – probíhající tajně. Jakousi podivnou shodou okolností, snad náhodou, všechno, co bylo pro něho zajímavé a nutné, v čem byl upřímný a neklamal sám sebe, co tvořilo podstatu jeho života, probíhalo před druhými tajně (…). Všechno osobní dění se odehrává ve skrytu a snad se kulturní člověk částečně proto tolik namáhá, aby bylo chráněno osobní tajemství."* Blíže vizte: KUNER, Christopher. A Chekhovian view of privacy for the internet age. Oxford University Press Blog [online]. 2015 [cit. 2018-12-08]. Dostupné z: https://blog.oup.com/2015/10/chekhov-privacy-internet-age/

[22] SOLOVE, Daniel. *Understanding Privacy*. Harvard University Press, 2008, s. 74. ISBN 978-0674027725.

[23] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law School Legal Scholarship Repository*, s. 1161 [online]. [cit. 2018-12-06]. Dostupné z: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.cz/&httpsredir=1&article=1647&context=fss_papers

[24] Planned Parenthood v. Casey, 505 U.S. 833 (1992). Dostupné z: https://supreme.justia.com/cases/federal/us/505/833/

[25] „*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."* Dle The Constitution of the United States of America (ústava Spojených států amerických).

[26] K povaze čtvrtého dodatku Nejvyšší soud Spojených států amerických zmiňuje následující: „*at the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental*

tzv. *writs of assistance*, na základě kterých docházelo k nepřiměřeným domovním prohlídkám za účelem odhalení pašovaného zboží.[27] Ve prospěch existence práva na ochranu soukromí poprvé komplexně argumentovali Samuel Warren s Louisem Brandeisem ve svém proslulém článku „*The Right to Privacy"*[28] , kdy zmíněné právo popisovali jako „*the right to be let alone*"[29]. Rozdílnost přístupů lze ilustrovat na tom, které aspekty současné společnosti jsou v jednotlivých zemích či právních kulturách považovány za problematické. Z amerického pohledu je tak např. zarážející v Evropě běžná praktika, kdy stát má možnost rozhodovat o tom, že vybrané dětské jméno je nevhodné a rodiče jej dítěti nemohou udělit[30], stejně jako je značně kontroverzní otázka zavedení povinných federálních identifikačních průkazů.[31] Nelze tedy tuto problematiku zjednodušit tak, že v USA není právo na soukromí důležité – koneckonců, některé z nejkontroverznějších rozhodnutí amerického Nejvyššího soudu jsou založeny právě na ochraně soukromí.[32] Stejně tak nelze zjednodušit, že ve Spojených státech je úroveň ochrany soukromí nižší, spíše jde o jiné pojetí. Zároveň je třeba zdůraznit, že také evropské pojetí je blízce spjato se svobodou.[33]

Výše zmíněné kontinentální pojetí ochrany soukromí jako prostoru svobody rozvoje jednotlivce pojmenovává Wachter jako první stupeň soukromí, a to vnitřní soukromí (*internal privacy*). Vnitřní soukromí je hodnotou nejen pro jednotlivce, ale také pro společnost, neboť je nezbytným předpokladem pro vznik plurality názorů.[34] Vnější soukromí (*external privacy)* je

intrusion." Silverman v. United States, 365 U.S. 505 (1961). Dostupné z: https://supreme.justia.com/cases/federal/us/365/505/

[27] AMITAI, Etzioni a Christopher RICE. *Privacy in a Cyber Age: Policy and Practice*. Palgrave, 2015, s. 63. ISBN 978-1-137-51396-0.

[28] WARREN, Samuel a Louis BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. **4**(5) [cit. 2018-12-06]. Dostupné z: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[29] Z tohoto amerického pojetí vychází citát z úvodu práce.

[30] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law School Legal Scholarship Repository*, s. 1158 [online]. [cit. 2018-12-06]. Dostupné z: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.cz/&httpsredir=1&article=1647&context=fss_papers

[31] K tomu blíže vizte např.: AMERICAN CIVIL LIBERTIES UNION. *5 Problems with national ID cards* [online]. [cit. 2018-12-06]. Dostupné z: https://www.aclu.org/other/5-problems-national-id-cards

[32] Za všechny zmiňme případ týkající se zákazů interrupcí, Roe v. Wade .Vizte: Roe v. Wade, 410 U.S. 113 (1973), Dostupné z: https://supreme.justia.com/cases/federal/us/410/113/

[33] Srov. v čase 1:00:10 LENAERTS, Koen. *The General Data Protection Regulation five months on* [online]. [cit. 2018-12-18]. Dostupné z: https://www.youtube.com/watch?v=fZaKPaGbXNg

[34] WACHTER, Sandra. Privacy: Primus Inter Pares: Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights. *The Alan Turing Institute* [online]. [cit. 2019-02-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514

pak prostorem, ve kterém dochází k vyjádření a k projevu jednotlivce, který se díky vnitřnímu soukromí mohl svobodně rozvinout. Toto propojení vnímá též český Ústavní soud, podle kterého *„zjednodušeně řečeno, v podmínkách vševědoucícho a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.“*[35] Třetí stupeň soukromí, *premium privacy*, pak představuje prostor ochrany citlivých osobních údajů. Na základě tohoto rozdělení Wachter dovozuje, že ochrana soukromí, respektive právo na ochranu soukromí, je nutným předpokladem rozvoje navazujících práv (např. svobody slova, práva na vzdělání) a je tak v jistém ohledu oproti těmto právům vyvýšeno (Wachter mluví o *primus inter pares)*.[36]

Také třístupňový, jinak ale zcela odlišný model soukromí či přesněji „digitální identity“ nabízí Szymielewiczová.[37] Tento model je partikulární v tom, že se zabývá soukromím výhradně v digitálním prostředí. První vrstvu představují údaje, které jednotlivec vědomě vyplňuje či jiným způsobem vědomě sdílí s určitou službou či aplikací (může jít o vyplněnou emailovou adresu, o historii hledání nebo o nahrané fotografie). Druhou vrstvu představují informace, které lze vyčíst z interakcí s danou službou, které ale zároveň nejsou vědomě poskytnuty (zde patří rychlost psaní, překlepy ve psaní, čas strávený čtením daného příspěvku apod.). Konečně třetí vrstvu představují informace o jednotlivci, které na základě dvou výše zmíněných vrstev dovozuje daná služba. Dle Szymielewiczové bude typické, že třetí vrstva soukromí bude namířena na zjištění těch informací, které jednotlivec není ochoten sdílet dobrovolně a které jsou zároveň důležité z hlediska času stráveného používáním dané služby či z hlediska nákupního chování. Problematické pak je, že přímou kontrolu má jednotlivec pouze nad první vrstvou, přestože rozhodnutí o něm může služba činit zejména na základě údajů vyvozených v rámci třetí vrstvy (k automatizovanému individuálnímu rozhodování blíže v kapitole 4).

[35] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, 94/2011 Sb.

[36] WACHTER, Sandra. Privacy: Primus Inter Pares: Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights. *The Alan Turing Institute,* s. 21 [online]. [cit. 2019-02-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514

[37] SZYMIELEWICZOVÁ, Katarzyna. Your digital identity has three layers, and you can only protect one of them. *Quartz* [online]. [cit. 2019-02-19]. Dostupné z: https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

Ve výše zmíněných modelech je ochrana soukromí chápána jako ochrana před nadměrnými zásahy státu či obecně třetích stran[38] do soukromé sféry jednotlivce, která má umožnit jeho rozvoj. Tento koncept je převažující, nikoliv ovšem jediný. Lze také zmínit názor, že zásahy do soukromí jsou ve skutečnosti zásahy do majetkových práv (teorie redukcionalismu), že zájmy chráněné jako soukromí nejsou rozlišitelné a soukromí je tak chráněno ekonomicky nevhodnými způsoby (law and economics) nebo že koncept soukromí ve skutečnosti slouží zájmům vládnoucí skupiny k zakrývání dominance nad znevýhodněnými skupinami, zejm. nad ženami (feministická kritika soukromí).[39]

Právo na ochranu osobních údajů

Zatímco smysl (a možné rozdílné pojetí) práva na soukromí byly popsány výše, právo na ochranu osobních údajů má zajistit spravedlivé zpracování a, v jistém ohledu[40], také spravedlivost výsledků jednotlivého zpracování.[41] Pro naplnění tohoto cíle slouží řada zásad (zásada korektnosti, transparentnosti, omezení účelu, minimalizace údajů aj.). Odborná debata, která následovala poté, co bylo právo na ochranu osobních údajů vloženo do primárního práva a uznáno jako jedno ze základních práv v rámci Evropské unie, v podstatě stále trvá. Lze shrnout, že nepanuje shoda nad tím, jaký význam toto povýšení mezi základní

[38] S tím, že v zásazích do soukromí je patrné stoupající množství zásahů ze strany soukromých společností. K tomu trefně Kühn: *„Kdo dnes vskutku může zasáhnout více do soukromí lidí? Je to stát s tisíci soudně povolených odposlechů ročně a systémem vzájemně nepropojených a na sobě nezávislých veřejně provozovaných kamerových systémů, nebo mamutí společnosti typu Facebook či Google, které o stovkách milionů uživatelů vědí více než tito uživatelé sami? (…) Ostatně nazývat vztah mezi uživatelem Faceboooku a korporací vztahem* horizontálním*, tedy svou povahou rovným, je samo o sobě sice právně čisté, nicméně v naprostém rozporu s realitou."* Dle: KÜHN, Zdeněk. Lidská práva v zajetí dvě stě let starých doktrín. AGHA, Petr a kol. *Budoucnost státu?.* Praha: Academia, 2017, s. 155-160. Společnost (Academia). ISBN 978-80-200-2681-1.

[39] Shrnutí kritických teorií dle WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. ŠIMÍČEK, Vojtěch. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011, s. 50, ISBN 978-80-210-5449-3.

[40] Tento sekundární cíl je dle současné judikatury ESD značně omezen, doktrinálně se dovozuje nutnost proaktivnějšího přístupu.
Blíže: WACHTER, Sandra a Brent MITTELSTADT. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review* [online]. [cit. 2019-02-20]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
Dále vizte: Rozsudek Soudního dvora ze dne 20. prosince 2017. Peter Nowak v. Data Protection Commissioner, Věc C-434/16, ECLI:EU:C:2017:994. Dostupné z:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=13042823

[41] TZANOU, Maria. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law* [online]. **3**(2) [cit. 2018-12-06]. Dostupné z: https://academic.oup.com/idpl/article/3/2/88/709116?searchresult=1

práva mělo, respektive co toto nové právo přináší oproti právu na soukromí. Někteří autoři jej také stále považují pouze za součást práva na soukromí.[42] Není ovšem příliš účelné odhlížet od reality primárního práva – podle toho totiž jde o samostatné právo, které tedy „něco navíc" přináší. Dle de Herta a Gutwirtha je právo na soukromí nástrojem neprůhlednosti (*opacity*), zatímco ochrana osobních údajů je naopak nástrojem transparentnosti. Neprůhlednost jako nástroj soukromí chrání jednotlivce před nadměrnými zásahy zvnějšku, zatímco ochrana osobních údajů, jako nástroj transparentnosti, zaručuje legitimitu těchto jednotlivých zásahů.[43] Tato teorie je ale podle jiných autorů vnitřně rozporná, když zároveň prezentuje ochranu osobních údajů jako neodmyslitelnou součást právního rámce a zároveň jako pouhý doplněk určující povolenou úroveň zpracování.[44] Dle Lynskey přidaná hodnota spočívá v rozšíření dostupných nástrojů (jakým je např. právo na přenositelnost) pro subjekty údajů a samostatná existence práva přináší „přidanou hodnotu" zejména ve snižování nerovnosti ve vztazích mezi správci a subjekty údajů.[45] Příkladem tohoto snižování nerovnosti je právě regulace automatizovaného individuálního rozhodování, která vychází z ochrany osobních údajů.[46]

V případě *Promusicae* z roku 2008 (v té době již bylo právo na ochranu osobních údajů součástí Listiny základních práv Evropské unie, její právní status ovšem nebyl ještě zřejmý[47]) ESD určil, že *„je však třeba konstatovat, že se sporná situace, v jejíž souvislosti předkládající soud tuto otázku pokládá, dotýká krom dvou výše uvedených práv i dalšího základního práva, totiž práva, které* ***zaručuje ochranu osobních údajů, a tedy soukromí"***[48](zdůraznění doplněno). Z výše

[42] Např. dle Žůrka jde o „*imanentní součást práva na ochranu soukromí"*. Dle ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 12, ISBN 978-80-7554-097-3

[43] TZANOU, Maria. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law* [online]. **3**(2) [cit. 2018-12-06]. Dostupné z: https://academic.oup.com/idpl/article/3/2/88/709116?searchresult=1

[44] Tamtéž.

[45] LYNSKEY, Orla. Deconstructing data protection: the 'added value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*. 2014, **63**(3). DOI: 10.1017/S0020589314000244. ISSN 0020-5893. Dostupné také z: http://www.journals.cambridge.org/abstract_S0020589314000244

[46] Tamtéž, s. 24.

[47] CRAIG, Paul a Gráinne DE BÚRCA. *EU law: text, cases, and materials*. Sixth edition. New York: Oxford University Press, 2015, s. 394, ISBN 9780198714927.

[48] Bod 63, Rozsudek Soudního dvora ze dne 29. 1. 2008. Productores de Música de España (Promusicae) v. Telefónica de España SAU, Věc C-275/06, ECLI:EU:C:2008:54. Dostupné z: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06

zmíněného spojení (*a tedy soukromí*) plyne, že ESD považoval ochranu osobních údajů za součást ochrany soukromí.

V případě *Schecke* (kdy již nebylo o závaznosti Listiny základních práv Evropské unie pochyb), ESD nejdříve mluví o tom, že ochrana osobních údajů „(…) *úzce souvisí s právem na respektování soukromého života zakotveným v článku 7 téže Listiny"*[49] a dále uzavírá, že „*za těchto podmínek je třeba mít za to, že se jednak* ***respektování práva na soukromý život v souvislosti se zpracováním osobních údajů****, přiznaného články 7 a 8 Listiny, vztahuje na* (…)"[50](zdůraznění doplněno). I v tomto případě ESD, zdá se, podřazuje ochranu osobních údajů pod ochranu soukromí, respektive pod právo na respektování soukromého života, a to přestože generální advokátka Sharpston ve svém stanovisku mluvila o dvou samostatných právech.[51]

Ochrana osobních údajů je koncipována jako součást práva na ochranu soukromí také v řadě ústav členských států Evropské unie, např. v ústavě nizozemské, španělské či finské.[52] Lze tedy shrnout, že právo na ochranu osobních údajů je úzce spjato s právem na ochranu soukromí, s tím, že není zcela zřejmé, nakolik je skutečně právo na ochranu osobních údajů samostatným právem, byť *de lege lata* se o samostatné právo jedná. Judikatura ESD v této otázce doposud nezaujala pevné a vnitřně bezrozporné stanovisko, s tím že výše zmíněné judikáty poukazují na zdrženlivost ESD.

[49] Bod 47, Rozsudek Soudního dvora ze dne 9. listopadu 2010. Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3584200

[50] Tamtéž, bod 52.

[51] Bod 71, Stanovisko generální advokátky Eleanor Sharpston ve věci spojených věcí C-92/09 a C-93/09 Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:62009CC0092&from=GA

[52] LYNSKEY, Orla. Deconstructing data protection: the 'added value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*, s. 2, 2014, **63**(3). DOI: 10.1017/S0020589314000244. ISSN 0020-5893. Dostupné také z: http://www.journals.cambridge.org/abstract_S0020589314000244

2.2 Přehled unijní právní úpravy

Ještě předtím, než se dostaneme k unijní úpravě, je vhodné zmínit, že případ Stauder[53], který představoval zlom v do té doby zdrženlivé judikatuře týkající se ochrany základních práv, se týkal právě kategorie ochrany soukromí či ochrany osobních údajů. Zmíněný případ se týkal posouzení toho, zda má fyzická osoba povinnost prokazovat svoji totožnost pro možnost obdržení benefitu, zde slevy na máslo. Byť nejdůležitějším výsledkem zmíněného případu byla konstrukce doktríny základních práv jako obecné zásady právní[54], není bez zajímavosti, že se případ obsahově týkal právě ochrany soukromí, respektive šířeji ochrany lidské důstojnosti.

Na úrovni primárního práva nalézáme úpravu ochrany osobních údajů na třech místech. V Listině základních práv Evropské unie, která je, jak již bylo zmíněno, součástí primárního práva, je ochrana osobních údajů upravena článkem 8. Ten určuje, že toto právo náleží každému a osobní údaje musí být *„zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“*[55] Jinými slovy je již na úrovni primárního práva stanovena zásada korektnosti, zásada omezení účelu a právo subjektů údajů na přístup k osobním údajům a na jejich opravu. Principy a práva subjektů údajů GDPR dále rozšiřuje. Zejména v případech, kdy se uvažuje o omezení nebo dokonce upuštění od některých principů je důležité uvážit, které principy jsou zakotveny pouze skrze sekundární právo, a které jsou výslovně uvedeny i v právu primárním. Úpravu obsaženou v Listině lze zároveň, na úrovni primárního práva, považovat za nejdůležitější.

[53] Rozsudek Soudního dvora ze dne 12. listopadu 1969. Erich Stauder v City of Ulm, Sozialamt, Věc C-29/69, ECLI:EU:C:1969:57. Dostupné z: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=29-69&td=ALL

[54] TOMÁŠEK, Michal, Vladimír TÝČ, Jiří MALENOVSKÝ, et al. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017. Student (Leges), s. 332. ISBN 978-80-7502-184-7.

[55] Článek 8, Listina základních práv Evropské unie (Charta základních práv EU), vyhlášená pod č. 111/2009 Sb. m. s.

Dále je v článku 5, odst. 3 SEU[56] zakotven, vedle společných ústavních tradic členských států, odkaz na Evropskou úmluvu o ochraně lidských práv a základních svobod[57], která obsahuje právo na respektování soukromého a rodinného života, a to taktéž v článku 8. Judikatura ESLP je také důležitým doplněním pro výklad práva na ochranu soukromí a následně práva na ochranu osobních údajů. ESLP například potvrdil, že smyslem ochrany soukromí je svobodný rozvoj a naplnění osobnosti jednotlivce[58], s tím že dokonce mluví o právu na osobní rozvoj.[59] Judikatura ESLP, která Evropskou úmluvu rozvíjí v duchu doktríny „živoucího nástroje", pak ochranu soukromí vztahuje na široké spektrum různých situací.[60] V podstatě sektorovou implementací[61] článku 8 Evropské úmluvy je pak Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů (úmluva č. 108).[62] Ochrana poskytována výše zmíněným čl. 8 LZPEU překračuje svým rozsahem čl. 8 EÚLP, s tím že ve světle vývoje sekundárního práva můžeme uzavřít, že unijní standard ochrany osobních údajů je širší oproti standardu štrasburskému, ze kterého ovšem vychází.[63]

Článek 16 SFEU[64] opětovně stanovuje, že *„každý má právo na ochranu osobních údajů"* a v druhém odstavci zplnomocňuje EP a Radu k přijetí příslušných pravidel pro případy, kdy osobní údaje zpracovávají orgány, instituce, jiné subjekty Unie a členské státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie.

[56] Smlouva o Evropské unii.
[57] Evropská úmluva o ochraně lidských práv ve znění Protokolů č. 11 a 14
[58] Rozhodnutí EKLP ze dne 11. 7. 1980 ve věci Deklerck v. Belgie, stížnost č. 8307/78.
[59] Rozsudek ESLP ze dne 28. 1. 2003 ve věci Peck v. Spojené království, stížnost č. 44647/98.
[60] WACHTER, Sandra. Privacy: Primus Inter Pares: Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights. *The Alan Turing Institute* [online]. [cit. 2019-02-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514
[61] NOVÁK, Daniel. *Problémy ochrany soukromí a osobních údajů v právu EU*, s. 32, Brno, 2011. Disertační práce. Právnická fakulta Masarykovy univerzity. Vedoucí práce Filip Křepelka**.**
[62] Úmluva Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat
[63] Ostatně v roce 1995, ve kterém byla na unijní úrovni přijata směrnicová úprava ochrany osobních údajů, byly všechny tehdejší členské státy též smluvními stranami úmluvy č. 108. Dle: AGENTURA EVROPSKÉ UNIE PRO ZÁKLADNÍ PRÁVA. *Příručka evropského práva v oblasti ochrany údajů*. Lucemburk: Úřad pro publikace Evropské unie, 2015, s. 18. ISBN 978-92-871-9933-1.
[64] Smlouva o fungování Evropské unie

Na úrovní sekundárního práva je centrálním předpisem GDPR, které nahradilo předchozí směrnicovou úpravu.[65] Většina autorů zdůrazňuje, že GDPR není revolucí, ale navazuje na základní schéma původní úpravy, stejně jako na dosavadní judikaturu a zavádí spíše dílčí novinky.[66] Za největší rozdíl je označována volba formy právní regulace, kdy skrze formu nařízení má dojít ke skutečnému sjednocení právní regulace v členských státech. Vzhledem k rozsahu a cílům práce se srovnání těchto dvou úprav dále nevěnuji.

Nový rámec evropské právní úpravy dále tvoří Směrnice Evropského parlamentu a Rady (EU) 2016/680 (tzv. trestněprávní směrnice)[67] a Směrnice Evropského parlamentu a Rady (EU) 2016/681 (tzv. PNR – *passenger name record* - směrnice).[68] První zmíněná směrnice upravuje ochranu osobních údajů při činnosti orgánů činných v trestních řízeních a druhá zmíněná směrnice upravuje povinnosti leteckých dopravců ohledně předávání jmenné evidence cestujících osob příslušným orgánům. Tato úprava tak nemá na běžné správce či zpracovatele praktický dopad[69], ani přímo nesouvisí s dále zkoumaným tématem práce.

Posledním souvisejícím předpisem pak je tzv. e-Privacy nařízení, které mělo původně nabýt účinnosti spolu s GDPR[70] a které bude upravovat mj. problematiku cookies a šíření obchodních sdělení. Zatímco GDPR se týká pouze fyzických osob, e-Privacy nařízení chrání důvěrnost elektronických komunikací osob fyzických i právnických.[71] Vzhledem ke zdržení příprav tohoto předpisu zůstává prozatím účinná tzv. e-Privacy směrnice.[72]

[65] Směrnice 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

[66] Např. MORÁVEK, Jakub. Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?. *Právní rozhledy*. 2018(13-14), 487.

[67] 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

[68] Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

[69] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 17, ISBN 978-80-7554-097-3

[70] Tamtéž, s. 17.

[71] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Tisková zpráva: Nařízení o ePrivacy jako doplněk k GDPR* [online]. [cit. 2018-12-19]. Dostupné z: https://www.uoou.cz/tiskova-zprava-narizeni-o-nbsp-eprivacy-jako-doplnek-k-nbsp-gdpr/d-27454/p1=1017

[72] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

Závěrem lze shrnout, že unijní úprava se blíží konceptu jednotné (*omnibus*) úpravy ochrany osobních údajů, kterou můžeme odlišit od sektorového přístupu typického pro úpravu ve Spojených státech.[73]

[73] LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. Oxford studies in European law, s. 15. ISBN 978-019-8718-239.

3 Big Data

„Big data is our generation's civil rights issue, and we don't know it."[74]

3.1 Technický úvod

Není přehnané říci, že žijeme v éře velkých dat (*big data,* česky někdy též jako veledata). Jedním z hlavních důvodů je fakt, že stále více věcí data generuje; ať už jde o telefony, nositelnou elektroniku (např. „chytré hodinky") či domácí spotřebiče. Postupné rozšiřování trendu různých chytrých doplňků do nových oblastí lidského života ilustrují příklady chytrého stojanu na vajíčka[75] nebo třeba chytré vidličky[76] – příklady jsou pochopitelně zvoleny záměrně a význam zmíněných produktů je nevelký, ukazují ovšem proměnu technologií a rozmach tzv. „Internetu věcí" (*Internet of Things, IoT*)[77]. Pro ochranu osobních údajů je důležitým rysem také to, že tento rozvoj lze popsat jako třetí krok digitalizace světa, kterou je digitalizace člověka (tedy převedení chování, tělesných funkcí či výkonů do strojově zpracovatelné podoby).[78] Vytváření digitální stopy dnes patří k běžné součásti života. Jinými slovy, generování obšírných dat o sobě samém již není výsadou minoritního, aktivního a vědomého

[74] CROLL, Alistair. Big data is our generation's civil rights issue, and we don't know it: What the data is must be linked to how it can be used. *Radar* [online]. [cit. 2018-10-29]. Dostupné z: http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html

[75] GARUN, Natt. Egg Minder smart tray lets you remotely check the freshness of your eggs. *Digital Trends* [online]. [cit. 2018-10-29]. Dostupné z: https://www.digitaltrends.com/home/egg-minder-smart-tray-lets-you-remotely-check-the-freshness-of-your-eggs/

[76] FLACY, Mike. HAPIfork tracks your eating habits, encourages healthier eating. *Digital Trends* [online]. [cit. 2018-10-29]. Dostupné z: https://www.digitaltrends.com/home/hapifork-tracks-your-eating-habits-encourages-healthier-eating/

[77] Ostatně o ambicích největších hráčů v tomto směru svědčí směr jejich akvizicí. U Googlu, přesněji Alphabet Inc., výběr z dlouhého seznamu zahrnuje Waze (svérázná sociální síť, respektive navigační systém do aut fungující skrze aplikace v telefonu či přímo v systému auta), Nest (společnost vyrábějící mj. chytré termostaty), Dropcam (chytré bezpečnostní kamery), Senosis Health (měření tělesných funkcí) či Cronologics (chytré hodinky). Všechny tyto služby mají potenciál dále zvýšit intenzitu sběru dat. Čím více dat společnosti jako Google mají, tím lépe mohou odhadnout zákaznické chování a tím lépe mohou obsloužit a monetizovat zákazníka. Slovy Jeffa Hammerbacha: *„The best minds of my generation are thinking about how to make people click ads."*
Dle: O`REILLY, Tim, Mike LOUKIDES, Julie STEELE a Colin HILL. *How Data Science Is Transforming Health Care*. O'Reilly Media, 2012, ISBN 9781449356187.

[78] KOUBSKÝ, Petr. Poznámky k digitalizaci člověka. *067.cz* [online]. [cit. 2018-10-30]. Dostupné z: https://067.cz/archiv/33/poznamky-k-digitalizaci-cloveka.html

přístupu *quantified self*[79], ale je spíše nevyhnutelnou, byť často netušenou, součástí života a práce s moderními technologiemi. Trefně se mluví o *„digitálních zplodinách"*, kdy lidé svým životem o sobě generují data jako nechtěný vedlejší produkt.[80] Realita tvorby mohutné digitální stopy ze strany Evropanů nás tedy přivádí zpět k fenoménu *big data.*

Big data jsou klasicky definovány skrze tři V – volume, velocity a variety[81], tedy skrze objem, rychlost zpracování a různorodost dat. Přirozeným problémem je klasifikace velikosti, kdy se s rostoucím objemem dat na internetu mění naše chápání toho, co je dostatečně velkou datovou sadou pro zařazení do kategorie *big data*.[82] Přestože bylo vůči původní definici tří V z roku 1997 v dalších letech navrženo mnoho možných doplnění (např. definice skrze 4V od IBM či skrze 6V od Microsoftu)[83], pro účely této práce vyjděme z toho, že *big data* odkazují k postupu kombinování velkého objemu dat, které byly typicky získány z rozmanitých zdrojů a následně jsou analyzovány sofistikovanými algoritmy.[84] Charakteristikou fenoménu *big data* není jen samotná existence datových setů v dosud nevídaných velikostech, ale také to, že tyto data neleží ladem.[85] Přestože součástí těchto dat nemusí nevyhnutelně být osobní údaje, když

[79] Přístup vznikl okolo roku 2007, spolu s rozvojem chytrých telefonů, a spočíval v záměrném sběru dat o svém životě a následném, zejména individuálním, vyhodnocování korelací. Známý příklad „výročních zpráv" ze života Nicholase Feltrona je přiložen do přílohy.
Dle: LEIBENGER, Dominik, Frederik MÖLLERS, Anna PETRLIC, Ronald PETRLIC a Christoph SORGE. Privacy Challenges in the Quantified Self Movement – An EU Perspective. *Proceedings on Privacy Enhancing Technologies* [online]. 2016, **2016**(4), 315-334 [cit. 2018-10-30]. DOI: 10.1515/popets-2016-0042. ISSN 2299-0984. Dostupné z: http://content.sciendo.com/view/journals/popets/2016/4/article-p315.xml

[80] MUNIR, Abu Bakar, Siti Hajar Mohd YASIN a Firdaus MUHAMMAD-SUKKI. Big Data: Big Challenges to Privacy and Data Protection. *International Journal of Computer and Information Engineering* [online]. **9**(1) [cit. 2018-10-31]. Dostupné z: https://waset.org/publications/10000669/big-data-big-challenges-to-privacy-and-data-protection

[81] BUYYA, Rajkumar, Rodrigo CALHEIROS a Amir Vahid DASTJERDI. *Big data: Principles and paradigms*. Cambridge, MA: Elsevier/Morgan Kaufmann, 2016, s. 7, ISBN 978-012-8053-942.

[82] Zatímco např. dle Koubského pojem *big data* začíná vycházet z užívání, když *„skoro všechna data jsou dnes big"*, dle Pfeffera a Gawlasové naopak *„takto velký objem dat v současné době téměř nikdo nemá k dispozici".*
KOUBSKÝ, Petr. Hrnečku, vař! řekl Mark Zuckerberg. *Deník N* [online]. [cit. 2019-02-23]. Dostupné z: https://denikn.cz/66855/hrnecku-var-rekl-mark-zuckerberg/?ref=tit
PFEFFER, Jan a Hana GAWLASOVÁ. Big Data právním pohledem. Hospodářské noviny [online]. [cit. 2018-10-29]. Dostupné z: https://ihned.cz/c1-60126320-big-data-pravnim-pohledem

[83] BUYYA, Rajkumar, Rodrigo CALHEIROS a Amir Vahid DASTJERDI. *Big data: Principles and paradigms*. Cambridge, MA: Elsevier/Morgan Kaufmann, 2016, s. 8, ISBN 978-012-8053-942.

[84] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28], s. 7, Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[85] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

big data nachází využití také např. při výzkumu meteorologických změn, největší potenciál mají *big data* právě v predikování lidského chování, či obecně řečeno v analýze osobních údajů skrze hledání vzájemných vztahů, trendů a korelací.[86]

Pro dopad na práva subjektů je důležitým poznatkem také to, že rozvoj schopnosti shromažďovat a efektivně pracovat s rozsáhlými sadami dat je v jistém smyslu předpokladem pro uplatnění dalších, příbuzných technologií. Mezi tyto technologie, které mohou mít znatelný negativní dopad na základní práva a které jsou s *big data* úzce provázány, patří zejména nové modely strojového učení (*machine learning*). Výsledky analýzy těchto objemných datových setů nacházejí všestranná využití, která jsou již dnes samozřejmou součástí životů Evropanů; ať už jde o spamový filtr v emailových schránkách, rozpoznávání podvodných bankovních transakcí nebo třeba doporučování relevantního obsahu při poslechu hudby či sledování videí. Klíčovou charakteristikou těchto analýz a s nimi spojených predikcí je fakt, že jde o určování pravděpodobnosti určitého chování na základě chování minulého.[87] Přirozenou vlastností těchto systému je tedy chybovost a vytváření buďto falešně pozitivních nebo falešně negativních výsledků. Druhou důležitou charakteristikou těchto analýz je, že své predikce sice zakládají na určitém širokém datovém setu, ten ovšem často nepředstavuje reprezentativní vzorek z celkové populace.[88] V důsledku těchto omezení může algoritmus, který je sám o sobě navržen neutrálně, vydávat diskriminační výsledky (někteří autoři mluví o fenoménu „*digitální diskriminace*“[89]), jak je blíže popsáno v kapitole 4.2.3 – Zásada přesnosti a algoritmické vězení. Tuto limitaci pramenící z nereprezentativnosti vzorku[90] musíme odlišit

[86] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28], s. 7, Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[87] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *#BigData: Discrimination in data-supported decision making* [online]. (2018) [cit. 2018-10-28]. DOI: 10.2811/343905. Dostupné z: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

[88] ŽLIOBAITĖ, Indrė. Measuring discrimination in algorithmic decision making. *Data Mining and Knowledge Discovery* [online]. 2017, **31**(4), 1060-1089 [cit. 2018-10-28]. DOI: 10.1007/s10618-017-0506-1. ISSN 1384-5810. Dostupné z: http://link.springer.com/10.1007/s10618-017-0506-1

[89] Tamtéž, s. 6.

[90] Někteří autoři tvrdí, že v případě *big data* bude často analyzovaným vzorkem celá populace určitého jevu (n = populace). Taková situace může nastat např. při analýze chování návštěvníků určité webové stránky, kdy lze snadno analyzovat všechny návštěvníky (byť taková analýza nemusí vůbec šíří svého datového setu spadat pod *big data*), obecně jde ale, alespoň prozatím, spíše o techno-optimistické přání.
Dle: HILDEBRANDT, Mireille. Esclaus de les macrodades. O no? / Slaves to Big Data. Or Are We?. *IDP. Revista de Internet, Derecho y Política* [online]. [cit. 2018-11-15]. Dostupné z:

od záměrné analýzy chyb či chybných údajů, jakou je například analýza překlepů, kterých se uživatelé dopouští při používání internetových vyhledávačů.[91]

3.2 Právní úprava ochrany osobních údajů

3.2.1 Obecně

V případě, kdy *big data* zpracovávají osobní údaje, se uplatní úprava GDPR. Obecně lze říci, že existuje velká pravděpodobnost, že velké datové sety budou osobní údaje obsahovat (a spadat tak pod úpravu GDPR), a to i když se na první pohled může jevit, že datový set obsahuje pouze technické údaje či obsahuje již anonymizované údaje. Voigt a von dem Bussche[92] nabízí příklad, kdy výrobní společnost pro zvýšení efektivity zpracovává statistické údaje ohledně počtu vyrobených kusů na jednotlivých výrobních linkách, spolu s umístěním jednotlivých linek a časovým harmonogramem výroby. Při zkombinování tohoto datového setu s rozvrhem práce jednotlivých zaměstnanců (který v tomto případě slouží jako podpůrná informace k primární datové sadě) může společnost určit produktivitu jednotlivých zaměstnanců, a půjde tedy o zpracování osobních údajů. Celý datový set tímto bude spadat pod právní úpravu ochrany osobních údajů. Tyto podpůrné informace ovšem zdaleka nemusí mít tak očividnou formu, jako v příkladu Voigta a von dem Busscheho. Podpůrné informace budou totiž nejčastěji extrahovány skrze *data mining* z jiných veřejně dostupných zdrojů, z digitálních otisků jednotlivých osob.

V těchto případech se tedy uplatní všechny povinnosti dopadající na správce osobních údajů. Ty ovšem mohou v případě zpracování *big data* představovat pro správce i regulátora výzvu, zejména s ohledem na nutnost dodržení zásad omezení účelu, minimalizace údajů a transparentnosti, jak je blíže popsáno níže.

https://idp.uoc.edu/articles/abstract/10.7238/idp.v0i17.1977/

[91] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

[92] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 236, ISBN 978-3-319-57959-7.

3.2.2 Odpovědnost

Z klasické definice (3V) vyplývá, že mezi základní prvky *big data* patří i různorodost dat (*variety)*, která je často spojena s různorodými zdroji, ze kterých jsou data získávána. Vzhledem k množství zdrojů může být obtížné pro správce určit, kdo je odpovědný za ochranu osobních údajů nebo kdo má vyřizovat žádosti subjektů osobních údajů.[93] Při obvyklém stavu, kdy ani velké společnosti často nemají kapacitu a potřebné know-how k provádění zmíněné analýzy, se obrací společnosti na specializované datové konzultanty.[94] V případě, kdy společnost zadává třetí straně analýzu svého datového setu, jde z hlediska GDPR o klasický vztah správce a zpracovatele, kdy správce má mj. povinnost vybrat zpracovatele, který poskytuje *„dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.“*[95] V případech, kdy účel a prostředky zpracování určuje více osob, budou všechny tyto osoby považovány za správce[96], když všechny naplňují definici správce.[97]

Z hlediska odpovědnosti bude, vzhledem k principu odpovědnosti správce, klíčové identifikovat, který subjekt určil účel a prostředky zpracování. Pro identifikaci správce je důležité zejména hledisko určení účelu[98], s tím že bude stačit, aby prostředky zpracování vymezil jen obecným způsobem (jen obecné vymezení odpovídá složitosti zapojených

[93] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 237, ISBN 978-3-319-57959-7.
[94] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028
[95] Článek 28, Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[96] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 237, ISBN 978-3-319-57959-7.
[97] Správcem se rozumí, dle článku 4, *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení“*.
[98] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 86, ISBN 978-80-7554-097-3.

statistických modelů). Správce následně bude odpovědný za to, že zpracování osobních údajů odpovídá všem níže zmíněným zásadám.

3.2.3 Zásada zákonnosti

Zásada zákonnosti je předpokladem naplnění dalších zásad, když podle této zásady může správce osobní údaje k určitému účelu zpracovávat (a tedy je mít) jen tehdy, svědčí-li mu k takovému zpracování právní důvod (titul).[99] Právní tituly jsou vyjmenovány v článku 6. V případech *big data* půjde zejména o souhlas, plnění smlouvy a o oprávněné zájmy správce. Vzhledem k různorodosti zdrojů, ze kterých se získávají data k další analýze, není jednoduché zobecnit, jakým způsobem bude právní titul získán. V níže uvedené analýze nejčastěji vztahuji použitelné právní tituly vůči *IoT* zařízením, která jednak tvoří důležitý zdroj dat a jednak představují výzvu vzhledem k naplnění zásady zákonnosti.

V případě plnění smlouvy určuje článek 6, že takové zpracování musí být „***nezbytné** pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“* (zdůraznění doplněno). Vzhledem k podmínce nezbytnosti a rozsahu údajů, které zařízení *IoT* může zpracovávat, se tento právní titul uplatní jen v omezeném okruhu případů.[100] Zatímco tento právní důvod se uplatní např. pro zpracování platebních údajů a doručovací adresy při online nákupu, následná analýza *big data* bude, ze své podstaty, zaměřena na zasazení těchto údajů do širšího kontextu pro nalezení korelací, což je činnost, kterou nelze považovat za nezbytnou pro splnění smlouvy.[101]

Oprávněné zájmy se uplatní jako právní titul pro zpracování když, dle článku 6, „*zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů*

[99] Tamtéž, s. 58.
[100] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 241, ISBN 978-3-319-57959-7.
[101] INFORMATION COMMISSIONER'S OFFICE (ICO). B*ig data, artificial intelligence, machine learning and data protection,* s. 35, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě." Toto ustanovení lze rozdělit na tři podmínky, které je třeba splnit: 1) má správce (nebo třetí strana) oprávněný zájem?; 2) je zpracování nezbytné pro naplnění tohoto oprávněného zájmu (jinými slovy, neexistuje méně invazivní zpracování, které by vedlo ke stejnému cíli?); 3) převažuje tento oprávněný zájem správce nad zájmy a základními právy a svobodami subjektu údajů?[102] Tyto tři podmínky se dají shrnout jako nutnost provedení balančního testu mezi zájmy subjektu údajů a správcem, při zvážení výhod stejně jako rizik plynoucích pro obě strany z tohoto zpracování.[103] Slovní spojení „balanční test" je dále v práci používáno ve dvou významech. Jednak jde o výše zmíněný balanční test jako test proporcionality při rozhodnutí o tom, jestli byl naplněn právní titul pro zpracování, a to konkrétně titul oprávněných zájmů. Jednak se jako balanční test nazývá též posouzení slučitelnosti *dalšího* zpracování (též *compatability assessment*), v rámci kterého se posuzuje pět dílčích bodů dle čl. 6 (4). Hledání hranice bude v rámci obou balančních testů velice obtížné. Nizozemský dozorový úřad (*Autoriteit Persoonsgegevens*), ještě za účinnosti směrnicové úpravy, provedl šetření společnosti Google, která kombinovala údaje ze svých služeb (Gmail, YouTube, Google Search aj.) za účelem personalizace těchto služeb a reklam, webovou analytiku a pro získání informací pro další vývoj. To, co uživatel vyhledával skrze Google Search tak ovlivňovalo doporučování videí ze strany serveru YouTube apod.[104] V části věnované tvrzeným oprávněným zájmům správce dovodil dozorový úřad, že Google nedokázal dostatečně prokázat své oprávněné zájmy pro kombinování těchto údajů, stejně jako neprokázal, že nebylo možné užít jiné, méně invazivní metody, než je kombinování všech dat. Takovou méně invazivní metodou může být analýza chování vybrané skupiny uživatelů, kteří s tímto souhlasili. Dozorový úřad proto rozhodl, že vzhledem k povaze dat, rozdílnosti kombinovaných služeb a absenci adekvátního informování

[102] MOEREL, Lokke a Corien PRINS. Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things. *SSRN Electronic Journal,* s. 3 [online]. [cit. 2018-11-24]. DOI: 10.2139/ssrn.2784123. ISSN 1556-5068. Dostupné z: http://www.ssrn.com/abstract=2784123

[103] Blíže ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC [online]. [cit. 2018-11-25]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[104] DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS). *Investigation into the combining of personal data by Google: Report of Definitive Findings,* s. 28 [online]. 2013 [cit. 2018-11-25]. Dostupné z: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf

stejně jako možností *opt-outu,* nepřevážily oprávněné zájmy správce nad zájmy subjektů údajů, zpracování tedy neprošlo balančním testem a nebylo tak po právu.[105]

Při posuzování operačního systému Windows 10, který posílal telemetrická (diagnostická) data společnosti Microsoft, nizozemský dozorový úřad dovodil, že toto zasílání dat nenaplňovalo oprávněný zájem, když společnost nedostatečně rozlišila, která data a za jakým účelem potřebuje. Vzhledem k tomu, že šlo o plná telemetrická data, která mohla obsahovat citlivé údaje, a účely byly vymezeny široce (včetně zobrazování personalizovaných reklam v prohlížeči Edge a Windows Store), ani toto zpracování neprošlo balančním testem.[106] Zpracování telemetrických dat by bylo po právu, kdyby základní telemetrická data byla sdílena s Microsoftem za účelem udržování aktuálního softwaru a řešení chyb (např. počítač zašle každý týden informaci o tom, jaká je na něm nainstalovaná verze operačního systému, pokud je k dispozici verze novější, systém aktualizaci nabídne nebo rovnou provede), což naplňuje kritérium oprávněného zájmu, s tím že pro další využití by byl vyžadován souhlas.[107] Balanční test, mimo jiné, použil také ESD ve vlivném případu *Google Spain*[108], když uvedl, že *„s ohledem na možnou závažnost takového zásahu* [míněno zásahu do soukromí, který může způsobit indexace výsledků vyhledávání vztahující se k subjektu údajů] *je nutno konstatovat, že tento zásah nelze odůvodnit pouze hospodářským zájmem provozovatele vyhledávače na takovém zpracování.“*[109] Aplikací tohoto právního názoru na *IoT*, kde často bude skrze nositelnou elektroniku (*wearables)* či chytré doplňky domácnosti docházet k rozsáhlému zpracování osobních údajů, nebude ani v těchto případech možné zpracování odůvodnit pouhým ekonomickým zájmem správce.[110]

---

[105] Tamtéž, s. 96.

[106] DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS). *Summary of investigation report; Microsoft Windows 10 Home and Pro investigation by the Autoriteit Persoonsgegevens (Dutch DPA), August 2017: Public version,* s. 4 [online]. [cit. 2018-11-25]. Dostupné z: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf

[107] Tamtéž, s. 4.

[108] Rozsudek Soudního dvora ze dne 13. května 2014. Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD),Mario Costeja González, Věc C-131/12, ECLI:EU:C:2014:317. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A62012CJ0131

[109] Tamtéž, bod 81.

[110] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* s. 15 [online]. [cit. 2018-11-25]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Pro zpracování osobních údajů může mít společnost skutečně celou řadu legitimních důvodů, mezi které může patřit zabezpečování bezpečnosti zařízení či předcházení podvodům. Klíčové ovšem vždy bude posouzení, jestli je pro tyto legitimní důvody dané zpracování skutečně nezbytné a pokud ano, zda nepřevažují zájmy subjektu údajů.[111] Vzhledem k tomu, že toto posouzení bude často náročné, je vhodné jednak takový záměr konzultovat s dozorovým úřadem, jednak tam, kde je to žádoucí (tedy zejména v případech, kdy *big data* slouží jako podklad pro automatizované individuální rozhodnutí) ustanovit interní Etický výbor (*ethics committee* / *board*).[112]

Konečně lze využít také souhlasu. Dle článku 4, odstavce 11 je „*`souhlasem` subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů"*. Podobně jako u zásady transparentnosti je problémem skutečné dodržení informovanosti subjektů ohledně zamýšleného zpracování, a to vzhledem ke složitosti těchto procesů. Při získání souhlasu lze tak doporučit, aby se správce zaměřil na to, jaký konkrétní přínos může výsledná analýza mít pro uživatele (vůči obvyklé formulaci *„ (…) ke zlepšení našich službeb*" mohou být subjekty údajů netečné) a následně subjektům umožnit skutečnou volbu. Ohledně skutečné volby bude velice zajímavé sledovat, jak rozhodnou dozorové úřady ve stížnostech podaných organizací noyb, za kterou stojí Max Schrems, patrně nejznámější právní aktivista v oblasti ochrany osobních údajů.[113] Tyto stížnosti míří proti společnostem Google, Facebook, WhatsApp a Instagram (opět skrze Facebook, respektive Facebook Ireland Ltd.). Bez zacházení do podrobností těchto případů lze konstatovat, že ve všech těchto případech docházelo, alespoň dle stížností, různými způsoby k vynucení souhlasu; například aplikace Instagram po změně svých zásad ochrany osobních údajů nabídla uživatelům pouze dvě možnosti, a to souhlasit nebo smazat svůj účet, Google při aktivaci mobilního telefonu

[111] INFORMATION COMMISSIONER'S OFFICE (ICO). B*ig data, artificial intelligence, machine learning and data protection,* s. 33, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[112] Např. pro společnost Google jde o DeepMind Ethics & Society. Blíže: DEEPMIND. *DeepMind Ethics & Society* [online]. [cit. 2018-11-25]. Dostupné z: https://deepmind.com/applied/deepmind-ethics-society/

[113] NOYB - EUROPEAN CENTER FOR DIGITAL RIGHTS. *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook* [online]. [cit. 2018-11-25]. Dostupné z: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

nabídnul pouze možnost souhlasu se svými zásadami. Relevance těchto případů pro *big data* je zjevná, když obchodní model společností, které stojí na využití *big data*, je často nabídnutí služby zadarmo právě výměnou za možnost získávat o uživateli osobní údaje. Tento obchodní model funguje pouze při použití přístupu „*take it or leave it"*.[114] Dle stanoviska Pracovní skupiny ovšem GDPR článkem 7 (4) zajišťuje, aby „*se zpracování osobních údajů, pro které se žádá o souhlas, nemohlo přímo či nepřímo stát protiplněním smlouvy. Oba tyto zákonné základy pro zákonné zpracování osobních údajů, tj. souhlas a smlouva, nemohou být sloučeny a jejich hranice rozostřeny."*[115]

Ohledně souhlasu lze uzavřít, že při naplnění vyjmenovaných charakteristik souhlasu (tj. svobodný, konkrétní, informovaný a jednoznačný) je vhodným titulem pro „prvotní" zpracování v rámci *big data*. Ovšem při snaze data dále využít bude zpracování kolidovat se zásadou omezení účelu, jak popisuji dále v práci.

Dlouhodobě je ovšem dle mého názoru systém stojící na udělování velkého množství jednotlivých souhlasů pro každou službu, kterou jednotlivec používá, neudržitelný. Při předpokladu dalšího rozšíření chytrých doplňků by subjekt údajů čelil každý den výzvám k souhlasu, jejichž smysl by se tak vzhledem k četnosti zcela vyprázdnil. Domnívám se, že správným koncepčním řešením by mohla být vhodná kombinace praktik „*sticky policies"* a tvorby uživatelského *dashboardu*. S*ticky policies* se vztahují k technickému postupu, kdy jsou osobní údaje označeny metadaty, které označují, jak mají být využívány, respektive jaké preference s nimi uživatel spojil. Tato metadata by byla s osobními údaji nerozlučně spojena (odtud ono „sticky", tedy „lepkavé", v názvu) a každý správce či dále zpracovatel osobních údajů by tak osobní údaje obdržel vždy i s příslušnými metadaty. Pro každý přístup k těmto

[114] Kromě tohoto ultimáta dochází také k využívání celé řady psychologických triků, které reálně oslabují svobodu volby. Například Google v případě, kdy subjekt údajů vypíná personalizované cílení reklam, uživatelům sděluje, že tímto přijdou o možnost ztišit některé reklamy (*mute ads)*, aniž by vysvětloval, co tímto míní. Uživatelé se tak mohou obávat, že půjde o nemožnost ztišit hlasité reklamy na YouTube, nebo že pro příště nebudou moci ovlivnit zobrazování nevhodného obsahu v reklamách dětem. Nehledě na to, co ve skutečnosti spojení *mute ads* znamenalo, je toto omezení možnosti uživatele používat službu nad míru odpovídající nesdílení určitého typu osobních údajů neblahým trendem hodným pozornosti regulátora. Blíže k této problematice: FORBRUKERRÅDET - NORWEGIAN CONSUMER COUNCIL. Deceived by design [online]. [cit. 2018-11-25]. Dostupné z: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

[115] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro souhlas podle nařízení 2016/679 (WP259),* s. 8 [online]. [cit. 2018-10-29]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

datům by z technického hlediska bylo nutné vždy přistoupit nejdříve k přiloženým metadatům, na základě kterých by byla ověřena možnost vůbec přistoupit k samotným datům.[116] Technická řešení se mohou lišit, například pro zvýšení bezpečnosti lze místo klasické vztahu, kdy subjekt údajů předává osobní údaje přímo správci, mít vztah trojúhelníkový, kdy subjekt údajů předává správci zašifrované osobní údaje obsahující zmíněná metadata, s tím že pro zpracování musí správce dešifrovat data pomocí klíče, který mu poskytne, na základě ujištění ohledně splnění podmínek určených metadaty, důvěryhodná třetí strana (*trusted authority*).[117] Bez zacházení do dalších technických podrobností lze uzavřít, ze *sticky policies* umožňují efektivnější kontrolu využívání osobních údajů ze strany subjektu údajů a jsou tak vhodným nástrojem pro zpracování v rámci *big data*, stejně jako umožňují např. efektivnější výkon „práva být zapomenut".

Jako *dashboard* (česky též nástěnka či „palubní deska") je pak označováno přehledné vizuální zobrazení souhrnu určitých informací, které umožňuje uživateli rychle rozpoznat nejdůležitější údaje.[118] Nástěnka osobních údajů (*privacy dashboard*) pak zobrazuje pro určitou službu či vícero služeb souhrn využívání osobních údajů, informace o tom, které osobní údaje a jak jsou sbírány a zvolené preference uživatele.[119]

V situaci, kdy je uživatel denně žádán o souhlas se zpracováním osobních údajů, nemá čas a zřejmě ani motivaci seznamovat se s podmínkami jednotlivých služeb, stejně jako nutně brzy ztratí přehled o svých udělených souhlasech. Oproti tomu vytvoření „centrálního dashboardu", či „osobního cloudu"[120] by vedlo k tomu, že subjekt údajů by měl na jednom místě přehled o všech probíhajících zpracováních osobních údajů. Zároveň by mohl nastavit obecná pravidla pro různé druhy služeb, např. „pro služby umožňující mapovou navigaci chci

[116] NGUYEN, Carolyn a Jeffrey FRIEDBERG. A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy, s. 234. IN: O'HARA, Kieron, Michael WAIDNER a Mireille HILDEBRANDT. *Digital Enlightenment Yearbook 2013*. IOS Press, 2013. ISBN 978-1-61499-295-0.

[117] PEARSON, Siani a Marco CASASSA-MONT. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. *Computer* [online]. 2011, **44**(9), 60-68 [cit. 2018-11-26]. DOI: 10.1109/MC.2011.225. ISSN 0018-9162. Dostupné z: http://ieeexplore.ieee.org/document/5959137/

[118] FEW, Stephen. Dashboard Confusion Revisited. *Perceptual Edge* [online]. [cit. 2018-11-26]. Dostupné z: https://www.perceptualedge.com/articles/visual_business_intelligence/dboard_confusion_revisited.pdf

[119] Příkladem je *dashboard* poskytovaný společností Google: https://myaccount.google.com/dashboard?pli=1

[120] NGUYEN, Carolyn a Jeffrey FRIEDBERG. A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy, s. 239. IN: O'HARA, Kieron, Michael WAIDNER a Mireille HILDEBRANDT. *Digital Enlightenment Yearbook 2013*. IOS Press, 2013. ISBN 978-1-61499-295-0.

sdílet lokalizační údaje pouze při využívání navigace“. Subjekt údajů by tedy své preference mohl nastavit obecným způsobem, stejně jako by mohl efektivněji vykonávat např. právo na přenositelnost či „právo na zapomenutí“ díky centralizovanému přístupu a využití *sticky policies.* Zároveň by mohl veškeré nastavení provést zvolením jednoho z již existujících profilů nastavení, např. pokyn „nesdílet více údajů, než je nezbytně nutné“ by se následně projevil ve všech službách, které jedinec využívá. Díky využití metadat by se případná změna ve volbě sdílení osobních údajů projevila téměř okamžitě napříč všemi službami. Při existenci takového jednotného místa správy osobních údajů lze také uvažovat o automatizaci výkonu práva na přenositelnost tím způsobem, že by se např. historie vyhledávání sdílela mezi jednotlivými prohlížeči či oblíbené trasy mezi navigačními aplikacemi. Rubinstein pro obdobný přístup[121] navrhuje, aby Evropská unie podpořila výzkum v této oblasti, přinesla větší legislativní oporu pro *sticky policies* a konečně, aby podpořila společnosti, které s tímto přístupem začnou experimentovat.[122] Právní podporou tohoto přístupu může být možnost vytvoření kodexu chování týkající se této „*kategorie správců*“ (čl. 40). Tento samoregulační prvek nabývá v režimu GDPR větší důležitosti[123], když směrnicová úprava nestanovovala konkrétní důsledky přijetí kodexů a možnosti jejich vymáhání.[124] Komise může tento postup dále podpořit postupem dle čl. 40 (9), který vede k všeobecné platnosti schváleného kodexu chování v rámci Unie.[125] Pozitivně se k obdobnému konceptu[126] vyjádřil také Evropský inspektor ochrany

[121] Rubinstein mluví o *personal data services* (PDS), což vychází ze spíše ekonomické koncepce, podle které tento „osobní cloud“ má sloužit k signalizování spotřebitelských preferencí (vůči společnostem).

[122] RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law,* s. 86[online]. **3**(2) [cit. 2018-11-01]. Dostupné z: https://academic.oup.com/idpl/article/3/2/74/709082#12469607

[123] Jde o jeden z prvků, jimiž lze doložit, že správce plní příslušné povinnosti (čl. 24(3)), že dodržuje požadavky na zabezpečení osobních údajů (čl. 32(3)). Dále se dodržení kodexu řádně zohlední při posuzování dopadu operací zpracování, zejména pro posouzení vlivu na ochranu osobních údajů (čl. 35 (8), vzhledem k posuzování vhodných záruk při předávání do zahraničí (čl. 40(3)) a bude též zohledněn při rozhodování o udělení pokuty a její případné výši (čl. 83(2), pís.j).

[124] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář.* Praha: Leges, 2018, s. 305, ISBN 978-80-7502-288-2.

[125] RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law,* s. 87[online]. **3**(2) [cit. 2018-11-01]. Dostupné z: https://academic.oup.com/idpl/article/3/2/74/709082#12469607

[126] Tentokrát jde o koncept *personal data store* (PDS), což označuje „datový trezor“, ve kterém jsou uloženy osobní údaje. Tento pohled se zaměřuje více na bezpečné sdílení dat (a jejich možnou monetizaci).

osobních údajů[127], stejně jako britský dozorový úřad[128]. Zároveň je ovšem třeba vnímat zvýšené bezpečnostní riziko vzhledem ke shromáždění všech osobních údajů na jednom místě, stejně jako znovu otevírá diskuse ohledně možnosti monetizace osobních údajů ze strany subjektu osobních údajů, což by vedlo k přehodnocení právního přístupu a k zacházení s osobními údaji jako s majetkem.[129]

3.2.4 Zásada omezení účelu a zásada omezení uložení

Půvab analýzy velkých datových setů tkví v kontinuálním používání nových metod, které v důsledku vedou k nalézání překvapivých vztahů a korelací mezi různými údaji datového setu.[130] Rozvoj těchto metod vede v této oblasti k přesunu pozornosti z úpravy sběru dat k úpravě následného využití dat, zejména pak k možnosti opětovného využití dat za jiným účelem.[131] Zájem správců o využití dat tímto způsobem ovšem naráží na zásadu omezení účelu, když GDPR stanovuje, že *„zejména je zapotřebí, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní a aby byly stanoveny v okamžiku shromažďování osobních údajů.“*[132] Následně je, v případě, kdy je splněn účel zpracování,

---

[127] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data,* s. 14 [online]. 19.11.2015 [cit. 2018-10-28]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[128] INFORMATION COMMISSIONER'S OFFICE (ICO). B*ig data, artificial intelligence, machine learning and data protection,* s. 84-85, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[129] Příkladem takového přístupu je např. koncept kavárny Shiru, která současně funguje v Japonsku a USA. Za kávu se neplatí penězi, ale osobnímu údaji. Po vyplnění formuláře jsou návštěvníkům zobrazovány personalizované reklamy na okolo rozmístěných obrazovkách. Dle: FRANKEL, Joseph. One Coffee? Your Total Is Some Personal Data. New York Magazine - Intelligencer [online]. 2018 [cit. 2018-11-26]. Dostupné z: http://nymag.com/intelligencer/2018/08/shiru-cafs-offer-students-free-coffee-for-harvested-data.html

[130] Příkladem může být (zpětná) analýza hledání klíčových slov v internetových vyhledávačích, která umožňuje badatelům odhadnout vedlejší efekty při užívání dvou různých léků (tedy pokud statisticky významná skupina uživatelů nejdříve vyhledává určité léky a následně ve větší míře vyhledává daný symptom, může jít o důsledek negativní interakce těchto léků). Podobně užitečná analýza může vzejít pro určení efektů užívání nezákonných látek.
Dle: YOM-TOV, Elad a Shaul LEV-RAN. Adverse Reactions Associated With Cannabis Consumption as Evident From Search Engine Queries. *JMIR Public Health and Surveillance* [online]. 2017, **3**(4) [cit. 2018-10-30]. DOI: 10.2196/publichealth.8391. ISSN 2369-2960. Dostupné z: http://publichealth.jmir.org/2017/4/e77/

[131] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

[132] Recitál 39, Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

správce povinen údaje zlikvidovat (čl. 5 (1), pís. e), čemuž analogicky odpovídá právo subjektu údajů (čl. 17 (1), pís. a). Tato úprava je pak zhmotněním zásady omezení uložení.[133]

Při posouzení možnosti povolení dalšího zpracování vyjděme nejprve z preambule GDPR. Recitál 50 povoluje za určitých podmínek zpracování osobních údajů pro jiné účely, než pro které byly původně shromážděny. Zásada omezení účelu je převzatá z předchozí směrnicové úpravy[134], můžeme tak vyjít i z příslušeného stanoviska WP29[135], ve kterém se uznává, že povolení dalšího, odlišného použití osobních údajů přináší výhody[136] a kde jsou vyloženy principy posouzení možnosti takového dodatečného zpracování. Klíčové principy pro posouzení vychází v rámci současné úpravy z textu recitálu 50 a článku 6, odstavce 4 s tím, že obecně se přípustnost zpracování, dle názoru ICO, posoudí dle férovosti.[137] Můžeme shrnout, že GDPR předvídá, s přihlédnutím k výše zmíněným principům, čtyři situace, za kterých je další zpracování umožněno. Jde o situace, kdy 1) další zpracování je založeno na souhlasu subjektu údajů; 2) další zpracování je zpracováním pro účely archivace ve veřejném zájmu, pro účely historického výzkumu či pro statistické účely a probíhá v souladu s čl. 89 (1); 3) další zpracování je povoleno právem EU nebo členského státu, které se na správce vztahuje a které představuje v demokratické společnosti nutné a přiměřené opatření k zajištění jednoho z důležitých veřejných cílů stanovených v čl. 23 (1) nebo 4) nový účel je slučitelný s původním účelem a slučitelnost byla zjištěna na základě provedeného posouzení slučitelnosti dle čl. 6 (4).[138]

---

[133] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 60, ISBN 978-80-7554-097-3.

[134] *„Členské státy stanoví, že osobní údaje musejí být: (…) b) shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Další zpracování pro historické, statistické nebo vědecké účely není považováno za neslučitelné, pokud členské státy poskytnou vhodná ochranná opatření; (…).“* Článek 6, Směrnice 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

[135] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation (WP 203)* [online]. [cit. 2018-10-29]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[136] Tamtéž, s. 4.

[137] INFORMATION COMMISSIONER'S OFFICE (ICO). B*ig data, artificial intelligence, machine learning and data protection,* s. 38, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[138] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 141 – 144, ISBN 978-80-7598-068-7.

První možnost, tedy zajištění souhlasu subjektů údajů s dalším zpracováním, je pro využívání *big data* z právního hlediska plně dostupná (možnost získání předchozího dostatečně širokého souhlasu s dalším využíváním dat je pro účely *big data* ovšem reálně omezena, když souhlas musí být mj. konkrétní a informovaný, zatímco budoucí metody analýzy nemusí být toho času známy ani správci). Postup získání souhlasu pro každou další změnu účelu, byť právně vyhovující, je velice nepraktický[139], když by správce musel pravidelně získávat souhlasy od všech dotčených subjektů údajů, což je při objemných datových setech v podstatě nemožné. Každá změna účelu by tak vedla ke zmenšení datového setu, správce by musel poměřovat předpokládané pozitivní účinky nového účelu zpracování a s tím spojených analýz s negativními účinky ve formě zmenšení datového setu. Tento postup by tudíž tvořil překážku pro další inovace, s tím že ani z pohledu subjektu údajů nemusí být ideální, vzhledem k tomu, že by se tímto ještě zvýšil počet souhlasů, které se od jednotlivců denně vyžadují. Pracovní skupina WP29 mluví o *„únavě z klikání"*, která nastává v případech, kdy se uživatelé setkávají s mechanismy souhlasu příliš často – důsledkem je také bezmyšlenkovité potvrzování všech žádostí o souhlas[140], nebo naopak ignorování těch žádostí, které není nutné bezprostředně potvrdit. Tato možnost tedy v souhrnu není pro další vývoj *big data* řešením, jak již bylo naznačeno i v předcházející části.

Druhá možnost vyplývá zejm. z článku 89, na zpracování *big data* se ovšem nevztahuje, přestože mluví o zpracování *„pro statistické účely".* Statistickými účely se v souladu s celkovým vyzněním a účelem článku 89 totiž, dle některých autorů, nemyslí statistické účely sloužící pro podporu podnikání.[141] Jiní autoři dovozují, že tato výjimka uplatní i na *big data*, když sousloví

[139] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

[140] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro souhlas podle nařízení 2016/679 (WP259),* s. 18, [online]. [cit. 2018-10-29]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

[141] Např. dle NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 504, ISBN 978-80-7598-068-7.

„*statistické účely"* není v předpise blíže definováno a může být tedy vykládáno šířeji[142] tak, aby zahrnovalo různorodé zpracování označované souhrnně jako *big data.* Článek 89 v druhém odstavci obsahuje možnost členských států stanovit odchylky od práv subjektů údajů, recitál 156 spolu s recitálem 162 pak určuje, že vhodné záruky při statistickém zpracování určí členské státy.[143] Tato ustanovení dle některých autorů ukazují na záměr předpisu umožnit prolomení zásady omezení účelu v těchto případech zpracování (*big data*) a jsou tedy argumentem pro možnost využití této výjimky.*[144]* Bez ohledu na to, zda pod kategorii statistických účelů podřadíme zpracování *big data*, formulace na konci recitálu 162 využitelnost takového postupu výrazně znesnadňuje[145], když výsledek statistického zpracování spadajícího pod tuto výjimku nemá být použit „*na podporu opatření nebo rozhodnutí týkajících se konkrétní fyzické osoby"*, což bude ovšem často důvodem pro zapojení postupů *big data*. Tato výjimka se tedy na *big data* neuplatní, respektive její případné uplatnění s sebou nese výrazné omezení.

Ani třetí možnost není pro účely dodatečného zpracování údajů v *big data* využitelná, když takové zpracování nenaplňuje znaky vymezené článkem 23, odstavcem 1 GDPR (ten zmiňuje např. národní bezpečnost, obranu nebo ochranu nezávislosti soudnictví a soudních řízení) a zejména pak nesplňuje podmínku nezbytnosti upravenou týž článkem.

Poslední možnou situací, kterou GDPR předvídá, je slučitelnost nového účelu s původním účelem, k jehož zjištění se provede posouzení slučitelnosti (které by pak měl správce v souladu se zásadou odpovědnosti archivovat).[146] Pro posouzení slučitelnosti musí správce osobních údajů vzít v potaz pět faktorů, které, jak již bylo řečeno výše, vychází z článku 6, odstavce 4.

[142] MAYER-SCHÖNBERGER, Viktor a Yann PADOVA. Regime Change? Enablig Big Data through Europe`s new data protection regulation. *The Columbia Science & Technology Law Review*, s. 326, [online]. **17** [cit. 2018-11-15]. Dostupné z: http://stlr.org/download/volumes/volume17/SchonbergerPadova.pdf

[143] *„Členské státy by měly stanovit vhodné záruky týkající se zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely."*

[144] MAYER-SCHÖNBERGER, Viktor a Yann PADOVA. Regime Change? Enablig Big Data through Europe`s new data protection regulation. *The Columbia Science & Technology Law Review*, s. 327, [online]. **17** [cit. 2018-11-15]. Dostupné z: http://stlr.org/download/volumes/volume17/SchonbergerPadova.pdf

[145] ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* [online]. **47**(2), s. 1008, [cit. 2018-11-15]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646#

[146] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 141, ISBN 978-80-7598-068-7.

Zahrnutí tohoto posouzení (balančního testu, *compatibility assessment)* přímo do textu GDPR je jedním z důležitých úspěchů nové právní úpravy a výsledkem kompromisního řešení mezi Komisí a Evropským parlamentem.[147] Jmenovitě jde o posouzení: a) vazby mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování; b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem; c) povahy osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle článku 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10; d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů; e) existence vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.

Dle mého názoru je právě tato možnost vhodným základem pro umožnění zpracování *big data.* V tomto případě je nutný, slovy WP29, důkladný, vyrovnaný a flexibilní přístup k posouzení slučitelnosti, které má odpovídat užití v moderní společnosti.[148] Domnívám se, že provedení balančního testu, tedy v zásadě posouzení, zda-li je další zpracování *fér* (jak navrhuje britský ICO) a odpovídá očekáváním subjektů údajů[149], odpovídá charakteru *big data* a je dostatečně

[147] FORGÓ, Nikolaus, Stefanie HÄNOLD a Benjamin SCHÜTZE. The Principle of Purpose Limitation and Big Data. IN CORRALES, Marcelo, Mark FENWICK a Nikolaus FORGÓ. *'New Technology, Big Data and the Law*. Springer Singapore, 2017, s. 17-42. ISBN 978-981-10-5038-1.

[148] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation (WP 203)*, s. 40, [online]. [cit. 2018-10-29]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[149] Očekávání subjektů údajů je nutné posuzovat případ od případu; držitelé věrnostní karty určitého nákupního řetězce skutečně očekávají, že jejich nákupní chování je podrobeno analýze, na základě které jsou jim např. doručeny pro ně relevantní slevové kupóny nebo které pomáhá řetězci upravovat svou cenovou politiku. Ovšem zvažme příklad, který oprávněně získal pozornost médií i WP29. Americká síť obchodů Target na základě spojení veřejných registrů a informací z věrnostních karet určila, jakým způsobem se mění nákupní chování těhotných žen, respektive v jakém měsíci těhotenství ženy kupují určité výrobky. Tento algoritmus umožnil společnosti zasílat ženám, u kterých bylo určeno „vysoké skóre pravděpodobnosti těhotenství" personalizované nabídky k dalším relevantním produktům. Do pozornosti médií se případ dostal po stížnostech otce, kterému se nelíbilo, že společnost ponouká jeho dceru k těhotenství, když jí do schránky chodí ve zvýšené míře nabídky na dětské postýlky apod. Následně vyšlo najevo, že dcera je skutečně těhotná, jak Target správně odhadl skrze změny jejího nákupního chování. WP29, aniž by zmiňovala konkrétní reálie, ilustruje na tomto případě *nefér* další zpracování dat, když takový stupeň predikce zákazník nemůže rozumně očekávat. Jinými slovy, tento případ by balančním testem zjevně neprošel.
Dle: DUHIGG, Charles. How Companies Learn Your Secrets. *New York Times* [online]. [cit. 2018-11-01]. Dostupné z: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0
Dále dle: ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation (WP 203)*, s. 61, [online]. [cit. 2018-10-29]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

flexibilní a technologicky neutrální na to, abychom mohli učinit závěr, že v tomto bodě je právní úprava nejen odpovídající nárokům *big data*, ale také odolná budoucím změnám (*futureproof).* Zároveň tento přístup nastoluje rovnováhu mezi ekonomickými přínosy *big data* a ochranou práv jednotlivců. Na rozdíl od některých autorů proto nepovažuji za nutné ani vhodné pro případy zpracování *big data* např. předpokládat souhlas s dalším zpracováním[150], když tato kazuistika drolí právní úpravu a taková výjimka by narušila konstrukci souhlasu dle GDPR, a v důsledku by dost možná přivedla více otázek než odpovědí (např. vzhledem k obtížnosti definice *big data,* a tedy k obtížnému určování rozsahu dané výjimky). Podobně lze odmítnout i názory podporující úplné zrušení zásady omezení účelu, která je popisována jako marná snaha zvrátit nevyhnutelný pokrok.[151] Zásada omezení účelu je navíc zakotvena i v Listině základních práv Evropské unie[152], konkrétně v jejím článku 8, odstavci 2. Pokud by zároveň nedošlo ke změně Listiny, musí Obecné nařízení zásadu převzít[153], což příznivci opuštění zmíněné zásady obvykle opomíjejí.

3.2.5 Zásada minimalizace údajů

Zásada minimalizace údajů[154] je také jedním ze základů evropské ochrany osobních údajů, ovšem oproti výše zmíněné zásadě omezení účelů není v Listině základních práv Evropské unie explicitně zmíněna, což umožňuje větší flexibilitu při jejím užívání.[155] Možný rozpor s touto zásadou pramení ze samé podstaty *big data.*[156] Aplikace zásady směřuje ke stavu, kdy účelu

[150] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

[151] *„These concepts rely on the old idea that it is possible to decide on the purposes of a certain data processing beforehand (…) [and] therefore start from the wrong premise. They are trying to hold off the future, which is impossible to do. It is against the technical imperative. The world will be about big data and the internet of things with sensors collecting data just for the sake of collecting the data (…).“*
Dle MOEREL, Lokke. *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof,* s. 53-54, [online]. [cit. 2018-11-13]. Dostupné z: https://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf

[152] Listina základních práv Evropské unie (Charta základních práv EU), vyhlášená pod č. 111/2009 Sb. m. s.

[153] Srov. posouzení SDEU v případech Digital Rights Ireland (ECLI:EU:C:2014:238 9) a Volker und Markus Schecke a Eifert (body 44-47; ECLI:EU:C:2010:662).

[154] Vyjádřena zejména v článku 5, odstavci 1, písmeni c, recitálu 39 a článku 25 GDPR.

[155] ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* [online]. **47**(2), s. 1009, [cit. 2018-11-15]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646#

[156] Dle přiléhavé definice George Dysona: „*big data* je to, co nastane, když náklady na uchování informací jsou nižší, než náklady na jejich odstranění.“ Dle: INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial*

zpracovávání bude dosaženo s použitím co nejužší skupiny osobních údajů.[157] Setkáváme se tak s názorem, že *„analýza dat v rámci Big Data projektů a zásada minimalizace dat při jejich zpracování jdou zásadně proti sobě, a proto tato zásada bude porušena v každém případě, kdy v rámci analýzy dat budou zpracovávány osobní údaje.“*[158] Takovýto striktní výklad, v podstatě zakazující užití *big data* pro data obsahující osobní údaje, by měl značně negativní důsledky pro konkurenceschopnost evropských společností, stejně jako pro další rozvoj inovací. Ostatně právě v režimu úpravy ochrany osobních údajů někteří autoři spatřují důvod úspěchu amerických internetových společností ve srovnání s jejich evropskými protějšky[159], s tím že internetoví titáni jako Amazon, Google či Facebook postavili svůj obchodní model zejm. na sběru a využívání *big data*.[160] Pokud je výhodou přístupu *big data* nacházení různých korelací mezi datovým setem, bude tento přístup fungovat tím lépe, čím více dat bude mít k dispozici. Zároveň je vlastností analýzy *big data* to, že správce často dopředu neví, co vlastně bude výsledkem analýzy dat, což dále komplikuje určení přesného účelu zpracování a tomu odpovídajících potřebných (osobních) údajů.[161] Řada společností, jejichž obchodní model je založen na analýze *big data*, se pak nejprve zabývá získáním co nejširšího datového setu, a následně hledá možnosti dalšího komerčního využití.[162]

intelligence, machine learning and data protection, s. 41, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[157] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018, s. 7, ISBN 978-80-7552-248-1.

[158] PFEFFER, Jan a Hana GAWLASOVÁ. Big Data právním pohledem. Hospodářské noviny [online]. [cit. 2018-10-29]. Dostupné z: https://ihned.cz/c1-60126320-big-data-pravnim-pohledem

[159] V tomto ohledu se mluví o tzv. „*Evropského paradoxu*“, což je situace, kdy na jedné straně patří státy Evropské unie k vědecky nejpokročilejším státům světa, přesto nejsou schopny vyrovnat se v IT inovacích americkým, případně čínským společnostem. Dle: ZARSKY, Tal. The Privacy–Innovation Conundrum. Lewis & Clark Law Review, s. 156 [online]. **19**(1) [cit. 2018-10-29]. Dostupné z: https://law.lclark.edu/live/files/19418-lcb191art4zarskyfinalpdf

[160] CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

[161] PFEFFER, Jan a Hana GAWLASOVÁ. Big Data právním pohledem. Hospodářské noviny [online]. [cit. 2018-10-29]. Dostupné z: https://ihned.cz/c1-60126320-big-data-pravnim-pohledem

[162] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 238, ISBN 978-3-319-57959-7.

Dle některých autorů by trvání na zásadě minimalizace údajů znehodnotilo postupy spojené s *big data* natolik, že by následně nemohly přinést očekávané výsledky[163], z čehož tedy dovozují, že je nutné tento princip neuplatňovat na *big data*, a to s přihlédnutím k tomu, o jaké výhody bychom se mohli připravit.[164] Zde platí výše zmíněné; tato kazuistika by vedla k drolení a nekoncepčnosti právní úpravy, která by místo technologické neutrality ustupovala různým novým trendům. Následné objevení určité neobvyklé korelace nemůže zpětně odůvodnit zpracování a shromažďování osobních údajů.[165] Přestože je pro správce, zejména v případech *big data*, jistě snadnější vydat se cestou maximalizace shromažďovaných údajů, tento přístup není v ničem odůvodněný a jasně odporuje zásadě minimalizace údajů.

Argumentem proti dalšímu uplatňování zásady minimalizace údajů je také to, že v případech *big data* není pro subjekty údajů zásada smysluplná, když subjekty vzápětí o sobě vytvoří nová data k analýze.[166] Ani tento argument dle mého názoru neobstojí. Důvodem k opuštění jednoho ze základních principů ochrany osobních údajů nemůže být fakt, že lidé v běžném životě o sobě generují stále větší množství dat (jak bylo popsáno v úvodní části); právě naopak, tato okolnost volá po o to důslednějším principu aplikace principu minimalizace údajů ze strany správců.[167] Argument je navíc vnitřně rozporný; přestože o sobě subjekty údajů vytvoří *další* data, tato další data budou také podléhat zásadě minimalizace údajů. Konkrétně tedy

[163]RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law,* s. 78 [online]. **3**(2) [cit. 2018-11-01]. Dostupné z: https://academic.oup.com/idpl/article/3/2/74/709082#12469607

[164] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28], s. 8, Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[165] INFORMATION COMMISSIONER'S OFFICE (ICO). B*ig data, artificial intelligence, machine learning and data protection,* s. 41, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[166] RHOEN, Michiel a Qing Yi FENG. Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science. *International Data Privacy Law*. 2018, **8**(2), 140-159. DOI: 10.1093/idpl/ipy005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article/8/2/140/5045225

[167] Je pak otázka, jestli má být ochrana osobních údajů v tomto rozsahu regulována, pokud by o ni lidé nestáli. Zarsky se domnívá, že lidé se kontroly nad svými osobními údaji vzdávají velice snadno, čímž ukazují, že je buďto kontrola nad svými údaji nezajímá, nebo že svým údajům přisuzují jen zanedbatelnou ekonomickou hodnotu. Není pak ochrana osobních údajů v těchto podmínkách výrazem paternalismu státu (respektive EU)? Za současného stavu panuje nejspíše shoda nad tím, že lidé mají o ochranu svých osobních údajů zájem, je ale skutečně možné, byť tomu dle mého názoru prozatím nic nenasvědčuje, že se tento zájem vytratí s tím, jak se promění individuální i společenské hodnoty. Dle: ZARSKY, Tal. Transparent Predictions. *University of Illinois Law Review,* s. 1544 [online]. 2013, 2013(4), 1503-1570 [cit. 2018-11-26]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324240

nelze např. dovodit nutnost opuštění zmíněné zásady pro osobní údaje vzniklé při procházení webových stránek na základě tvrzení, že subjekt údajů stejně bude dále procházet množství dalších, odlišných webových stránek. Jinými slovy zde není důvod pro to, aby faktický stav generování velkého množství dat vedlo k negaci zásady minimalizace údajů, ale právě naopak, tento stav vede k potvrzení její důležitosti.

Pro úplnost je třeba dále uvést, že GDPR určuje, že v případech, které spadají pod zpracování *„pro statistické účely"* může být tato zásada naplněna pseudonymizací.[168] Jak bylo uvedeno výše, zpracování *big data* pod statistické účely podřadit nelze, respektive lze jen se značnými obtížemi a omezeními.

Přestože minimalizace údajů skutečně může zabránit některým druhům zpracování, a tedy i dosažení některých inovací, je to také základní princip ochrany osobních údajů a stejně tak zabrání mnohým negativním důsledkům. V případě aplikace této zásady je třeba hledat rovnováhu. Vzhledem k rozmanitosti a složitosti zpracování není možné vynést kategorický soud o tom, jaké údaje má správce zpracovávat, ale je třeba posuzovat jednotlivé zpracování případ od případu. Zejména je vhodné omezit shromažďování plných, analytických údajů a místo nich použít pouze binární hodnoty.[169] Aplikace na chytré parkování si má při placení vystačit s tím, jestli je na účtu (vytvořeném v aplikaci) dostatek peněz (ano/ne, tedy binární hodnota), nikoliv kolik přesně je tam peněz, jakým způsobem byly peníze doplněny, v kolik hodin, kde apod. I v rámci *big data* musí správce určit způsob uchovávání dat, stejně jako musí hledat možnosti využívání co nejmenšího možného okruhu údajů pro hledání korelací.[170]

[168] Dle článku 89, odstavce 1 GDPR.

[169] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, s. 57, [online]. [cit. 2018-11-01]. Dostupné z: https://arxiv.org/pdf/1512.06000.pdf

[170] BUTTERWORTH, Michael. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review*, s. 260 [online]. **34**(2), 257-268 [cit. 2018-11-14]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S026736491830044X

3.2.6 Zásada transparentnosti

Řečeno slavným úslovím soudce Brandeise: *„sunlight is the best disinfectant“.* Transparentnost je v případě *big data* obzvlášť důležitá, když tyto postupy umožňují získat personalizované výsledky analýzy, které u subjektů údajů vyvolávají pocit sledování ze strany velkého či malého Bratra.[171] Nedodržení této zásady vede ke stavu, kdy subjekty údajů neví, jakým způsobem jsou jejich data analyzována, které údaje analýze vůbec podléhají a případně jaké profily byly na základě dat o jedinci vytvořeny.[172] Tento nežádoucí stav v současné době trvá, neboť řada správců používá vágních a nejasných pojmů.[173] Příkladem může být informování subjektů o využití jejich osobních údajů pro *„zlepšení kvality našich služeb“* či k *„ochraně našich práv“* bez dalšího upřesnění.

I v tomto případě můžeme zopakovat, že dostát této zásadě nebude v případě *big data* jednoduché, když jde o velice složité procesy, o nichž mají subjekty údajů jen omezené povědomí a které se dají vysvětlit jen s velkými obtížemi.[174] Je zjevné, že, technicky třeba i přesné, zato však zahlcující vysvětlení, které je rozvláčně a složitým jazykem psané přes mnoho stran nenaplňuje účel, který zásada transparentnosti sleduje.[175] V tomto ohledu je zejména při takto složitých procesech téměř nutností využít vícevrstvé (*layered)* informování, případně

[171] Někteří autoři rozlišují mezi „velkým Bratrem“ ve smyslu státního sledování a „malým Bratrem“ ve smyslu sledování ze strany soukromých entit. Dle: ZARSKY, Tal. Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society. *University of Miami Law Review* [online]. 2004, **58**(4) [cit. 2018-11-27]. Dostupné z: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1398&context=umlr

[172] DATATILSYNET. *Big Data - privacy principles under pressure,* s. 27, [online]. 2013 [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/big-data-engelsk-web.pdf

[173] CPVP - COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE. *Rapport Big Data*, s. 42 [online]. [cit. 2018-11-25]. Dostupné z: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf

[174] LEONARD, Peter. Customer data analytics: privacy settings for ‘Big Data’ business. *International Data Privacy Law*[online]. 2014, **4**(1), 53-68 [cit. 2018-10-29]. DOI: 10.1093/idpl/ipt032. ISSN 2044-3994. Dostupné z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipt032

[175] Jen četba „zásad ochrany osobních údajů“ (*privacy policies*) webů, které navštíví průměrný uživatel internetu by zabrala přibližně 30 pracovních dní ročně.
Dle: MCDONALD, Aleecia a Lorrie CRANOR. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, s. 17 [online]. [cit. 2018-11-16]. Dostupné z: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

využít přehledných, standardizovaných ikon.[176] U vícevrstvého informování je vhodnou praktikou, která bezezbytku naplňuje účel a smysl právní normy, nabídnout první, nejobecnější „vrstvu“ ve „stravitelné formě“, jakou je například komiks či video. Přestože správci mohou argumentovat, že jejich techniky zjednodušit do formy videa není možné, je legitimní požadovat, aby společnosti inovativní ve zpracování dat byly inovativní také v informování subjektu údajů o tomto zpracování.[177] Navíc není záměrem, aby správci podrobně vysvětlovali technický způsob zpracování, ale spíše aby vysvětlili účel takového zpracování.[178] Za vhodný příklad ilustrující tyto možnosti lze považovat přístup britské veřejnoprávní stanice Channel 4[179], které se podařilo přehledným a stručným videem dostatečně vysvětlit i složitější praktiky jako šifrování dat či využívání personalizovaných reklam.

Big data z definice spoléhají na různorodost dat (*variety)*, při zpracování tedy budou osobní údaje často získány skrze chytré telefony, nebo skrze jiné zařízení spadající pod kategorii *IoT*. V případě chytrých telefonů patří mezi vhodné postupy informování subjektů sdílení základních informací o zpracování ještě před stáhnutím aplikace (např. v popisu aplikace na Google Play či App Storu), doručování příslušných informací a/nebo žádostí o souhlas tzv. *just-in-time*, tedy ve chvíli, kdy uživatel chce spustit funkci závisející na zpracování dodatečných údajů (např. v aplikaci na vyhledávání vlakových spojení může uživatel využít funkce nalezení nejbližší vlakové zastávky; až ve chvíli, kdy uživatel tuto funkci skutečně chce využít má

[176] Užití těchto ikon předvídá článek 12, odstavec 7 GDPR, s tím že ke stanovení podrobnějších pravidel je zmocněna dle článku 92 EK; odpovídající prováděcí předpisy ovšem prozatím nebyly přijaty. Ze soukromých iniciativ lze zmínit zejména sady ikon Mozzilla či Disconnect Privacy Icons. Ani jedna z těchto sad prozatím není šířeji užívána.
Dle: EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, s. 45, [online]. [cit. 2018-11-01]. Dostupné z: https://arxiv.org/pdf/1512.06000.pdf
PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 146, ISBN 978-80-7502-288-2.
[177] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data,* s. 14 [online]. 19.11.2015 [cit. 2018-10-28]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf
[178] INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial intelligence, machine learning and data protection,* s. 66-67, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
[179] CHANNEL 4. *Your Data* [online]. [cit. 2018-11-25]. Dostupné z: https://www.channel4.com/4viewers/your-data

aplikace požadovat přístup k lokalizačním údajům) či zmíněné využití vícevrstvého informování.[180] V případě chytrých telefonů lze uzavřít, že tyto principy jsou dnes samozřejmou součástí vývoje aplikací, kdy takové nastavení vyžadují i poslední verze nejrozšířenějších mobilních operačních systémů. Na druhé straně je takový jednotný přístup a s tím související informovanost subjektu údajů nižší u *IoT*. Vzhledem k tomu, že z povahy *IoT* plyne jejich konektivita, je vhodným přístupem využívat chytré telefony pro doručování informací obdobně, jako v případě aplikací fungujících pouze skrze chytrý telefon.

Pokud bude chtít správce využít údaje k novému účelu, který neprošel balančním testem a nebude moci využít ani anonymizace, bude muset opětovně informovat subjekt údajů, respektive jej žádat o souhlas.[181] Tam, kde má dojít k anonymizaci, se stále jeví být vzhledem k celkové koncepci právní úpravy a vzhledem ke konstrukci práva na informační sebeurčení správné, aby správce dopředu informoval o možném dalším využití i anonymizovaných údajů, byť k tomu nemá právní povinnost.[182]

Společnosti zabývající se analýzou *big data* odpovídají často svým charakterem tzv. start-upům, do kterých v případě úspěchu obvykle vstupuje větší společnost. Je vhodné, dle britského ICO dokonce v některých případech nutné, informovat subjekty údajů v případech, kdy správce údajů (společnost) přejde pod kontrolu jiné společnosti nebo dojde k její fúzi. I přesto, že se v těchto případech nebude nic měnit na způsobu zpracování osobních údajů, by měl správce o tomto opětovně ujistit subjekty údajů a zároveň by je měl informovat o tom, jestli, respektive za jakých podmínek, mají možnost se svými daty nepřejít pod novou společnost.[183]

[180] INFORMATION COMMISSIONER'S OFFICE (ICO). *Privacy in mobile apps: Guidance for app developers,* s. 10-17 [online]. [cit. 2018-11-25]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

[181] INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial intelligence, machine learning and data protection,* s. 68-69, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[182] ROUVROY, Antoinette. "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. *Council of Europe, Directorate General of Human Rights and Rule of Law,* s. 30 [online]. [cit. 2018-11-16]. Dostupné z: https://works.bepress.com/antoinette_rouvroy/64/

[183] INFORMATION COMMISSIONER'S OFFICE (ICO). *Data sharing code of practice,* s. 22 [online]. [cit. 2018-11-25]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Nakonec lze uzavřít, že dodržování transparentnosti je také v zájmů správců, když, alespoň teoreticky, transparentnost s sebou přináší zvýšenou důvěru ze strany subjektů údajů, kteří následně své údaje svěří spíše té službě, ke které mají větší důvěru.[184] Je ovšem na zvážení, nakolik skutečně volí uživatelé služby na základě jejich důvěryhodnosti co do „datové politiky" a nakolik volí na základě užitečnosti služby.[185]

V případech, kdy analýza *big data* následně vede k automatizovanému rozhodnutí, zásadu transparentnosti naplňuje některými autory dovozované právo na vysvětlení individuálního rozhodnutí, kterému se blíže věnuji v kapitolách 4.2.4 a 4.2.5.

3.2.7 Zásada přesnosti

Zásadu přesnosti upravuje článek 5 (1), pís. d ve kterém je určeno, že osobní údaje musí být *„přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny."* V případech *big data* budou v tomto ohledu existovat dva problémy; za prvé, vzhledem k velikosti analyzovaných datových setů je nevyhnutelná určitá chybovost, za druhé, datový set může být v jednotlivostech přesný, stejně ale nemusí podávat reprezentativní obrázek o zkoumaném jevu.

Při chybách v jednotlivých datech nejde pro *big data* jako takové o problém, protože tato chybovost bude vyrovnána množstvím dat a výsledek celkové predikce tak nebude ovlivněn. Problém ovšem nastává v případě, kdy je na základě těchto mylných údajů rozhodnuto v konkrétním, individuálním případě nebo je vytvořen mylný profil subjektu údajů.[186] Správci mají obecně povinnost zavést opatření k průběžnému ověřování a zajištění, aby opakovaně

[184] INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial intelligence, machine learning and data protection,* s. 82, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[185] Příkladem může být využití vyhledávaní na Googlu oproti DuckDuckGo či Startpage.com.

[186] INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial intelligence, machine learning and data protection,* s. 43, [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

používané údaje nebo údaje obdržené nepřímo byly přesné a aktuální.[187] Obecně lze říci, že v těchto případech vyvstává problém zejména s určením, zda tréninková data, na základě kterých algoritmus rozhoduje, jsou skutečně reprezentativní a naopak nejsou diskriminační.

V druhém případě mohou být jednotlivé údaje vstupující do analýzy správné, ale vzorek nebude reprezentativní vůči populaci. Často totiž bude hrozit, že více zastoupeni budou mladší lidé z vyšších příjmových skupin oproti starším lidem z nižších příjmových skupin, což souvisí s dostupností zařízení, ze kterých probíhá sběr dat. Jinými slovy, pokud analýza nepřímo stojí např. pouze na datech uživatelů s chytrým telefonem, lze očekávat, že v těchto datech vznikne nepoměrné zastoupení. Známým příkladem je analýza dat ohledně zasažení New Yorku hurikánem Sandy. Kombinací tweetů a lokalizačních dat ze služby Foursquare bylo možné určit, jak se lidé před příchodem hurikánu chovají, což může pro příště pomoci v koordinování záchranných prací. Problémem ovšem je, že zdaleka nejvíce dat přicházelo z Manhattanu (kde se dá předpokládat větší koncentrace lidí s přístupem k chytrému telefonu a účtem na Twitteru a na Foursquare), zatímco o nejhůře zasažených oblastech bylo dat málo, neboť v těchto místech byl v té chvíli nefunkční mobilní signál, stejně jako byla přerušena dodávka elektrického proudu.[188] Tato nereprezentativnost se může stát problémem v případě, kdy by byla skutečně na základě obdobných dat rozdělována pomoc. Obdobný příklad pak představují různé aktivity státu nebo krajů, které mají adresovat připomínky občanů. Např. webová aplikace Středočeského kraje „Hlášení závad", skrze kterou se mohou „*občané aktivně podílet na zlepšení stavu silničních komunikací ve svém okolí*"[189] bude z povahy věci zpracovávat více námětů ze strany počítačově zdatných občanů vybavených zařízením umožňující přístup k internetu. Tento příklad sice nepředstavuje závažný problém, ukazuje ale na možné budoucí úskalí, které by širší spoléhání na *big data* mohlo přinést.

[187] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, s. 12 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

[188] CRAWFORD, Kate. The Hidden Biases in Big Data. *Harvard Business Review* [online]. 2013 [cit. 2018-11-26]. Dostupné z: https://hbr.org/2013/04/the-hidden-biases-in-big-data

[189] STŘEDOČESKÝ KRAJ. *Hlášení závad - Středočeský kraj* [online]. [cit. 2018-11-26]. Dostupné z: https://musimetoopravit.cz/

3.2.8 Anonymizace jako řešení?

Vymezme nejdříve anonymizované údaje recitálem 26 jako informace, „*které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo přestal být identifikovatelný*.“ Pseudonymizované údaje jsou pak výsledkem procesu pseudonymizace, který článek 4, odstavec 5 definuje jako *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“* Zatímco na anonymní údaje se GDPR nevztahuje (a mohly by tedy být volně využity k analýzám), na pseudonymizované údaje se stále hledí jako na osobní údaje, které jsou pouze dodatečně chráněny pseudonymizací.[190]

Pro ilustrování rozdílu Žůrek[191] nabízí příklad datové sady, ve které jsou následující údaje: *Jméno / Příjmení / Adresa / Věk / Vzdělání / Bydliště / Měsíční příjem / Četnost nákupu / Kupovaný sortiment / Průměrná útrata.*
Při oddělení jména, příjmení a adresy a uchování těchto údajů odděleně půjde o údaje pseudonymizované, zatímco při nevratném oddělení těchto údajů a jejich likvidaci půjde o anonymizaci. Na základě tohoto příkladu se zdá, že v zásadě jednoduché promazání určitých údajů povede k anonymizaci, tedy k vyloučení příslušné datové sady z působnosti GDPR, s tím že se následně nekladou z pohledu ochrany osobních údajů žádné překážky libovolným dalším analýzám – koneckonců již nejde o osobní údaje. Specifikem *big data* ale je, že takto jednoduše proces anonymizace nefunguje (byť v jiných odvětvích by skutečně výše zmíněné bylo anonymizováním údajů), a to vzhledem k možnostem re-identifikace.

Pro ilustraci můžeme zmínit známé případy bezpečnostního incidentu společnosti AOL, re-identifikování „anonymizované“ sekvence DNA až k jednotlivcům skrze algoritmy zkoumající

[190] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi, s. 69, ISBN 978-80-7380-689-7.
[191] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 42, ISBN 978-80-7554-097-3

povahu a četnost pacientových návštěv nemocnice[192], či zpětnou identifikaci uživatelů Netflixu. V posledním zmíněném případě společnost Netflix, jedna ze streamovacích služeb poskytující svým uživatelům filmy a seriály online, zpřístupnila „anonymizovaný" datový set pro vývojáře s tím, že zároveň vypsala cenu $1 000 000 pro nejlepší návrh zlepšení vyhledávacího prostředí služby vzhledem k preferencím uživatelů, které byly v datovém setu obsaženy ve formě jejich minulých hodnocení filmů či seriálů. Datový set neměl obsahovat žádné osobní údaje a Netflix sám k tomu uvedl, že nad to byla zveřejněna jen malá část databáze, a to navíc se záměrnou odchylkou.[193] Zdá se, že společnost provedla mnohem více opatření, než zmiňuje u anonymizace např. Žůrek, taková data by tedy na první pohled neměla podléhat GDPR. I přes všechny zmíněné opatření stačilo k zpětné identifikaci jen malé množství podpůrných informací (*auxiliary information*, *additional knowledge*). Autoři zmíněné studie využili veřejné databáze hodnocení filmů IMDb, ze které pomocí *data miningu* získali data o všech veřejně přístupných hodnoceních. I přes značný šum obsažený v těchto datech (uživatel mohl na IMDb zanechat jen slovní hodnocení, hodnotil totožné filmy v odlišný časový okamžik apod.) stačilo pouze 8 zanechaných recenzí na obou serverech o stejných filmech ze strany téhož uživatele k tomu, aby algoritmus identifikoval totožnost 99% všech uživatelů v „anonymizovaných záznamech". Pro identifikaci 68% uživatelů pak postačovala informace o pouhých dvou recenzích (na obou serverech) a jejich datech.[194] Autory zmíněné implikace, které lze na základě těchto dat činit, jsou neméně závažné, když na základě vyhraněných hodnocení (a ve spojení s IMDb i komentářů) lze provést zasvěcený odhad o politických názorech (hodnocení dokumentů s McCainem či Chomskym), náboženství (např. dle filmu

[192] MALIN, Bradley a Latanya SWEENEY. How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems. *Journal of Biomedical Informatics*[online]. 2000, , 179 - 192 [cit. 2018-10-30]. DOI: doi:10.1016/j.jbi.2004.04.005. Dostupné z: https://www.ncbi.nlm.nih.gov/pubmed/15196482

[193] *„Is there any customer information in the dataset that should be kept private? No, all customer identifying information has been removed; all that remains are ratings and dates. (…) Even if, for example, you knew all your own ratings and their dates you probably couldn't identify them reliably in the data because only a small sample was included (less than one-tenth of our complete dataset) and that data was subject to perturbation. Of course, since you know all your own ratings that really isn't a privacy problem is it*?" Dle: Netflix Prize - Frequently Asked Questions: Is there any customer information in the dataset that should be kept private? [online]. 2009 [cit. 2018-10-30]. Dostupné z: https://www.netflixprize.com/faq.html

[194] NARAYANAN, Arvind a Vitaly SHMATIKOV. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)* [online]. 2008 [cit. 2018-10-30]. Dostupné z: https://arxiv.org/pdf/cs/0610105.pdf

Evangelium podle Jana) i dalších citlivých údajích.[195] Přínosem této studie je vytvoření obecného algoritmu, který dokáže identifikovat jednotlivce na základě datové sady obsahující „mikrodata“, tedy dokáže deanonymizovat jednotlivce i při přístupu k malému vzorku dat z celkové populace, i přes záměrně uvedené odchylky, stejně jako při určité chybovosti podpůrných informací.

V případech *big data* nelze jednoduše rozhodnout o tom, že daná změna v databázi vedla skutečně k anonymizaci a neumožňuje zpětnou identifikaci. Výše naznačený pokrok v možnostech reidentifikace vede některé autory k názoru, že data mohou být za dnešních podmínek buďto užitečné a použitelné pro další analýzu *nebo* skutečně a plně anonymizované.[196] Tento vývoj vede také k úvahám nad změnou definice osobních údajů. Přestože by databáze mohla v dané chvíli být skutečně anonymní (tedy by neumožňovala zpětnou identifikaci), s rozvojem dalších možností analýzy dat se může tento stav změnit. Je nutné vyřešit, jakým způsobem se bude posuzovat případ, kdy správce skutečně anonymizuje datový set, anonymita datového setu ale následně v důsledku rozvoje technologií neobstojí. Na tuto otázku odpovídá recitál 26, podle kterého „*při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze* ***rozumně předpokládat****, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji“* (zdůraznění doplněno). Tento přístup vyjadřuje, že technická limitace anonymizačních postupů nemá automaticky vést k zařazení takto anonymizovaných datových setů pod plnou působnost GDPR. Anonymizace nemusí být zcela bez rizika, stačí, když je riziko sníženo na nepatrnou úroveň, což vychází jednak z technické limitace, jednak z možnosti re-identifikace skrze podpůrné informace osobního charakteru, které o sobě mají např. blízcí příbuzní. Při určování předpokladu možné re-identifikace mohou správci využít řadu praktických nástrojů, které

[195] Tamtéž.

[196] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review,s.* 1704 [online]. [cit. 2018-11-16]. Dostupné z: https://www.uclalawreview.org/pdf/57-6-3.pdf

berou v potaz dobu uchování údajů, pravděpodobnost vývoje relevantní technologie, dostupnost podpůrných informací nebo motivaci třetích stran data re-identifikovat.[197] Kodex chování (*code of practice*), vydaný v Británii ze strany Information Commissioner`s Office, předkládá řadu takových praktických doporučení, např. využití teplotní mapy (*heatmap)* v případech spojení informací s geografickými daty – tímto způsobem není možné z mapy získat přesné geografické pozice, ale jen odhad.[198] Podobně se jednotlivými technikami anonymizace zabývala WP29.[199]

Pro úplnost lze dodat, že ten, kdo re-identifikací získá osobní údaje, aniž by mu k tomu svědčil právní důvod, jedná protiprávně.[200] Další pokrok v re-identifikaci pravděpodobně povede ke snadnější identifikaci citlivých údajů a přispěje k tvorbě tzv. „*databases of ruin"* („zničujících databází").[201] Tento termín označuje stav, kdy lidé o sobě vygenerují dostatečně obsáhlé množství informací a re-identifikační techniky zároveň pokročí natolik, že při dostatku úsilí bude možné získat citlivé či kompromitující informace na téměř každého (tedy každý bude mít svou vlastní „zničující databázi").[202] Tato zatím teoretická možnost podtrhuje důležitost regulace osobních údajů a vydávání vodítek pro správnou anonymizaci dat.

Lze tedy uzavřít, že správný standard anonymizování dat je v éře *big data* nesmírně důležitý, což je důležité zejména v případech, kdy je zveřejnění určitých anonymizovaných dat dáno ze zákona, když chce správce zveřejněním takovýchto dat být pro veřejnost transparentnější nebo když chce umožnit dalším výzkumníkům pracovat na svých datech.[203] I přes technické limitace je koncept anonymizace použitelný i na *big data*, s tím, že volba konkrétních nástrojů

[197] SCHWARTZ, Paul a Daniel SOLOVE. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York Universtiy Law Review*, s. 1879, [online]. **86**(6) [cit. 2018-10-31]. Dostupné z: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs

[198] INFORMATION COMMISSIONER'S OFFICE (ICO). *Anonymisation: managing data protection risk code of practice,* s. 33, [online]. [cit. 2018-11-01]. Dostupné z: https://ico.org.uk/media/1061/anonymisation-code.pdf

[199]ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 05/2014 on Anonymisation Techniques* [online]. [cit. 2018-11-01]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[200] INFORMATION COMMISSIONER'S OFFICE (ICO). *Anonymisation: managing data protection risk code of practice,* s. 27, [online]. [cit. 2018-11-01]. Dostupné z: https://ico.org.uk/media/1061/anonymisation-code.pdf

[201] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, s. 1705 [online]. [cit. 2018-11-16]. Dostupné z: https://www.uclalawreview.org/pdf/57-6-3.pdf

[202] Tamtéž, s. 1750.

[203] INFORMATION COMMISSIONER'S OFFICE (ICO). *Anonymisation: managing data protection risk code of practice,* s. 8, [online]. [cit. 2018-11-01]. Dostupné z: https://ico.org.uk/media/1061/anonymisation-code.pdf

ze strany záleží na kontextu. Vodítkem mohou být texty WP29 (dnes Sboru), stejně jako srozumitelně sepsaný přehled od ICO. Je důležité nepřemýšlet pouze o technických možnostech identifikace daného datového setu (a to vzhledem k výše naznačeným možnostem re-identifikace), ale je třeba též zhodnotit širší kontext, např. možnou motivaci pro re-identifikaci[204] a „vyděračský potenciál", který případně daný datový set skýtá.[205] Tam, kde anonymizace neznehodnotí datový set, zůstává vhodným nástrojem ochrany osobních údajů, ovšem pouze při dodržení recentních zejm. technických doporučení. Pro úplnost lze dodat, že slibným trendem do budoucna je koncept *differential privacy.*[206] Tento inspirativní přístup lze zjednodušeně popsat tak, že spočívá v záměrném a nejlépe lokálním (tj. tento proces probíhá již na zařízení před odesláním na server) přidávání kalibrovaného šumu, záměrného zkreslení. Tento šum se pak při velkém počtu vstupů vyrovná a pro správce tak zůstanou v datovém setu nadále hodnotné údaje, zatímco soukromí jednotlivců bude ochráněno. Další slibný vývoj lze pozorovat ve využívání uměle vytvořených databází, které umožňují vyhnout se „závodům ve zbrojení" mezi anonymizačními a re-identifikačními technikami.[207]

[204] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, s. 1761 [online]. [cit. 2018-11-16]. Dostupné z: https://www.uclalawreview.org/pdf/57-6-3.pdf

[205] Vyděračský potenciál často nebude zjevný. Nevhodně zveřejněná data aplikací měřících sportovní výkon tak lze velice jednoduše využít k identifikaci utajených základen, stejně jako k určení přesné identity těch, kdo na nich pracují. Přesný postup popsán pro aplikaci Polar (známý je také případ aplikace Strava) v: TOKMETZIS, Dimitri, Maurits MARTIJN, Riffy BOL a Foeke POSTMA. Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app. *De Correspondent* [online]. [cit. 2018-12-17]. Dostupné z: https://decorrespondent.nl/8481/heres-how-we-found-the-names-and-addresses-of-soldiers-and-secret-agents-using-a-simple-fitness-app/412999257-6756ba27

[206] Blíže k tomuto matematicky robustnímu modelu: DIFFERENTIAL PRIVACY TEAM. Learning with Privacy at Scale. *Apple Machine Learning Journal* [online]. **1**(8) [cit. 2018-11-21]. Dostupné z: https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html#DMNS06

[207] BELLOVIN, Steven M., Preetam K. DUTTA a Nathan REITINGER. Privacy and Synthetic Datasets. *Stanford Technology Law Review, Forthcoming* [online]. [cit. 2019-02-26]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3255766

3.3 Dílčí závěr

Stanovisko Evropské unie je takové, že plná aplikace současného stupně ochrany osobních údajů napomáhá rozvoji *big data*, když zvyšuje důvěru zúčastněných jedinců.[208] Na základě výše uvedené analýzy lze provést dílčí závěr, že napětí mezi ochranou osobních údajů a současným využíváním *big data* skutečně existuje a *big data* představují pro právní úpravu značnou výzvu.

Na toto napětí jsou nabízena různá řešení. Ty nejradikálnější řešení navrhují např. změnit koncepci osobních údajů a nahlížet na ně jako na majetek, či neaplikovat různé zásady ochrany osobních údajů, a to buďto jen na případy *big data* nebo je již nadále neaplikovat vůbec. Záměrem EU je pak zjevně plně aplikovat všechny zásady ochrany osobních údajů i na případy *big data*, o čemž svědčí mimo jiné opětovné zařazení zmíněných zásad do GDPR; zatímco v době přijímání předchozí směrnicové úpravy byly možnosti *big data* oproti dnešnímu stavu omezené, GDPR již bylo přijímáno za situace, kdy byly dobře známy možnosti, výhody i rizika *big data*.[209]

Na základě výše provedené analýzy možností aplikace jednotlivých zásad na rozsáhlé datové sety lze uzavřít, že zachování všech relevantních zásad ochrany údajů je možné a správné i pro případy *big data*, přestože způsob jejich dodržení nemusí být vždy z pohledu správců zřejmý a snadný.

Pro naplnění zásady zákonnosti bude muset správce určit vhodný titul a vyrovnat se s jeho úskalími. Plnění smlouvy nebude vhodné jako titul pro zpracování osobních údajů pro kritérium nezbytnosti (vzhledem k plnění smlouvy). Pro využití titulu oprávněných zájmů bude muset provést balanční test; v případě, kdy jím plánované zpracování projde, je vhodným titulem. Souhlas je vhodný, bude ovšem nutné naplnit jeho předvídané charakteristiky (zejm.

[208] Kromě jiného dle ARTICLE 29 DATA PROTECTION WORKING PARTY. *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (WP221*), s. 2, [online]. [cit. 2018-11-15]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf
[209] Tamtéž.

svobodnost a informovanost může být problematická). Obecně je současný systém stojící na množství jednotlivých souhlasů kritizován pro faktické neplnění smyslu a účelu právní úpravy, s tím že jako alternativní přístup se nabízí využití *sticky policies* a *dashboardu*. Pro dodržení zásady omezení účelu při dalších zpracováních se jako vhodný postup jeví využití balančního testu (*compatability assessment*), spolu s převzetím měřítka testu ICO, které zavadí posouzení, zda je další zpracování fér (korektní, spravedlivé). Dodržení zásady minimalizace údajů omezuje současnou praktiku uchovávání co nejširšího okruhu dat a klade na správce nároky na posouzení charakteru zpracovávaných údajů, s tím že je např. vhodné používat pouze binární hodnoty (ano/ne). Zároveň pro dodržení této zásady je nutné určit postupy pro další uchování dat. Zásada transparentnosti je pro *big data* důležitá a pro informování subjektů je téměř nutností využít vícevrstvé informování, a to vzhledem ke složitosti zpracování. V případě mobilních aplikací je tento postup již standardem, v případě *IoT* zatím nikoliv. Zároveň je doporučeno informovat subjekty údajů i o tom, že jejich anonymizovaná data budou použita k další analýze. Pro splnění zásady přesnosti bude nutné mj. posoudit reprezentativnost vzorku vůči celkové populaci. Toto je obzvlášť důležité, pokud *big data* slouží jako podklad rozhodování. Využití anonymizace je v důsledku rozvoje re-identifikačních technik ztíženo, přesto je i nadále možné, ovšem správce musí být obeznámen se správnými postupy pro anonymizaci (které se mohou v čase měnit), stejně jako musí posoudit širší kontext zpracování. Zajímavou alternativou je vytváření umělých databází.

Je zjevné, že ne všechny dosavadní praktiky využívající *big data* jsou pod režimem GDPR dovolené – vzhledem k nutnosti vyvažování mezi ochranou subjektu údajů a společensko-ekonomickými benefity jsou takováto omezení samozřejmou součástí evropské ochrany osobních údajů a nejsou důkazem její nefunkčnosti. Právní úprava má být technologicky neutrální a není možné pro každou novou technologii pod tlakem jejich propagátorů zavádět nesystémové výjimky nebo dokonce dovodit, že ku příkladu realita generování značného objemu dat má vést k opuštění zásady minimalizace osobních údajů. Nejde zde ovšem jen o jakýsi právní purismus, ale zejména o to zabránit negativním důsledkům, které by mohlo neregulované využívání *big data* přinést.

Závěrem lze uzavřít, že i přes množství existujících oficiálních dokumentů vztahujících se k *big data* je orientace v dokumentech poměrně náročná a hledání konkrétních odpovědí může být pro správce obtížné. Přestože mohou využít konzultace u příslušného dozorového úřadu, jeví se jako vhodné vydat aktualizovaný dokument (či přehlednou minisite, jako pro GDPR vytvořil Úřad pro ochranu osobních údajů)[210], který by již existující informace a pokyny přehledně shromáždil na jednom místě. Zároveň je žádoucí do budoucna udržovat skrze činnost Evropského sboru pro ochranu osobních údajů aktuální dokument, který detailně upravuje postupy pro anonymizaci, a to vzhledem k zásadnímu pokroku v oblasti re-identifikačních technik.

[210] https://gdpr.uoou.cz/

4 Automatizované individuální rozhodování

„Základem síťové ekonomiky jsou technologie, ale vybudovat ji lze jedině na mezilidských vztazích. Začíná od čipů a končí u důvěry.“[211]

S fenoménem *big data* úzce souvisí problematika automatizovaného individuálního rozhodování. V evropském kontextu byla debata podnícena jednak praktickou otázkou personalizované cenotvorby[212], jednak hodnotovou otázkou, zda má být o lidech rozhodováno automatizovaně, tedy bez lidského prvku (který bere v potaz širší okolnosti a je schopen empatie).[213] Při narůstající složitosti algoritmů (jak je na příkladu neuronových sítí ilustrováno níže) je na místě obava před *„diktaturou dat“*[214], kdy se stále větší část lidských životů řídí pravidly, jejichž složitost přesahuje běžné chápání a rozhoduje se způsobem, kterému je vlastní neprůhlednost. Právní úprava na tuto obavu reaguje ustanovením práva nebýt předmětem automatizovaného rozhodování. V rámci GDPR nalézáme tuto úpravu zejména v článku 22, který někteří autoři považují za první komplexnější regulaci umělé inteligence.[215] Přestože se toto právo jeví být pro mnohé autory novinkou, bylo již součástí Směrnice 95/46/ES[216], stejně jako tuzemského zákona o ochraně osobních údajů[217], s tím že směrnici

[211] Parafráze výroku Kevina Kellyho dle: KOUBSKÝ, Petr. Kořeny digitálního světa. *067.cz* [online]. [cit. 2018-11-26]. Dostupné z: https://067.cz/archiv/14/koreny-digitalniho-sveta.html

[212] OFFICE OF FAIR TRADING. *Personalised Pricing: Increasing Transparency to Improve Trust*[online]. [cit. 2018-10-29]. Dostupné z: http://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf

[213] LEONARD, Peter. Customer data analytics: privacy settings for 'Big Data' business. *International Data Privacy Law*[online]. 2014, **4**(1), 53-68 [cit. 2018-10-29]. DOI: 10.1093/idpl/ipt032. ISSN 2044-3994. Dostupné z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipt032

[214] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28], s. 8, Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[215] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 7, ISBN 978-80-7502-288-2.

[216] Směrnice 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

[217] *„Žádné rozhodnutí správce nebo zpracovatele, jehož důsledkem je zásah do právních a právem chráněných zájmů subjektu údajů, nelze bez ověření vydat nebo učinit výlučně na základě automatizovaného zpracování osobních údajů. To neplatí v případě, že takové rozhodnutí bylo učiněno ve prospěch subjektu údajů a na jeho žádost.“* Dle §11 (6), zákona č. 101/2000 Sb., o ochraně osobních údajů.

předcházela úprava ve francouzském zákoně z roku 1978[218], stejně jako několik pozdějších národních úprav.[219]

4.1 Technický úvod

Automatizované rozhodnutí lze jinými slovy popsat jako rozhodnutí algoritmické. Přestože myšlenka umělé inteligence není novinkou (Turingův test spadá do padesátých let, konstrukce první neurální sítě do let šedesátých)[220], nedávné pokroky v této oblasti vedou k nové vlně zájmu, stejně jako k rozšiřování možností praktického využití.[221] Algoritmus označuje předem stanovený postup k řešení problému, který je následně možné opakovat automatizovaným způsobem.[222] Pokročilé algoritmy, pro které se používá obecně označení umělá inteligence (AI - *artificial intelligence*)[223], jsou konstruovány na základě širokých datových setů. Jinými slovy, *big data* často slouží jako podklad pro následné automatizované rozhodnutí, s tím že někteří autoři problematiku rozhodování na základě širokých datových setů označují souhrnně jako *big data*. Jako umělou inteligenci označujeme v tomto kontextu systémy, které jsou schopny řešit složité problémy v různých situacích a jsou schopny učení se. AI se tak dokáže přizpůsobit

[218] Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés. V článku 2 zákona čteme, že *„aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d`informations donnant une définition du profil ou de la personnalité de l`intéressé. Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d`informations donnant une définition du profil ou de la personnalité de l`intéressé.“.* Článek 3 pak doplňuje; *„Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.“*

[219] Později, ale stále před směrnicí, se úprava nacházela také ve španělském a portugalském právu. Dle: BYGRAVE, Lee A. Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Report,* s. 67 [online]. 2001, 17, 67-76 [cit. 2018-11-23]. Dostupné z: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf

[220] KAMARINOU, Dimitra, Christopher MILLARD a Jatinder SINGH. Machine Learning with Personal Data. *Queen Mary University of London, School of Law - Legal Studies Research Paper,* s. 3 [online]. 2016 [cit. 2018-11-18]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811

[221] KUNER, Christopher, Dan SVANTESSON, Fred CATE, Orla LYNSKEY a Christopher MILLARD. Machine learning with personal data: is data protection law smart enough to meet the challenge?. *International Data Privacy Law*[online]. 2017, **7**(1) [cit. 2018-11-17]. Dostupné z: https://academic.oup.com/idpl/article/7/1/1/3782694

[222] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 232, ISBN 978-80-7598-068-7.

[223] Označování těchto pokročilých algoritmů za AI je dle řady odborníků nesprávné, když za AI má být považován jen takový systém, který uspokojivě projde Turingovým testem či některou z jeho modernějších variací. V práci je pojem používán šířeji, a to pro sjednocení užívané terminologie s dozorovými úřady, které také používají pojem „AI“ široce.

novým datům a upravit svou analýzu bez lidského zásahu.[224] Právě fakt, že zmíněné systémy mají schopnost se učit a dokáží rozhodnout bez lidského zásahu je pro právní úpravu ochrany osobních údajů klíčový.

Zatímco AI je obecným pojmem, který označuje různé systémy s různými způsoby učení, strojové učení (ML - *machine learning)* je technologie, která umožňuje systémům se specifickým způsobem učit z minulých příkladů, dat a zkušeností.[225] Jak již bylo zmíněno, AI potřebuje rozsáhlé datové sety - důvodem je způsob učení. Způsob učení je zároveň klíčový pro pochopení fungování těchto systému, a tedy i možností regulace. Využívá se tří základních způsobů učení: učení bez učitele[226] (*unsupervised learning*, systém se učí bez předem cílových atributů /labelů/, sám je shlukuje, či mezi nimi určuje závislosti*)*, učení s učitelem (*supervised learning,* systém dostane sadu dat již roztřízených do cílových atributů /labelů/, následně nová data zařazuje pod tyto labely) a zpětnovazebné učení (*reinforcement learning*, systém se učí metodou pokusů a omylů, snaží se určit, které kroky vedly ke kýženému výsledku – např. k výhře ve hře*)*.[227] Výsledkem všech tří způsobů učení je vytvoření tzv. modelu, který v různé míře odráží tréninková data a který je buďto statický či dynamický.[228] Statický (též *offline*) model se v čase nemění, přináší tedy shodné výsledky po celou dobu své existence. Oproti tomu dynamický (též *online*) model je schopný měnit své výsledky v průběhu své existence v závislosti na nových datech; běžným příkladem využití tohoto modelu jsou spamové filtry, kdy uživatel označením zpráv za spam a naopak vytáhnutím zpráv označených jako spam

[224] DATATILSYNET. *Artificial intelligence and privacy,* s. 5, [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

[225] THE ROYAL SOCIETY. *Machine learning: the power and promise of computers that learn by example,* s. 16 [online]. [cit. 2018-11-17]. ISBN 978-1-78252-259-1. Dostupné z: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf

[226] Pro ilustraci rozdílů si představme dítě, které dostane různě barevné a různě velké kostky. Při učení bez učitele budeme čekat, dokud dítě samo nenajde způsob, jak v nich udělat pořádek. Při učení s učitelem bude dítěti nejdříve ukázáno, jak třídit podle barvy, následně bude třídit samo další (nové) kostky. Při zpětnovazebném učení dostane dítě bonbón vždy poté, kdy správně roztřídí kostky a rybí tuk vždy, když udělá něco jiného. Dítě se pak metodou pokus-omyl naučí, která činnost (třídění kostek) vede k bonbónu.
Dle: KURFÜRSTOVÁ, Jana. Strojové učení kouzla zbavené. *EDTECH KISK* [online]. [cit. 2018-11-17]. Dostupné z: https://medium.com/edtech-kisk/strojov%C3%A9-u%C4%8Den%C3%AD-kouzla-zbaven%C3%A9-e066d79ebe51

[227] THE ROYAL SOCIETY. *Machine learning: the power and promise of computers that learn by example,* s. 20 [online]. [cit. 2018-11-17]. ISBN 978-1-78252-259-1. Dostupné z: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf

[228] DATATILSYNET. *Artificial intelligence and privacy,* s. 10, [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

z koše dává systému nové podněty a dále jej zpřesňuje.[229] Dynamické modely skýtají mnoho výhod, ale nesou s sebou i samozřejmé riziko spojené s nižší mírou dohledu nad výsledky, když rozhodování a chování systému závisí na nových, v době tvorby algoritmu tedy neznámých, datech. Známým příkladem je AI společnosti Microsoft, chatbot jménem Tay, kterému založila společnost účet na Twitteru s tím, že se chatbot učil konverzovat s ostatními uživateli sociální sítě na základě probíhajících konverzací. Ani ne během 24 hodin od spuštění začal chatbot, využívající dynamického modelu strojového učení, propagovat nacismus, vyvolávat nenávist vůči různým menšinám či šířit konspirační teorie.[230] Případ Tay je zajímavý z několika důvodů. Překvapivá byla rychlost, se kterou došlo k neočekávaným výsledkům, to že Tay prošla před nasazením rozsáhlým testováním velkého množství různých možností a ze strany různorodých skupin lidí, a nakonec fakt, že Microsoft vycházel z předchozích zkušeností s chatbotem Xiaolce, se kterým si bez větších problémů psalo v Číně okolo 40 miliónů lidí.[231]

Pro ochranu osobních údajů a právo nebýt předmětem automatizovaného rozhodování je klíčový způsob, jakým daný model rozhoduje. Různých typů existuje celá řada, pro ilustraci jsou dále popsány dva modely, které jsou, co snadnosti pochopení rozhodovacího procesu a v možnostech kontroly, zcela odlišné. Prvním tímto modelem jsou rozhodovací stromy, které pro svou intuitivnost nacházejí využití v různých oborech lidské činnosti. S notnou dávkou zjednodušení lze říci, že při užití rozhodovacího stromu se data převedou do takového formátu, aby odpovídala jednotlivým částem stromu. Následně se pro dosažení rozhodnutí začíná odshora a postupuje se směrem dolů, kdy každý krok představuje zařazení pod jednu z možností stromu.[232] Zmíněná přehlednost se ovšem i v případě tohoto nejjednoduššího přístupu ztrácí v případě, kdy strom dosahuje mnoha stovek dílčích částí, či je např. propojen s dalšími stromy (vzniká tak tzv. „rozhodovací les“). Přesto lze shrnout, že tento postup dosažení automatizovaného individuálního rozhodnutí je pro subjekty údajů pochopitelný a je i snadno přezkoumatelný, když pro objasnění, proč systém rozhodl určitým způsobem, stačí

[229] Tamtéž, s. 10.
[230] CROCKETT, Emily. How Twitter taught a robot to hate. *Vox*[online]. [cit. 2018-11-17]. Dostupné z: https://www.vox.com/2016/3/24/11299034/twitter-microsoft-tay-robot-hate-racist-sexist
[231] LEE, Peter. Learning from Tay's introduction. *Official Microsoft Blog*[online]. [cit. 2018-11-17]. Dostupné z: https://secure.wikimedia.org/wikipedia/cs/wiki/Hlavn%C3%AD_strana
[232] DATATILSYNET. *Artificial intelligence and privacy,* s. 13, [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

následovat proces rozhodování v opačném směru. Pro přehlednou ilustraci tohoto postupu vizte přílohu práce.

Další možností dosažení rozhodnutí je využití tzv. neurálních sítí či umělých neuronových sítí. Ty napodobují neuronovou síť lidského mozku, s tím že základem je propojení formálních neuronů (perceptronů), které svou logikou zhruba odpovídá vzájemnému propojení neuronů biologických. Analogicky k biologickým neuronům má formální neuron více vstupů, ty jsou násobeny různou váhou (synaptická váha) a jejich vzájemná kombinace určuje výstup z neuronu; pokud je součet vstupů vynásobených příslušnou vahou větší než prahová hodnota (*threshold* či *bias value),* neuron sepne.[233] Výstup z neuronu je opět vstupem do (obecně i více) neuronů. [234] Takto jsou neurony, v případě vícevrstvé (dopředné) neuronové sítě, rozřazeny mezi vstupní vrstvu, pracovní (též skryté) vrstvy a vrstvu výstupní. Nejrozšířenějším modelem učení takto sestavené sítě je pak adaptační algoritmus zpětného šíření chyby (*backpropagation*), kdy se systém učí, tedy zejm. mění váhu u spojení mezi jednotlivými vrstvami tak, aby nastavení systému co nejlépe odpovídalo požadovaným výsledkům. Jinými slovy, pro tréninková data je znám jak vstup (data přicházející do vstupní vrstvy, tedy problém, který má neurální síť řešit), tak výstup (jakého výsledku měla neurální síť při daném vstupu dosáhnout). Tréninková data tedy obsahují mnoho modelových případů, na základě kterých neurální síť „nastavuje" vztahy mezi svými vrstvami tak, aby pro příště rozhodla obdobným způsobem. Zde se tedy vracíme k problematice širokých datových setů, když tréninková data musí pro správnou funkčnost obsahovat velké množství jednotlivých příkladů (i přes mnohá úskalí v zásadě platí poučka *„more data beats better algorithm"[235]).* Počet skrytých vrstev mezi vstupem a výstupem se může lišit a závisí na celé řadě faktorů, zejm. na složitosti řešených problémů. Zatímco před několika lety byl za složitou neurální síť považován systém s osmi vrstvami a za velmi složitou síť systém s 20 až 30 vrstvami, dnešní neurální sítě mohou

[233] KOUBSKÝ, Petr. Mysl je slepenec improvizací. *067.cz*[online]. [cit. 2018-11-27]. Dostupné z: https://067.cz/archiv/58/mysl-je-slepenec-improvizaci.html

[234] VOLNÁ, Eva. *Neuronové sítě 1* [online]. Vydání druhé. Ostrava: Ostravská univerzita v Ostravě, 2008 [cit. 2018-10-28]. Dostupné z: http://www1.osu.cz/~volna/Neuronove_site_skripta.pdf

[235] DOMINGOS, Pedro. *A Few Useful Things to Know about Machine Learning* [online]. [cit. 2018-11-26]. Dostupné z: https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf

obsahovat i přes 100 vrstev.[236] V roce 2015 např. vyhrál soutěž v rozpoznávání obrázků ImageNet systém se 152 vrstvami.[237]

Na tomto místě se dostáváme ke dvěma zásadním hrozbám, které složité rozhodovací algoritmy mohou představovat pro subjekty údajů. Za prvé, jak bylo naznačeno výše, systém se učí z dat; skladba tréninkových nebo v případě dynamických modelů i následných dat nebude vždy odpovídat skutečnému rozložení a model, které následně rozhoduje na základě nereprezentativního vzorku, může pro příště rozhodovat diskriminačně, jak blíže popisuji v další části práce. Za druhé, při složitých algoritmech založených na vícevrstvých neuronových sítích (tj. využívající *deep learning*) vzniká problém netransparentnosti a jen velice obtížné přezkoumatelnosti rozhodnutí systému. Pokud by měl subjekt údajů pochopit, proč daný algoritmus o jeho případě rozhodnul určitým způsobem, neexistuje žádný jednoduchý a přímočarý způsob, kterým by tyto informace získal. Podobně nesnadné je ovšem objevit systémovou chybu, která vede k diskriminačním rozhodnutím. Jinými slovy, jak určit, jestli dané nastavení 152 skrytých vrstev, které systém určil jako nejlépe odpovídající tréninkovému datovému setu, skutečně rozhoduje tak, jak jeho tvůrci zamýšleli.

4.2 Právní úprava ochrany osobních údajů

4.2.1 Obecně k profilování

Nejdříve je třeba definovat profilování a automatizované individuální zpracování. Tyto činnosti mají k sobě velmi blízko a často bude docházet k jejich překrývání, zároveň nejsou ale totožné. V definici profilování vychází Nařízení z vydaného doporučení Rady Evropy[238], ovšem není

[236] Zvýšit samotný počet vrstev není z technického hlediska problém, jde o to, který počet vrstev přináší nejlepší výsledky pro řešení daného problémů. Pokud problémy budou nejlépe řešit algoritmy s více než stovkou skrytých vrstev, šance na plné pochopení vnitřní logiky systému se dále snižuje jak pro subjekty údajů, tak i pro samotné tvůrce systému.

[237] LINN, Allison. Microsoft researchers win ImageNet computer vision challenge. *Official Microsoft Blog* [online]. [cit. 2018-11-18]. Dostupné z: https://blogs.microsoft.com/ai/microsoft-researchers-win-imagenet-computer-vision-challenge/

[238] *Doporučení CM/Rec (2010) 13 Výboru ministrů členským státům o ochraně osob s ohledem na automatizované zpracování osobních údajů.* [online]. [cit. 2018-11-23]. Dostupné z: https://www.uoou.cz/doporuceni-cm-rec-

s ním totožné.[239] Dle článku 4 GDPR je „`*profilováním*` *jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k* ***hodnocení*** *některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu"* (zdůraznění doplněno). Slovo „hodnocení" naznačuje, že profilování obsahuje posouzení osoby. Základní klasifikace podle věku či minulých nákupů tak ještě nemusí spadat pod úpravu profilování.[240]

Můžeme rozlišit tři možné způsoby profilování, a to obecné profilování, rozhodování na základě profilování a výhradně automatizované rozhodování, včetně profilování, které má na subjekt údajů právní účinky, nebo se ho obdobným způsobem dotýká.[241] Z těchto tří variant je dále rozebírána jen třetí varianta, stručné informace o profilování jsou v této části uvedeny pouze pro doplnění kontextu. Profilování bude též obvykle vycházet ze širokých datových setů; problematika *big data*, profilování a automatického individuálního rozhodování se tedy prolíná, a i zde se tak setkáváme s obdobnými problémy co do naplnění zásad ochrany osobních údajů.

Pro profilování specifická je možnost dovození zvláštní kategorie osobních údajů. Zmíněné zvláštní kategorie údajů lze zpracovávat pouze v případech předpokládaných článkem 9 (2) a článkem 6. Příkladem tohoto dovození může být jak výše zmíněna analýza dat poskytnutých společností Netflix, tak např. studie analyzující obsah, u kterého uživatelé na sociální síti Facebook klikli na „to se mi líbí" (like), což je známý mechanismus zmíněné sítě, kterým uživatel naznačuje svůj pozitivní vztah k dané věci.[242] Při analýze této datové stopy 58 000 dobrovolníků byli autoři studie schopni rozpoznat sexuální orientaci v 88% případů, etnicitu

2010-13-vyboru-ministru-clenskym-statum-o-ochrane-osob-s-ohledem-na-automatizovane-zpracovani-osobnich-udaju/ds-1801

[239] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 7 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

[240] Tamtéž, s. 7.

[241] Tamtéž, s. 9.

[242] KOSINSKI, Michal, David STILLWELL a Thore GRAEPEL. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* [online]. 2013, **110**(15), 5802-5805 [cit. 2018-11-24]. DOI: 10.1073/pnas.1218772110. ISSN 0027-8424. Dostupné z: http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110

v 95% případů a politické preference v 85% případů.[243] Pokud je možné z téměř libovolného dostatečně velkého datového setu vytvořit profil obsahující osobní údaje zvláštní kategorie, ztrácí dle některých autorů dělení na zvláštní kategorii smysl a dále by se měl regulátor zaměřit na to, jestli lze *využití* dat (bez jejich předchozího dělení na kategorie) klasifikovat jako citlivé, tedy spadající pod zvláštní kategorii.[244] To, že správci velkých datových setů mají možnost v rámci profilování vydedukovat i citlivé údaje ještě neznamená, že by dělení ztrácelo smysl. Naopak, toto dělení je pokynem správcům, aby k této dedukci citlivých údajů nepřistupovali, respektive přistoupili jen při splnění zvláštních podmínek, které jsou stanoveny v čl. 9 (2) a čl. 6. Taková úprava má vnitřní logiku a vyjadřuje zájem na zvýšené ochraně těch osobních údajů, jejichž neoprávněné zpracování má větší potenciál subjekt údajů poškodit, než je obvyklé.[245] Již zmíněný příklad americké společnosti Target, která na základě nákupního chování vytvořila systém, který odhadoval těhotenství žen, je dobrým příkladem takového postupu. Target, z hlediska GDPR, analyzoval nákupní chování pro získání informace o zdravotním stavu, zpracovával tedy zvláštní kategorii osobních údajů a toto zpracování by bylo po právu pouze pokud by prošlo výše zmíněným testem. Naopak v případě, kdy by Target nákupní údaje např. anonymizoval a dále z nich interně určoval efektivnější skladbu regálů v obchodě, zpracování zvláštní kategorie osobních údajů by se nedopustil, přestože by šlo o zpracování téhož datového setu. Toto rozdělení je intuitivní a naplňuje smysl a účel právní úpravy; pro zrušení zvláštní kategorie osobních údajů tak nejsou dostatečné důvody. Povinnosti s nimi spojené se zkrátka projeví ve chvíli, kdy se správce rozhodne tyto údaje ze svého datového setu dovodit.

Mezi práva subjektů údajů patří právo být informován (čl. 13, 14), právo na přístup (čl. 15), právo na opravu (čl. 16), právo na výmaz (čl. 17), právo na omezení zpracování (čl. 18) a právo vznést námitku (čl. 21). Z těchto práv je v jistém ohledu nejdůležitější právo být informován, když obeznámenost subjektu údajů s probíhajícím profilováním je předpokladem pro možnost

[243] Tamtéž, s. 1.
[244] MOEREL, Lokke a Corien PRINS. Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things. *SSRN Electronic Journal,* s. 11 [online]. [cit. 2018-11-24]. DOI: 10.2139/ssrn.2784123. ISSN 1556-5068. Dostupné z: http://www.ssrn.com/abstract=2784123
[245] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 50, ISBN 978-80-7554-097-3.

výkonu dalších práv. Podobně je pak právo na přístup předstupněm dalšího uplatnění práv.[246] Pro vytvoření profilu na základě *big data* může být relevantní recitál 63 *in fine*, kde je uvedeno: *„Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, měl by mít možnost před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká.“* Zatímco toto ustanovení nalezne své uplatnění např. u žádosti podané u zaměstnavatele, který zpracovává velké množství nestrukturovaných dat zaměstnance[247], s tím že zaměstnanec bude obvykle vyžadovat jen úzkou výseč těchto informací, u profilování na základě *big data* může být využití tohoto ustanovení problematické. V těchto případech totiž bude často využíváno různých zdrojů dat (když různorodost dat je definičním znakem *big data*), jejichž relevanci a charakter subjekt údajů posoudí nejlépe jen, když do nich bude mít plnou možnost nahlédnout. Místo toho je v těchto případech vhodnější umožnit subjektu údajů dálkově přistoupit k jeho osobním údajům, jak ostatně také předvídá recitál 63. Řešení, kdy jsou osobní údaje a z nich vytvořený profil dostupné subjektu údajů skrze jednoduché webové rozhraní, též umožňuje efektivní výkon navazujících práv.

4.2.2 Obecně k výhradně automatizovanému zpracování

Článek 22 v odstavci 1, který je též přezdíván jako „Kafkovo ustanovení“[248], stanovuje, že *„subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.“* Rozhodnutí by mělo být vzhledem k účelu a smyslu normy interpretováno tak, že zahrnuje nejen konečné, ale též přechodné rozhodnutí.[249] Výhradně automatizované zpracování je takové, ve kterém probíhá rozhodovací proces bez

[246] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 164, ISBN 978-80-7502-288-2.
[247] Tamtéž, s. 164.
[248] BORGESIUS, Frederik Zuiderveen. Discrimination, Artificial Intelligence and Algorithmic Decision-Making. *Council of Europe*, s. 22 [online]. [cit. 2019-03-18]. Dostupné z: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73
[249] KAMARINOU, Dimitra, Christopher MILLARD a Jatinder SINGH. Machine Learning with Personal Data. *Queen Mary University of London, School of Law - Legal Studies Research Paper,* s. 12 [online]. 2016 [cit. 2018-11-18]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811

lidského prvku.[250] Tuto podmínku je nutno posoudit materiálně. Pokud tedy automatizované zpracování předkládá relevantní data, ovšem na konci procesu rozhoduje člověk, který bere v potaz i další, jiné okolnosti, nejde o rozhodnutí založené výhradně na automatizovaném zpracování. Pokud je ovšem lidský prvek v procesu pouze uměle vložen za účelem splnění této normy, např. když člověk manuálně potvrzuje systémem navržené rozhodnutí, půjde stále o rozhodnutí založené výhradně na automatizovaném zpracování. Potvrzení tohoto materiálního posouzení ze strany Pracovní skupiny WP29 bylo velice důležité pro další výklad, když v legislativním procesu návrh GDPR nejdříve obsahoval zmínku o rozhodnutí založeném výhradně nebo převážně na automatizovaném rozhodnutí (*solely or predominantly*), ovšem v konečné verzi zůstalo pouze slovo výhradně, z čehož nebylo jasné, jestli je skutečně záměrem užívat materiálního posouzení.[251] Druhou částí hypotézy této normy pak jsou účinky tohoto rozhodnutí, které mají být pro uplatnění tohoto pravidla „*právní*" nebo s „*obdobnými účinky*". Právními účinky je míněn vznik, změna či zánik práv či povinností, s tím že toto ustanovení by mělo dopadat pouze na ty právní účinky, které jsou pro subjekty údajů významné. V opačném případě by se vztahovala tato úprava i na nevýznamné změny, jakými může být např. automaticky vypočtená sleva na každý pátý rohlík.[252] Obdobné účinky pro subjekty údajů zahrnují zejména zásah od osobní[253] či ekonomické[254] sféry subjektů, který je třeba posoudit případ od případu. Pro kategorii obdobných účinků uvádí recitál 71 příklad zamítnutí online podané žádosti o úvěr nebo postupy elektronického náboru bez lidského

[250] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*[online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

[251] EUROPEAN DIGITAL RIGHTS. *Comparison of the Parliament and Council Text on the General Data Protection Regulation* [online]. [cit. 2018-11-23]. Dostupné z: https://edri.org/files/EP_Council_Comparison.pdf

[252] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 235, ISBN 978-80-7598-068-7.

[253] Pro příklad zásahu do intimní sféry jednotlivce na základě analýzy předchozího chování vizte: BROCKELL, Gillian. Dear tech companies, I don't want to see pregnancy ads after my child was stillborn. *The Washington Post* [online]. [cit. 2019-02-19]. Dostupné z: https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/?noredirect=on&utm_term=.b2d2ffc8da03

[254] Aktuální otázkou je povaha vztahu mezi provozovateli platforem sdílené ekonomiky a osobami, které skrze tyto platformy poskytují služby; těmto osobám algoritmus nabízí např. jednotlivé jízdy či je naopak z výběru vyřazuje na základě netransparentních rozhodnutí. Dle: Uber drivers demand their data. *The Economist* [online]. [cit. 2019-03-22]. Dostupné z: https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data

zásahu.[255] Naopak do této kategorie obecně nespadá doručování personalizovaných reklam založených na profilování.[256] Ovšem z tohoto obecného pravidla mohou existovat výjimky, když např. „predátorská" reklama na půjčky s vysokým úrokem bude cílit na osoby s finančními potížemi.[257] Dle příslušných Pokynů pracovní skupiny WP29 patří mezi kritéria pro určení toho, jestli dané rozhodnutí má „*obdobné účinky"*, zda rozhodnutí může významně ovlivnit okolnosti, chování nebo volbu dotčených osob, či mít dlouhotrvající nebo trvalý dopad na subjekt údajů, nebo v nejkrajnějším případě vést k vyloučení či diskriminaci jedinců.[258] Z tohoto hlediska bude zajímavé sledovat, jestli a případně které z algoritmů doručujících a doporučujících obsah (např. tvorba „feedu" jednotlivých sociálních sítí, stejně jako doporučování další hudby k poslechu u tzv. streamovacích služeb) budou považovány za „mající obdobné účinky". V případě algoritmu doručujícího a třídícího jednotlivé položky Facebookového „feedu" lze mít za to, že způsob doručování zpráv spolu s často pokulhávajícím filtrováním obsahu může mít závažné důsledky. Nevhodné nastavení může vést k ovlivnění nálad[259], vytváření názorových bublin (*echo chambers*)[260], úmyslnému vedení uživatele

[255] Zaměstnavatel např. může využít software k automatickému třídění a rozdělování životopisů. V americkém kontextu tuto problematiku dobře ilustroval nedávný příklad diskriminace žen při výběru zaměstnanců skrze software. Dle: DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters* [online]. [cit. 2018-11-17]. Dostupné z: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[256] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 182, ISBN 978-3-319-57959-7.

[257] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 22 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

[258] Tamtéž, s.22

[259] Vybraní uživatelé Facebooku byli vystaveni experimentu, který jim cíleně měnil „feed" tak, aby se zobrazovalo více špatných či dobrých zpráv než obvykle. Uživatelé byli tímto, dle analýzy jejich chování na sociální síti, ovlivnění. Dle: KRAMER, Adam D. I., Jamie E. GUILLORY a Jeffrey T. HANCOCK. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences* [online]. 2014, **111**(24), 8788-8790 [cit. 2018-11-26]. DOI: 10.1073/pnas.1320040111. ISSN 0027-8424. Dostupné z: http://www.pnas.org/cgi/doi/10.1073/pnas.1320040111

[260] Působivou ukázkou schopnosti vytvářet bubliny je projekt Blue Feed, Red Feed, jehož ukázka je v příloze. Vizte: Blue Feed, Red Feed. *The Wall Street Journal* [online]. [cit. 2018-11-23]. Dostupné z: http://graphics.wsj.com/blue-feed-red-feed/#/immigration

k nevhodnému obsahu[261] či dokonce k šíření hate speech a k podněcování rasového násilí.[262] V určitých případech tak algoritmus rozhodující o tom, které zprávy se uživateli zobrazí, může naplnit všechny hlediska pro to, aby měl *„obdobné účinky"*. S očekávaným rozšířením algoritmů do dalších sfér lidského života tak bude pro regulátora do budoucna obtížné a zároveň nutné určit, které z těchto algoritmů (respektive která rozhodnutí) budou spadat pod kritérium *„obdobných účinků"* a které nikoliv.

Jazykovým výkladem článku 22 nelze jednoznačně dovodit, jestli GDPR obecně povoluje automatizované individuální rozhodování s tím, že dává subjektům údajů možnost proti takovému rozhodnutí vznést námitku, nebo jestli GDPR naopak obecně zakazuje takové rozhodování a z tohoto obecného zákazu stanovuje výjimky.[263] Při předchozí směrnicové úpravě členskými státy využity obě možnosti[264], při současné jednotné úpravě skrze GDPR se pak většina autorů přiklonila ke koncepci obecného zákazu s výjimkami, který subjektům údajů přináší vyšší standard ochrany. Toto pojetí potvrdila pracovní skupina WP29; vzhledem ke vlivu argumentace pracovní skupiny lze tedy uzavřít, že jde skutečně o obecný zákaz.[265]

[261] Tento problém vyšel najevo zejm. v souvislosti se serverem YouTube, jehož algoritmus vedl uživatele do „pasti" konspiračních videí či dokonce obsahu, který je na hraně s dětskou pornografií. Problém leží v samotném základu algoritmu, který jako úspěch hodnotí uživatele, který na serveru začne trávit více času. V případě, kdy na serveru začali trávit enormní množství času např. lidé podléhající konspiračním teoriím, YouTube se pokoušel opakovat jejich cestu skrze videa i u dalších uživatelů skrze mechanismus doporučování. Obecně k této problematice vizte: SEAVER, Nick. Captivating algorithms: Recommender systems as traps. *Journal of Material Culture* [online]. 2018 [cit. 2019-02-19]. DOI: 10.1177/1359183518820366. ISSN 1359-1835. Dostupné z: http://journals.sagepub.com/doi/10.1177/1359183518820366
K podrobnostem ohledně YouTube vizte: LOMAS, Natasha. YouTube under fire for recommending videos of kids with inappropriate comments. *TechCrunch* [online]. [cit. 2019-02-19]. Dostupné z: https://techcrunch.com/2019/02/18/youtube-under-fire-for-recommending-videos-of-kids-with-inappropriate-comments/

[262] Jako při nedávném podněcování násilí vůči muslimům v Barmě, ke kterému Facebook svým nevhodným nastavením přispěl. Dle: MCLAUGHLIN, Timothy. How Facebook`s rise fueled chaos and confusion in Myanmar. *Wired* [online]. [cit. 2018-11-23]. Dostupné z: https://www.wired.com/story/how-facebooks-rise-fueled-chaos-and-confusion-in-myanmar/

[263] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 180, ISBN 978-3-319-57959-7.

[264] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář, s. 233, ISBN 978-80-7598-068-7.

[265] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 19-20 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

Výjimky určuje článek 22, odstavec 2 GDPR, s tím že všechny tři výjimky dopadají na celou řadu možných případů zpracování. Uplatňuje-li se některá z těchto výjimek, musí být dle dikce článku 22 stanovena vhodná opatření k zaručení práv, svobod a oprávněných zájmů subjektu údajů.

První výjimka se uplatní, pokud je rozhodnutí *„nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů".* Nezbytnost se posoudí na základě předmětu smlouvy. Příkladem může být pojištění vozidla, kdy pojišťovací společnost navrhuje podmínky pojištění na základě analýzy předchozího chování za volantem. Pokud bez této automatické analýzy není pojišťovací společnost schopna vypočítat odpovídající pojistné, automatizované rozhodnutí je nezbytné k uzavření smlouvy.[266] Pod tento důvod bude spadat také nezbytné využití automatizovaného rozhodování pro předsmluvní zpracování, jako v případě vytřídění životopisů, kterých se na populární místo sejde značné množství.[267]

Druhá výjimka, která míří na boj proti daňovým únikům, se uplatní, pokud je rozhodnutí *„povoleno právem Unie nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů*". Pod tuto výjimku spadá např. plánovaná novela daňového řádu, která v §59a, odstavci 1, písmenu b zavádí možnost provádět výkon správy daní, s výjimkou vydávání rozhodnutí, i výhradně na základě automatizovaného zpracování osobních údajů.[268]

Třetí výjimka se uplatní na případy, kdy s takovým automatizovaným rozhodnutím subjekt údajů výslovně souhlasí. Souhlas musí splňovat obecné podmínky GDPR, musí být tedy svobodný, konkrétní, informovaný a jednoznačný.

---

[266] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 183, ISBN 978-3-319-57959-7.

[267] WP29 uvádí příklad, kdy podnik obdrží „desítky tisíc žádostí". Problémy pochopitelně budou s určením hranice nezbytnosti; je to 100 životopisů, 500, 1 000 nebo skutečně jen alespoň 20 000? Dle: PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 24 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

[268] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 219, ISBN 978-80-7502-288-2.

Přísnější režim je stanoven pro zvláštní kategorie osobních údajů, kde se výše zmíněné výjimky neuplatní. V těchto případech je automatizované rozhodování povoleno pouze v případech, kdy je založeno na základě souhlasu (s tím že v těchto případech bude obzvlášť těžké dosáhnout svobodného a informovaného souhlasu) nebo je upraveno právem EU či členského státu v rozsahu nezbytném pro významný veřejný zájem dle čl. 9 (2), pís. g. Tento přísnější režim se uplatní také v případech, kdy budou údaje spadající do zvláštní kategorie osobních údajů správcem dovozeny.

Dle recitálu 71 by se dále nemělo v případě dětí vůbec využívat výhradně automatizovaného rozhodování, včetně profilování, které má právní nebo obdobné účinky. Dle WP29 ovšem nejde o absolutní zákaz, když recitál slouží k interpretaci právní normy a sám závazný není. Správci tedy jednak mohou využít tohoto rozhodování tam, kde rozhodnutí nebude mít na dítě právní nebo obdobný účinek, stejně jako mohou nastat případy, kdy správci budou muset provést výhradě automatizované rozhodnutí, které bude mít právní nebo obdobné účinky, a to např. za účelem ochrany dobrých životních podmínek dětí.[269]

Správce bude mít také obvykle povinnost provést posouzení vlivu na ochranu osobních údajů (*DPIA – data protection impact assessment).* Pokud je, dle čl. 35 (1), „p*ravděpodobné, že určitý druh zpracování, zejména při využití* ***nových technologií****, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů"* (zdůraznění doplněno). Posouzení je pak dle čl. 35 (3), pís. a zejména nutné v případě systematického a rozsáhlého *„vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad."* Zároveň bude muset správce jmenovat, dle čl. 36 (1), pís. b pověřence pro ochranu osobních údajů v případě, kdy *„hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své*

[269] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 29 [online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů".
Tyto povinnosti mají za cíl, aby si správce interně rozmyslel, jaké povinnosti na něj dopadají a jaké zvolit vhodná opatření pro snížení rizik spojených s jeho zpracováním.

Subjekty údajů pak v těchto případech mají dále právo být informovány (dle čl. 13 a 14), právo na přístup (dle čl. 15 (1) pís. h), právo na lidský zásah ze strany správce (dle čl. 22(3)), právo vyjádřit svůj názor a napadnout rozhodnutí (čl. 22(3)). V další části práce rozebírám právo být informován, respektive právo na vysvětlení, které z textu GDPR někteří autoři dovozují.

K povaze modelu z hlediska ochrany osobních údajů

Ať už slouží daný model k výhradně automatizovanému rozhodování či nikoliv, je nutné posoudit jeho charakter z hlediska ochrany osobních údajů. Tato otázka je nesmírně důležitá vzhledem k současnému trendu, kdy správci mezi sebou obvykle neobchodují přímo s osobními údaji (vzhledem k přísným právním požadavkům), ale nabízejí již hotové modely, a to buďto skrze licencování API[270] daného programu (Cortana Intelligence Gallery) či přímo prodejem hotového „krabicového řešení" (Tensorflow Mobile).[271] Jak bylo zmíněno v úvodní technické pasáži, model vždy odráží tréninková data. Pokud je daný model zranitelný vůči některým druhům útoků, je z něj různými způsoby možné, v podstatě skrze zneužití jeho fungování, původní tréninková data získat, s tím že byl-li model trénován na osobních údajích (respektive na datech obsahujících osobní údaje), půjde tímto způsobem z modelu osobní údaje získat.

Možných útoků, které umožňují získání osobních údajů, existuje vícero. Blíže zmiňuji pouze dva, a to inverzní útok (*model inversion*) a útok zaměřený na ověření toho, zda-li jednotlivec

[270] API, tedy rozhraní pro programování aplikací, zjednodušeně řečeno umožňuje komunikaci a výměnu dat mezi různými službami, programy či aplikacemi.
[271] VEALE, Michael, Reuben BINNS a Lilian EDWARDS. Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* [online]. 2018, **376**(2133) [cit. 2019-02-26]. DOI: 10.1098/rsta.2018.0083. ISSN 1364-503X. Dostupné z: http://rsta.royalsocietypublishing.org/lookup/doi/10.1098/rsta.2018.0083

byl součástí tréninkových dat (*membership inference*), s tím, že související téma útoků cílících nikoliv na získání osobních údajů, ale na zmatení daného modelu vedoucí k nesprávnému rozhodnutí, rozvíjím v navazující části.

První typ útoku, *model inversion*, je možné využít v situaci, kdy má útočník k dispozici sadu či databázi osobních údajů a přístup k modelu, jehož tréninková data obsahovala osobní údaje, s tím že někteří jednotlivci, kteří byli součástí tréninkových dat jsou zároveň součástí databáze, kterou má k dispozici útočník. Snahou útočníka následně je získat další, bližší informace o jednotlivcích ve své databázi, respektive doplnit jemu dostupné informace o nich o další informace (osobní údaje), které získá tím, že z modelu dovodí tréninková data.[272] Jedním z příkladů takového postupu je zneužití algoritmů doporučujících obsah na základě analýzy (předchozího) chování uživatelů. U řady služeb (Last.fm[273] či Amazon) uživatelé o sobě dobrovolně sdílejí část informací, např. na e-shopu zanechají veřejnou recenzi u několika zakoupených produktů, algoritmy doporučující dalším návštěvníkům obdobný obsah nebo produkty ke koupi berou ovšem v potaz celkovou nákupní historii jednotlivce.[274] Zejména v případě menších služeb je tak na základě veřejných informací (např. recenzí) možno dovodit dobrovolně nesdílenou informaci (např. nákup výrobku, považovaný subjektem údajů za citlivý) na základě změn v obecných doporučeních činěných ze strany dané služby, respektive daného modelu.

V případě druhého typu útoku, *membership inference*, bude jedinou získanou informací to, zda daný jednotlivec byl součástí tréninkových dat. Můžeme mít za to, že i tato informace je

[272] Tamtéž, s. 4.

[273] Služba umožňuje uživatelům sledovat a vzájemně poměřovat statistiky poslouchání hudby, s tím, že na základě osobních preferencí jim následně doporučuje individualizované „rádio“. Na obdobném principu fungují dnes značně rozšířené streamovací služby jako Spotify či Apple Music.

[274] CALANDRINO, Joseph A., Ann KILZER, Arvind NARAYANAN, Edward W. FELTEN a Vitaly SHMATIKOV. "You Might Also Like: " Privacy Risks of Collaborative Filtering. *2011 IEEE Symposium on Security and Privacy* [online]. IEEE, 2011, 2011, , 231-246 [cit. 2019-02-26]. DOI: 10.1109/SP.2011.40. ISBN 978-1-4577-0147-4. Dostupné z: http://ieeexplore.ieee.org/document/5958032/

osobním údajem, a to s přihlédnutím k rozhodnutí ESD v nedávném případě Nowak[275], které je ovšem leckdy kritizováno jako maximalistické.[276]

S přihlédnutím k výše zmíněnému považují Veale, Binns a Edwards, v některých případech, data obsažená v modelu (respektive model samotný) za pseudonymizovanou verzi osobních údajů užitých k trénování modelu, s tím že pseudonymizované osobní údaje je třeba dle GDPR stále považovat za osobní údaje.[277] V takovém případě by se při nakládání s modelem plně uplatnila příslušná práva a povinnosti týkající se zpracování osobních údajů. Naplnění práv i povinností v těchto případech bude nesmírně obtížné, zejména co do výkonu „práva být zapomenut" (a s tím spojené nutnosti přetrénovat systém) či co do naplnění zásady omezení uložení.[278] V řešení těchto otázek je technický i právní výzkum teprve na počátku.

Výše zmíněný volný přístup k rozhodování daného systému zároveň může vést k závažným hrozbám z hlediska kyberbezpečnosti, kdy i bez přístupu k tréninkovým datům a bez jakékoliv bližší znalosti modelu je možné jej zneužít (tzv. *black box attack).*[279] Zjednodušeně řečeno, útočník např. skrze API posílá obrázek[280] k rozpoznání, zpět dostává odpověď, co se dle

[275] Přestože se případ vztahuje ke směrnicové úpravě, lze jeho závěry nepochybně převzít i pro novou úpravu. ESD se v tomto případě vyjádřil, že pojem osobní údaje má široký význam a neomezuje se *„na informace, které jsou citlivé nebo patří do soukromé sféry, ale potenciálně zahrnuje všechny druhy informací, a to jak objektivní, tak subjektivní ve formě nebo názoru nebo hodnocení pod podmínkou, že jsou `o` dotčené osobě".* Bod 34, Rozsudek Soudního dvora ze dne 20. prosince 2017. Peter Nowak v. Data Protection Commissioner, Věc C-434/16, ECLI:EU:C:2017:994. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=13042823

[276] Vizte např. PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* [online]. 2018, **10**(1), 40-81 [cit. 2019-02-26]. DOI: 10.1080/17579961.2018.1452176. ISSN 1757-9961. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

[277] VEALE, Michael, Reuben BINNS a Lilian EDWARDS. Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* [online]. 2018, **376**(2133) [cit. 2019-02-26]. DOI: 10.1098/rsta.2018.0083. ISSN 1364-503X. Dostupné z: http://rsta.royalsocietypublishing.org/lookup/doi/10.1098/rsta.2018.0083

[278] Tamtéž, s. 9-12.

[279] V případě, kdy útočník má o modelu úplné informace, hovoříme o tzv. *white box attack*, v případech částečných znalostí útočníka pak o *gray box attack.* Dle: MOLNAR, Christoph. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.* [online]. 2018 [cit. 2018-11-24]. Dostupné z: https://christophm.github.io/interpretable-ml-book/index.html

[280] V této části se zabývám výhradně neurálními sítěmi, jejichž cíl je rozpoznávat obsah obrázků, a to vzhledem k rozšířenosti a dostupnosti těchto modelů a zároveň k vizuální názornosti tohoto postupu. Princip funguje obdobně i když není využita neurální síť, stejně jako v případech, kdy má systém dojít nikoliv k rozpoznání obrázku, ale k individuálnímu rozhodnutí.

modelu na obrázku nachází. Na základě těchto informací útočník vytváří svou vlastní neurální síť, tedy vytváří svůj vlastní model[281], který má zhruba odpovídat modelu původnímu.[282] Na svém modelu pak pomocí matematických postupů hledá, která změna obrázku vede k nesprávné klasifikaci, s tím že úspěšnost takové změny lze opět skrze API jednoduše ověřit. Možnosti těchto útoků jsou pozoruhodné[283] – zmást běžně používané neurální sítě lze bez toho, aby si člověk jakékoliv změny na obrázku povšimnul, a to přidáním šumu[284], pomocí změny jediného pixelu[285] či dokonce lze 3D tiskem vytvořit objekt, který neurální síť (ať už jej hodnotí z jakéhokoliv úhlu) rozpoznává jako objekt zcela jiný.[286] Tyto příklady jsou obzvláště nebezpečné pro bezpečnostní systémy, které spoléhají na detekci objektů v reálném světě pomocí kamer. Zároveň ilustrují hrozby, před kterými stojí neurální sítě používané k automatizovanému individuálnímu rozhodování.

4.2.3 Zásada přesnosti a algoritmické vězení

Významným ohrožením práv subjektů údajů je fakt, že algoritmus může dojít k diskriminačním rozhodnutím, aniž by takový způsob rozhodování byl záměrem jeho tvůrců. Diskriminaci je následně velice obtížné odhalit[287], a to vzhledem ke složitosti systémů a způsobům učení algoritmu, lidé navíc u algoritmických rozhodnutí předpokládají vysokou přesnost a mnohdy

[281] Což má také důsledky co do ochrany duševního vlastnictví k danému modelu.

[282] MOLNAR, Christoph. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.* [online]. 2018 [cit. 2018-11-24]. Dostupné z: https://christophm.github.io/interpretable-ml-book/index.html

[283] Dále zmíněné příklad jsou převzaty z MOLNAR, Christoph. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.* [online]. 2018 [cit. 2018-11-24]. Dostupné z: https://christophm.github.io/interpretable-ml-book/index.html

[284] Vizte klasifikaci pandy jako gibbona po přidání šumu do obrázku v příloze práce. Dle: GOODFELLOW, Ian, Jonathon SHLENS a Christian SZEGEDY. Explaining and harnessing adversarial examples. *ArXiv preprint* [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1412.6572.pdf

[285] SU, Jiawei, Danilo Vasconcellos VARGAS a Kouichi SAKURAI. One Pixel Attack for Fooling Deep Neural Networks. *ArXiv* [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1710.08864.pdf

[286] ATHALYE, Anish, Logan ENGSTROM, Andrew ILYAS a Kevin KWOK. Synthesizing Robust Adversarial Examples. *ArXiv preprint* [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1707.07397.pdf

[287] BAROCAS, Solon a Andrew SELBST. Big Data's Disparate Impact. *California Law Review* [online]. [cit. 2018-11-19]. Dostupné z: http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf

na ně příliš spoléhají[288], a to i přes zjevnou nelogičnost rozhodnutí.[289] Řešení algoritmické diskriminace je pro právo výzvou z mnoha důvodů; vyžaduje alespoň elementární chápání fungování těchto algoritmů (jejichž povaha se s technologickým pokrokem mění), koncepčně je opakováním debaty ohledně role práva ve zmírňování rozdílů ve společnosti a doktrinálně vzniká tření mezi systémem ochrany osobních údajů a anti-diskriminační právní úpravou.[290] To, že jde o aktuální téma, dokazuje také zmínka o hrozbě „algoritmického vězení" ve Zprávě o stavu lidských práv v České republice za rok 2015, kterou každoročně vypracovává Rada vlády pro lidská práva, dle které sice může být užití rozhodovacích algoritmů užitečné v celé řadě ohledů, toto použití je ale nutné řádně regulovat.[291]

GDPR se příliš k tomuto problému nevyjadřuje; v recitálu 71 najdeme, že by správce *„v zájmu zajištění spravedlivého a transparentního zpracování (…) měl použít **vhodné matematické nebo statistické postupy** profilování, zavést technická a organizační opatření, která zejména zajistí opravu faktorů vedoucích k nepřesnosti osobních údajů a minimalizaci rizika chyb, a zabezpečit osobní údaje takovým způsobem, který zohledňuje potenciální rizika pro zájmy a práva subjektu údajů a který mimo jiné **předchází diskriminačním účinkům** vůči fyzickým osobám (…) nebo předchází přijímání opatření, jež mají takové účinky"* (zdůraznění doplněno). Povinnost zavést takové postupy spadá pod úpravu čl. 22 (3), podle kterého má správce provést „*vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí."*

[288] BUTTERWORTH, Michael. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review*, s. 265 [online]. **34**(2), 257-268 [cit. 2018-11-14]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S026736491830044X

[289] Fenomén známý jako *„computer says no"* či *„automation bias".* Toto spoléhání na algoritmy, které zdánlivě snímají z jednotlivců individuální odpovědnost, tvoří obtížně regulovatelnou kategorii tzv. polo-automatizovaného rozhodování. Blíže: VEALE, Michael a Lilian EDWARDS. Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review,* s. 45 [online]. 2017, **16**(18) [cit. 2019-02-20]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

[290] HACKER, Philipp. Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, s. 1146, [online]. (55), 1143 - 1186 [cit. 2018-11-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164973

[291] RADA VLÁDY PRO LIDSKÁ PRÁVA. *Zpráva o stavu lidských práv v České republice v roce 2015*, s. 17 [online]. [cit. 2018-11-21]. Dostupné z: https://www.vlada.cz/assets/ppov/rlp/dokumenty/zpravy-lidska-prava-cr/zprava-2015.pdf

Nezamýšlená diskriminace se může stát vlastností algoritmu z celé řady důvodů. Jak bylo popsáno v technickém úvodu, výsledný model závisí na tréninkových datech; diskriminace bude tedy často pramenit z nezamýšlených a netušených nedostatků těchto dat. V prvé řadě jde o nevhodné určení cílových atributů (labelů), tedy „správných výsledků", ke kterým má systém dojít, případně neodpovídající reprezentace určitých skupin obyvatel v tréninkových datech. Příkladů takové diskriminace můžeme nalézt mnoho. Mediální zájem tak mj. vzbudil algoritmus Googlu, který „rozpoznával" Afroameričany jako gorily[292], algoritmus určující výhradně bělošské královny krásy[293], nebo algoritmus určují zejména muže jako vhodné kandidáty pro práci.[294] Ve všech těchto případech byla diskriminace způsobena nedostatečným zastoupením určitých skupin v tréninkových datech, na základě kterých se algoritmus učil a následně rozhodoval. Tento problém nelze redukovat pouze na zajištění dostatečného zastoupení různých skupin v tréninkových datech. Zatímco některá schémata objevující se v datech jsou pro autory modelu užitečná (zvýšená konzumace slazených nápojů a s tím zvýšené riziko vybraných nemocí), jiná představují stereotyp, kterému se má model vyhnout (hoši preferují modrou, dívky růžovou).[295] Algoritmy při učení ovšem nerozlišují např. mezi výše zmíněnými stereotypy (s tím, že některé mohou být škodlivé, zvlášť při jejich znásobení ze strany algoritmu) a cennými informacemi. Vhodným příkladem tohoto omezení je fungování strojových překladů, které vycházejí z širokých, nejčastěji nijak neredigovaných datových setů.[296] V těchto případech pak systém vychází ze statisticky nejčastějších dvojic, což např. při překladu z jazyků nerozlišujících mužská a ženská zájmena vede k násobení

[292] Složitost algoritmu v pozadí pak potvrzuje fakt, že ani po 3 letech nedokázal Google uspokojivě vyřešit tento problém a pro příště pouze vyřadil kategorii goril z výsledků detekce obrázků. Dle: VINCENT, James. Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech. *The Verge* [online]. [cit. 2018-11-19]. Dostupné z: https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai

[293] PEARSON, Jordan. Why An AI-Judged Beauty Contest Picked Nearly All White Winners. *Vice – Motherboard* [online]. 2016 [cit. 2018-11-19]. Dostupné z: https://motherboard.vice.com/en_us/article/78k7de/why-an-ai-judged-beauty-contest-picked-nearly-all-white-winners

[294] DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters* [online]. [cit. 2018-11-17]. Dostupné z: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[295] BAROCAS, Solon, Arvind NARAYANAN a Moritz HARDT. *Fairness and machine learning: Limitations and Opportunities,* s. 19-20 [online]. fairmlbook.org, 2018 [cit. 2019-03-21]. Dostupné z: https://fairmlbook.org/

[296] Pro příklad stavu tréninkových dat vizte fungování klasifikace na podkladě ImageNet, jedné z největších databází obrázků, ke kterým byl ručně doplněn popis: RYGE, Leif. *ImageNet Roulette* [online]. [cit. 2019-03-22]. Dostupné z: https://imagenet-roulette.paglen.com/

genderových stereotypů[297], z hlediska algoritmu ovšem pouze k větší přesnosti vzhledem k dostupným tréninkovým datům.

Z výše uvedeného je zřejmé, že regulace a odhalování nesprávného či diskriminačního rozhodování algoritmů je pro regulátora obtížné, není ovšem nemožné. Správci budou často pro své modely využívat některé z již existujících frameworků, jako např. Core ML nebo ML Kit, což usnadňuje následnou kontrolu. Dalším, a do budoucna nejspíše klíčovým, vývojem v této oblasti je rozvoj různých nástrojů, které pomáhají odhalit diskriminační rozhodování daného modelu. V této souvislosti můžeme zmínit volně dostupné repozitáře audit-AI[298], Aequitas[299], FairML[300] či What-If. Posledním pokrokem v této oblasti je pak nedávný vývoj nástroje AI Fairness 360 ze strany IBM, který vyniká jednak intuitivním rozhraním, jednak také svým důrazem na kroky vedoucí ke zmírnění diskriminačního rozhodování, oproti prostému určení existence takové diskriminace.[301] Zmíněné modely v příkladu svého fungování (tzv. demu) obvykle pracují s případem amerického systému COMPAS, který ostatně dobře ilustruje hrozby spojené s algoritmickou diskriminací. COMPAS byl využíván některými americkými soudy k určení pravděpodobnosti recidivy a ovlivňoval tak rozhodování soudu.[302] Jak bylo později prokázáno, posuzoval černošské obžalované přísněji než bělochy, kterým naopak určoval příznivější skóre častěji, než měl.[303]

[297] Vizte přílohu pro příklad překladu z angličtiny (rozlišující *he* a *she*) do turečtiny (pro oba rody užito jedno slovo *o*) a nazpět. Dle BAROCAS, Solon, Arvind NARAYANAN a Moritz HARDT. *Fairness and machine learning: Limitations and Opportunities,* s. 19-20 [online]. fairmlbook.org, 2018 [cit. 2019-03-21]. Dostupné z: https://fairmlbook.org/

[298] Audit-AI. *GitHub* [online]. [cit. 2018-11-21]. Dostupné z: https://github.com/pymetrics/audit-ai

[299] SALEIRO, Pedro, Benedict KUESTER, Abby STEVENS, Ari ANISFELD, Loren HINKSON, Jesse LONDON a Rayid GHANI. Aequitas: A Bias and Fairness Audit Toolkit. *Center for Data Science and Public Policy - University of Chicago* [online]. [cit. 2018-11-20]. Dostupné z: https://arxiv.org/pdf/1811.05577.pdf

[300] FairML. *GitHub* [online]. [cit. 2018-11-21]. Dostupné z: https://github.com/adebayoj/fairml

[301] VARSHNEY, Kush. Introducing AI Fairness 360. *IBM* [online]. 2018 [cit. 2018-11-20]. Dostupné z: https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

[302] HACKER, Philipp. Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, s. 1144, [online]. (55), 1143 - 1186 [cit. 2018-11-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164973

[303] LARSON, Jeff, Surya MATTU, Lauren KIRCHNER a Julia ANGWIN. How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica* [online]. [cit. 2018-11-19]. Dostupné z: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Neexistuje ovšem jasná a přímočará cesta, jak vytvořit model, které je nediskriminační a férový (korektní). Nepanuje totiž shoda na tom, jaký způsob výběru a zastoupení určitých skupin lidí je férový. Tuto problematiku dobře ilustrují možnosti, které při auditu algoritmů nabízí nástroj společnosti Google What-if.[304] Mějme algoritmus, který rozhoduje, komu se nabídne půjčka, s tím že mezi uchazeči, kterým byla půjčka skutečně nabídnuta je jen 30 procent žen (odhlédněme teď od toho, že využití takového algoritmu by dle GDPR bylo problematické, když porušuje právo subjektů údajů nebýt předmětem automatizovaného individuálního rozhodování a zamítnutí půjčky patří mezi jiné významné důsledky). Základem prvního hlediska (v modelu What-If pod názvem *group unaware)* posouzení férovosti je snaha, aby algoritmus nijak nepracoval s údaji o pohlaví, stejně jako s údaji, ze kterých lze pohlaví dovodit. Pro obě pohlaví tedy budou jinak použity stejné statistické modely (respektive stejný konfidenční interval, *confidence level*), které vedou k přijetí či zamítnutí žádosti. Pokud toto rozhodování bude ve výsledku schvalovat žádosti o půjčku převážně jednoho pohlaví, bude systém přesto férový. S ohledem na toto první hledisko je vhodné zmínit, že v oblasti pojištění je zakázáno rozdílné zacházení s pojištěnci na základě pohlaví jak v USA[305], tak též v Evropské unii, když rovnost mužů a žen je základní zásadou Evropské unie. Ve věci Test-Achats[306] ESD rozhodl, že při stanovování výše pojistného a pojistného plnění musí pojistitelé změnit svou cenovou politiku s cílem zavést rovné zacházení se zákazníky mužského a ženského pohlaví, respektive zneplatnil čl. 5 odst. 2 směrnice.[307] Ten dával členským státům právo odchýlit se u pojistných smluv od pravidla stejného přístupu k oběma pohlavím, bylo-li pohlaví určujícím faktorem při posuzování rizika založeném na příslušných a přesných pojistněmatematických a statistických údajích. Nadále jsou tedy veškeré postupy, jejichž výsledkem jsou rozdíly v

[304] Následující popis možností nástroje What-If je kompletně převzat z: WEINBERGER, David. Playing with AI Fairness. *What-If Tool* [online]. [cit. 2018-11-21]. Dostupné z: https://pair-code.github.io/what-if-tool/ai-fairness.html

[305] Inspiraci USA zmiňuje generální advokátka Kokott ve svém stanovisku: *„(…) S takovým rozsudkem by se mimo jiné Soudní dvůr ocitl v dobré společnosti: již před více než třiceti lety rozhodl Nejvyšší soud ve Spojených státech v souvislosti s důchodovým pojištěním, že Civil Rights Act z roku 1964 zakazuje rozdílné zacházení s pojištěnci podle jejich pohlaví.“* Dle: Stanovisko generální advokátky Juliane Kokott ve věci C‑236/09 Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=82589&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3975414#Footnote49

[306] Rozsudek Soudního dvora ze dne 1. března 2011. Test-Achats. Věc C-236/09, ECLI:EU:C:2011:100. Dostupné z http://curia.europa.eu/juris/document/document.jsf?text=&docid=80019&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3975414#Footnote*

[307] Směrnice Rady 2004/113/ES ze dne 13. prosince 2004, kterou se zavádí zásada rovného zacházení s muži a ženami v přístupu ke zboží a službám a jejich poskytování

pojistném a pojistném plnění v důsledku použití pohlavní identity jako faktoru při výpočtu výše pojistného a pojistného plnění, zakázány čl. 5 odst. 1 příslušné směrnice. Ten ovšem nezakazuje použití pohlavní identity jako rizikového faktoru obecně, takové použití je povoleno při celkovém výpočtu pojistného a pojistného plnění do té míry, pokud nevede k rozdílům na úrovni jednotlivých pojištěnců.[308] Tento případ přináší otázku, zda má být objektivní statistika, např. ohledně úmrtnosti mužů a žen, podřízena právním pravidlům rovnosti.

Dle druhého hlediska (*group thresholds)* by první přístup mohl dále opakovat historické předsudky např. v preferenci mužských žádostí a výsledný model by sankcionoval znaky typické pro ženy, a to i při nejlepší snaze nemít v datovém setu údaje o pohlaví (přesto údaj o pohlaví zůstane v datech nepřímo, když např. z doložené historie příjmů může být patrné, jestli žadatel byl na mateřské dovolené).[309] Z tohoto důvodů by se dle druhého hlediska měla pro každé pohlaví určit odlišná podmínka, při které žadatel půjčku dostane, aby se vyvážily historické předsudky obsažené v předchozích případech, které sloužily jako tréninková data. Muž by tak dostal půjčku při 60% pravděpodobnosti, že ji splatí zpět, žena při pravděpodobnosti nižší. Dle třetího hlediska (*demographic parity)* by počet úspěšných žadatelů daného pohlaví mělo odpovídat celkovému počtu žadatelů daného pohlaví. Pokud o půjčku žádá 1000 lidí, z toho 300 žen a 700 mužů, půjčku by spravedlivě mělo dostat například zhruba 30 žen a 70 mužů. Čtvrté hledisko (*equal opportunity*) určuje, že algoritmus je férový, pokud stejné procento z těch mužů a žen, kteří mají shodný rizikový profil, skutečně obdrží nebo neobdrží půjčku. Tedy ti, kdo se kvalifikují pro určitý příznivý výsledek, mají mít stejnou šanci na tento příznivý výsledek. Systém nabízí i další, složitější hlediska posuzování férovosti systému, ale i z tohoto stručného přehledu je jasné, že určit, co je „férový algoritmus“ je nesmírně obtížné.

[308] Pokyny k uplatňování směrnice Rady 2004/113/ES v pojišťovnictví s ohledem na rozsudek Soudního dvora Evropské unie ve věci C-236/09 (Test-Achats) [online]. [cit. 2019-3-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52012XC0113(01)&from=GA

[309] St. George`s Hospital Medical School využíval v 70. letech jeden z prvních takovýchto algoritmů pro předvýběr žadatelů o studium. Systém se „učil“ na základě minulých dat a jeho výsledkem bylo diskriminování žen a žadatelů z některých oblastí Británie, stejně jako žadatelů z ciziny. Algoritmus tak ve výsledku vedl ke znásobení předchozí diskriminace. Dle: O`NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, 2016, s. 97-98. ISBN 0553418815.

Zásada přesnosti je tedy v případech algoritmického rozhodování stěžejní pro tvorbu nediskriminačního modelu, když v případě nevhodně zvolených tréninkových dat může algoritmus vykazovat diskriminační rozhodování. Přestože se skryté vrstvy neurální sítě popisují jako „*black box*“, který v zásadě téměř nelze kontrolovat, začínají vznikat různé nástroje měřící pomocí různých oklik diskriminační tendence daného algoritmu. Tyto nástroje vyvíjí největší technologické společnosti světa (z výše zmíněných nástrojů šlo např. o nástroje od IBM či Google). Důvěra veřejnosti v rozhodování algoritmů je i pro ně důležitá pro další rozvoj v této oblasti, lze tedy očekávat další dynamický vývoj těchto systémů. Tento v podstatě technologický problém ovšem znovuotevírá klasickou debatu o tom, co považujeme za spravedlivé, což ale není otázka technického řešení, ale spíše právní filosofie. Zajímavým důsledkem je přesun pozornosti správců údajů k tomu, kde získat data, která neobsahují předchozí diskriminační rozhodnutí. Jednou z možností, jak řešit tento problém je použití tzv. *Generative Adversial Networks*, které byly již zmíněny v části týkající se anonymizace a *big data.* Tento postup vytváření umělých dat pro trénování se v současnosti využívá zejména k tvorbě obrázků, do budoucna je ale možné předpokládat větší všestrannost.[310] Ani tento přístup ovšem neřeší zmíněnou otázku toho, co je to spravedlivé rozhodnutí. Můžeme si sice vytvořit „férová“ data, ale jaká data to budou?

4.2.4 Zásada transparentnosti a právo na vysvětlení

Souvisejícím problémem je otázka existence práva na vysvětlení, které je z textu GDPR dovozováno některými dozorovými úřady i experty.[311] V tomto kontextu se nejedná o právo na vysvětlení dle předchozí tuzemské úpravy, tedy dle §21 zákona o ochraně osobních údajů[312], které sloužilo subjektům údajů v situacích, kdy se domnívaly (ale nevěděly to s

[310]DATATILSYNET. *Artificial intelligence and privacy*, s. 26 [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

[311]Debatu původně vyvolal zejm. následující článek; GOODMAN, Bryce a Seth FLAXMAN. European Union regulations on algorithmic decision-making and a ‘‘right to explanation’’. *AI Magazine* [online]. 2017, **38**(3) [cit. 2018-10-27]. DOI: 10.1609/aimag.v38i3.2741. Dostupné z: https://ora.ox.ac.uk/objects/uuid:593169ee-0457-4051-9337-e007064cf67c/download_file?safe_filename=euregs.pdf&file_format=application%2Fpdf&type_of_work=Journal+article

[312] Zákon č. 101/2000 Sb., o ochraně osobních údajů.

jistotou), že je zpracování jejich osobních údajů protiprávní.[313] Ekvivalentem tohoto práva na vysvětlení dle předchozí tuzemské úpravy je v nové úpravě možnost vznést námitku proti zpracování osobních údajů.[314] Právem na vysvětlení je dále míněno právo subjektu údajů na vysvětlení automatizovaného (algoritmického) rozhodnutí, které se jej týká.[315] Jde tedy o právo na vysvětlení konkrétního rozhodnutí poté, co daný systém rozhodl.[316] Pro úplnost dodávám, že v textu rozlišuji mezi vysvětlením charakteristiky systému a vysvětlením jednotlivých rozhodnutí, což vychází ze zjednodušení reálného stavu. Striktně vzato, pokud jsou zmíněné systémy deterministické, tedy při dodání totožného vstupu systém vždy přinese totožný výstup, by kompletní vysvětlení charakteristiky systému vždy také obsahovalo vysvětlení všech možných případů, logicky tedy i všech minulých případů.[317] Rozdělení vychází z toho, že představa práva na takovéto úplné vysvětlení je, již jenom z praktických důvodů, neproveditelná, když takovým úplným vysvětlením by bylo pouze poskytnutí kompletního modelu komukoliv, kdo o to požádá. Nejenže vývoj těchto modelů představuje pro jednotlivé správce značnou investici, ale je navíc pochybné, nakolik by povinnost na požádání poskytnout složitý matematický model odpovídala charakteru a účelu práva na vysvětlení.

Právo je dovozováno zejména ze spojení článku 22 (3)[318] s recitálem 71[319], případně ze článků 13 a 14 ve spojení s recitály 60 – 62, či ze článku 15 ve spojení s recitálem 63.[320] V celém GDPR

[313] KUČEROVÁ, Alena a kolektiv. Zákon o ochraně osobních údajů. Komentář. 1. vydání, Praha: C. H. Beck, 2012, s. 278 – 286, ISBN 978-80- 7179-226-0

[314] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Práva subjektů údajů: Základní příručka k GDPR [online]. 5.3.2018 [cit. 2018-10-27]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

[315] ROSSI, Francesca. Artificial Intelligence: Potential Benefits and Ethical Considerations. *European Parliament: Briefing* [online]. [cit. 2018-10-27]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf

[316] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 184, ISBN 978-3-319-57959-7.

[317] SELBST, Andrew a Julia POWLES. Meaningful information and the right to explanation. International Data Privacy Law [online]. 2017, 7(4), 233-242 [cit. 2018-10-29]. DOI: 10.1093/idpl/ipx022. ISSN 2044-3994. Dostupné z: http://academic.oup.com/idpl/article/7/4/233/4762325

[318] *„V případech uvedených v odst. 2 písm. a) a c) provede správce údajů **vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů**, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.“* (zdůraznění doplněno)

[319] *„ (…) V každém případě by se na takové zpracování měly vztahovat vhodné záruky, které by měly zahrnovat konkrétní informování subjektu údajů a právo na lidský zásah, na vyjádření svého názoru, **na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a na napadnutí tohoto rozhodnutí.** Toto opatření by se nemělo týkat dítěte“ (*zdůraznění doplněno)

[320] WACHTER, Sandra, Brent MITTELSTADT a Luciano FLORIDI. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, **7**(2), 76-

je právo na vysvětlení explicitně zmíněno pouze v recitálu 71, který ovšem (jako recitál, tedy součást preambule) nemůže být sám o sobě závazný, slouží tedy pouze jako interpretační vodítko při výkladových nejasnostech článků[321], což tvoří první argument proti existenci zmíněného práva. Při absenci předchozí výslovné úpravy tohoto práva, a tedy analogicky při absenci úpravy této povinnosti na straně správce osobních údajů, je případné pokutování nebo jiné vymáhání nedodržování této povinnosti potenciálně v rozporu s článkem 4, odstavcem 1 Listiny základních práv a svobod[322], dle kterého „*povinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod"*, případně s článkem 47[323] Listiny základních práv Evropské unie.[324] Pro neexistenci práva svědčí také historický výklad, když úmysl toto právo v normě nezakotvit naznačuje přesunutí zmíněného práva z textu článku 22 (v tehdejším návrhu Evropského parlamentu článku 20) do právně nezávazné preambule.[325] Ve prospěch existence práva by tak případně mohl svědčit pouze výklad teleologický, tedy výklad usilující o vystižení smyslu, respektive cíle právní normy.[326] Uznání práva by vedlo k naplnění zásady transparentnosti, a tím i k větší ochraně práv subjektů údajů.

Další teoretická možnost dovození zmíněného práva leží v článcích 13 až 14, které se týkají poskytování informací subjektům údajů, ve spojení s recitály 60 – 62. Článek 13 (2), pís. f mluví o povinnosti správce poskytnout subjektu údajů informace o skutečnosti*, „že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech* ***smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků*** *takového zpracování pro subjekt údajů"* (zdůraznění

99. DOI: 10.1093/idpl/ipx005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005

[321] Tamtéž.

[322] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

[323] Listina základních práv Evropské unie (Charta základních práv EU), vyhlášená pod č. 111/2009 Sb. m. s.

[324] WACHTER, Sandra, Brent MITTELSTADT a Luciano FLORIDI. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, **7**(2), 76-99. DOI: 10.1093/idpl/ipx005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005

[325] WACHTER, Sandra, Brent MITTELSTADT a Luciano FLORIDI. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, **7**(2), 76-99. DOI: 10.1093/idpl/ipx005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005

[326] Tamtéž, s. 136.

doplněno). Tato zvláštní informační povinnost stanovuje povinnost správce informovat např. na základě práce se kterými vstupními údaji dochází k automatizovanému rozhodnutí. Informování musí proběhnout *smysluplně*, tedy tak, aby subjekt údajů měl reálnou šanci postup pochopit.[327] Dle jiných autorů spojení *„smysluplné informace týkající se použitého postupu"* (anglicky *„meaningful information about the **logic** involved"*, zdůraznění doplněno), které se opakuje v článcích 13 až 15, představuje právo na vysvětlení nehledě na to, jestli je doslova použit obrat „právo na vysvětlení".[328] Zdá se ovšem, že ani z tohoto článku nelze dovodit tvrzené právo na vysvětlení, když nejde o *ex post* vysvětlení konkrétního rozhodnutí, protože z dikce první věty druhého odstavce článku 13 vyplývá, že jde o poskytnutí informací, které *„(…) poskytne správce subjektu údajů **v okamžiku získání osobních údajů***" (zdůraznění doplněno). Okamžik získání osobních údajů musí logicky předcházet rozhodnutí, tato povinnost tedy zahrnuje poskytnutí obecných informací o systému ještě před tím, než vůbec k danému rozhodnutí může dojít.

Poslední možností dovození práva z textu GDPR představuje článek 15 ve spojení s recitálem 63. Článek 15[329] v odstavci prvním, písmenu h stanovuje právo subjektu údajů získat přístup k informaci o skutečnosti*, „že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech **smysluplné informace týkající se použitého postupu**, jakož i významu a **předpokládaných důsledků** takového zpracování pro subjekt údajů"* (zdůraznění doplněno), s tím že recitál 63 doplňuje, že „k*aždý subjekt údajů by proto měl mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány, kdo jsou příjemci osobních údajů, **v čem spočívá logika automatizovaného zpracování osobních údajů** a jaké*

[327] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 154, ISBN 978-80-7502-288-2.

[328] SELBST, Andrew D a Julia POWLES. Meaningful information and the right to explanation. *International Data Privacy Law* [online]. 2017, **7**(4), 233-242 [cit. 2018-11-26]. DOI: 10.1093/idpl/ipx022. ISSN 2044-3994. Dostupné z: http://academic.oup.com/idpl/article/7/4/233/4762325

[329] V českém znění je nadpis článku nepřesně, respektive restriktivně, přeložen jako *„Právo subjektu údajů na přístup k osobním údajům"*, jde ovšem o právo na přístup nejen k osobním údajům, ale také k dalším informacím, které jsou pro zpracování důležité (srov. anglickou verzi titulku *„Right of access by the data subject")*. Dle PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018, s. 163, ISBN 978-80-7502-288-2.

mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování" (zdůraznění doplněno). Oproti právu na informace, kdy je třeba informace poskytnout již ve chvíli získání osobních údajů (v případě získání informací přímo od subjektu údajů)[330], respektive v přiměřené lhůtě po získání, nejpozději však do 1 měsíce (v případě, kdy informace nebyly získány přímo od subjektu údajů)[331], je právo na přístup k osobním údajům aktivním právem subjektů údajů, tedy správci vzniká povinnost ve chvíli, kdy subjekt údajů o přístup požádá.[332] Z toho, pro účely tvrzeného práva na vysvětlení, vyplývá, že v tomto případě je z časového hlediska možné, aby subjekt údajů požádal o přístup k osobním údajům poté, co nastane automatizované rozhodnutí, a to právě vzhledem k aktivnímu charakteru práva. Argumentem proti je ovšem jazykové znění článku 15, ve kterém je zmínka o *„předpokládaných důsledcích"* (*envisaged consequences* v anglickém znění, či *angestrebten Auswirkungen* ve znění německém) takového zpracování osobních údajů. I tato ustanovení se tak vztahují k předchozímu informování subjektu údajů o funkčnosti systému, nikoliv k následnému vysvětlení určitého rozhodnutí.[333]

Pouze právní interpretací textu současné úpravy tedy nelze jednoznačně dovodit existenci práva na vysvětlení. Probíhající debatu neobjasnila zcela ani WP29 ve svých Pokynech, i když se spíše přiklonila na stranu neexistence práva na vysvětlení. WP29 vylučuje možnost opření existence práva o článek 15, podle kterého by správce *„měl subjektu údajů poskytnout informace o předpokládaných důsledcích zpracování, spíše než vysvětlovat* ***konkrétní*** *rozhodnutí"*[334] (zdůraznění původní). Dále pak potvrzuje, že článek 15 a články 13 a 14 se vztahují k témuž okruhu informací: *„Čl. 15 odst. 1 písm. h) opravňuje subjekt údajů* ***k získání***

[330] Článek 13, odstavec 1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679

[331] Článek 14, odstavec 3 tamtéž.

[332] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 129, ISBN 978-80-7554-097-3.

[333] WACHTER, Sandra, Brent MITTELSTADT a Luciano FLORIDI. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, **7**(2), 76-99. DOI: 10.1093/idpl/ipx005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005

[334] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679,* s. 27[online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

stejných informací *o výhradně automatizovaném rozhodování, včetně profilování, jaké jsou požadovány v čl. 13 odst. 2 písm. f) a v čl. 14 odst. 2 písm. g) (…)"*[335] (zdůraznění doplněno). Logicky tedy ani články 13 a 14 nemohou být základem zmíněného práva, když nepřináší nic navíc oproti článku 15, pro který je explicitně vyloučena možnost, aby byl základem pro právo na vysvětlení. Zatímco WP29 v podstatě vyloučila možnost použití těchto dvou zdrojů pro konstrukci práva na vysvětlení, k článku 22 ve spojení s recitálem 71 se dále nevyjádřila. První verze pokynů pak obsahovala v části věnované „osvědčeným postupům" následující pasáž: „*Information about the categories of data that have been or will be used in the profiling or decision making process and why these are considered pertinent will generally be more relevant than* ***providing a complex mathematical explanation*** *about how algorithms or machine learning work,* ***although the latter should also be provided if this is necessary to allow experts to further verify how the decision–making process works****."* (zdůraznění doplněno). Tato část budila nejasnosti[336] ohledně toho, kdy a jakým způsobem bude nutné poskytnout komplexní matematické vysvětlení, v druhé verzi pokynů se tato věta ovšem již nevyskytuje. Zdá se tedy, že se WP29 definitivně přiklonila na stranu neexistence práva na vysvětlení. To ovšem neznamená, že toto právo nemůže být do budoucna projudikováno. Stejně tak se, *de lege ferenda*, může stát součástí závazné části právního předpisu. Tento postup by ostatně, dle mého názoru, přinesl subjektům údajů lepší možnosti výkonu svých práv.

4.2.5 K povaze vysvětlení

Z právního pohledu má vysvětlení přinést subjektu údajů pochopení vnitřní logiky systému, což má zabránit nezákonnému (tedy zejména diskriminačnímu) rozhodování a přinést možnost rozhodnutí napadnout. V návaznosti na technický úvod lze shrnout, že vysvětlení v obecném smyslu je při složitých algoritmech využívajících strojové učení v zásadě nemožné. Jinými slovy, možnost „otevřít černou skříňku", tedy detailně vysvětlit jakým způsobem došel

[335] Tamtéž, s. 27.

[336] VEALE, Michael a Lilian EDWARDS. *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling* [online]. 2018, **34**(2), 398-404 [cit. 2018-11-26]. DOI: 10.1016/j.clsr.2017.12.002. ISSN 02673649. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S026736491730376X

systém k určitému způsobu rozhodování a proč následně rozhodnul určitým způsobem v konkrétním případě, je povahou těchto algoritmů velice limitována. Možnost takového vysvětlení ovšem naráží nejen na technické obtíže, ale také na neochotu správců údajů uvádět ke svým algoritmům bližší vysvětlení, když tyto algoritmy považují za obchodní tajemství a jejich vývoj byl pro správce velice nákladný. Nakonec lze zmínit obavu, že v případě, kdy subjekty údajů přesně ví, jakým způsobem algoritmus rozhoduje, mohou pro příště záměrně změnit své chování tak, aby byl systém zmanipulován.

Důležitým bodem v debatě o povaze vysvětlení je návrh na podávání srovnávacích vysvětlení (*counterfactual explanations*).[337] Tento typ vysvětlení vychází z premisy, že subjekt údajů ve skutečnosti nemá zájem o vysvětlení interního fungování systému, ale chce vědět následující: 1) co se stalo (proč byla žádost odmítnuta?), 2) informace pro napadení rozhodnutí, pokud se subjekt údajů domnívá, že je rozhodnutí nespravedlivé a 3) i když bylo rozhodnutí spravedlivé, co může pro příště subjekt dělat pro zvýšení svých šancí.[338] Místo vysvětlení fungování neurální sítě srovnávací vysvětlení poskytuje informaci ohledně závislosti externích vstupů na výsledku a jejich možných změnách. Jinak řečeno, vychází se z toho, že jednotlivce nezajímá fungování systému, ale zajímá ho dopad tohoto systému na jeho případ a možnosti změny tohoto dopadu. Toto je klíčové rozlišení, když interní fungování algoritmu se může sestávat z miliónů různých proměnných, jejichž vysvětlení je v určitých případech téměř nemožné, ne-li zcela. Externí faktory se oproti tomu vztahují k charakteristikám subjektu údajů, kterým tak jednotlivec nejenže dobře rozumí, ale zároveň ví, co by měl dělat pro příště. Příkladem je situace, kdy je osobě A zamítnuta žádost o půjčku, zároveň je mu ale podáno srovnávací vysvětlení: *„Kdybyste měl příjem 40 000 Kč, místo současných 30 000 Kč, půjčku byste obdržel.“* Toto vysvětlení matematicky představuje nejmenší možnou (smysluplnou) změnu ve vstupu, která může změnit výsledek rozhodnutí.

[337] WACHTER, Sandra, Brent MITTELSTADT a Chris RUSSELL. Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal of Law & Technology* [online]. (forthcoming) [cit. 2018-11-24]. Dostupné z: https://arxiv.org/pdf/1711.00399.pdf

[338] MITTELSTADT, Brent, Sandra WACHTER, David SUTCLIFFE a Chris RUSSELL. Could Counterfactuals Explain Algorithmic Decisions Without Opening the Black Box?. *Oxford Internet Institute* [online]. [cit. 2018-11-24]. Dostupné z: https://www.oii.ox.ac.uk/blog/could-counterfactuals-explain-algorithmic-decisions-without-opening-the-black-box/

Problémem srovnávacích vysvětlení je tzv. efekt „Rašomon“ - pro každý jednotlivý případ odmítnutí bude typicky existovat vícero různých scénářů, které by vedly k přijetí, ovšem tyto alternativní scénáře si budou vzájemně protiřečit.[339] Tedy při složitějších algoritmech změní rozhodnutí např. zvýšení veličiny A, stejně jako snížení veličiny A při současném zvýšení veličiny B.[340] Dalším problémem je, že nejmenší nutná změna se určuje matematickým vzorcem s ohledem na data, ovšem námaha pro změnu jednotlivých veličin se pro jednotlivé subjekty údajů bude lišit. Vzhledem k výše zmíněnému je otázka, jak by měl systém informovat v případě, že srovnávacích vysvětlení, tedy možných scénářů, které by vedly k odlišnému výsledku, bude vícero (co když jich bude 10, 30, 150?). Má systém ukázat jen ta vysvětlení, která sám považuje za nejsnadněji změnitelné, nebo má ukázat všechny? Odpověď není jednoduchá, když nezobrazení všech odpovědí omezuje subjekt údajů v jeho volbě, ovšem zobrazení přílišného množství možností může činit volbu pro subjekt údajů nesrozumitelnou.

Jak bylo pojednáno v technickém úvodu, tzv. dynamický model mění své rozhodování na základě nových vstupních dat, je tedy možné, aby systém podal srovnávací vysvětlení určující, že zvýšení příjmů na 40 000 Kč povede k potvrzení žádosti o půjčku, aby následně půjčku témuž žadateli odmítnul, přestože ten mezitím dosáhnul odpovídajícího příjmu. Takové rozhodnutí by zásadně narušilo důvěru subjektu údajů v algoritmické rozhodování. Na druhé straně je pravděpodobné, že rozhodovací systémy (byť využívající dynamického modelu) nebudou mít v čase přílišné odchylky. Řešením může být též „zmražení“ systému v čase pro tohoto jednotlivého uživatele – tím se ale ovšem opět dostáváme k otázce spravedlnosti.

Zároveň se vysvětlení podává vždy jen jednotlivci, není tak možné bez kontroly ze strany dozorového úřadu účinně odhalit, jestli nedochází k diskriminaci určitých skupin. Tento bod bude vlastní individuálnímu vysvětlení vždy, když z definice jde o vysvětlení jednotlivého rozhodnutí v určitém případě, zatímco pro odhalení systémové diskriminace jsou vhodnější statistické nástroje zaměřené na větší vzorek. I přes zmíněné limitace je zavedení srovnávacích

[339] MOLNAR, Christoph. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.* [online]. 2018 [cit. 2018-11-24]. Dostupné z: https://christophm.github.io/interpretable-ml-book/index.html
[340] Tamtéž.

vysvětlení správným krokem vpřed a možnost prohlédnutí srovnávacích případů je nově možná např. skrze nástroj společnosti Google What-If. I bez užití modelu What-If je případná implementace technicky snadná, jako obecný princip funguje srovnávací vysvětlení stejně dobře pro ty nejkomplexnější neurální sítě jako pro jednoduchou sadu pravidel napsanou na papíře.[341]

Vhodným postupem správce pro plné naplnění zásady transparentnosti se tak jeví v případě komplexních algoritmů vytvoření webového rozhraní, ve kterém by si jednak mohl subjekt údajů prohlédnout srovnávací vysvětlení vztahující ke svému případu, jednak by získal celkový přehled o tom, jak model rozhoduje a jakým způsobem byl vytvořen[342], a to skrze zjednodušený model rozhodování, který by ovšem neodhaloval samotný zdrojový kód a nebyl by tak problematický z hlediska chránění obchodního tajemství. Ohledně problému s množstvím srovnávacích odpovědí by dle mého názoru nejlépe odpovídalo účelu a smyslu právní úpravy, kdyby byly poskytnuty všechny alternativní scénáře, současně s rozdělením do přehledných kategorií. Subjekt údajů by byl např. dotázán: „Které z následujících faktorů můžete nejsnadněji změnit? 1) Příjem, 2) Rozsah současných závazků, 3) Přidání ručení.“ Po zvolení jedné z těchto možností by se zobrazily odpovídající možnosti, s tím, že odpovědi na tyto rozřazovací otázky by mohl subjekt údajů kdykoliv změnit.

[341] Tamtéž.

[342] Pro přehledný dotazník, který se, správcem vyplněný, navrhuje přikládat subjektům údajů vizte MALGIERI, Gianclaudio a Giovanni COMANDÉ. Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law,* s. 28 – 30 [online]. forthcoming, **7**(3) [cit. 2019-03-22]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976

4.3 Dílčí závěr

I přes nejasné znění článku 22 se domnívám, že GDPR obecně zakazuje automatizované individuální rozhodování, které má pro subjekt údajů právní účinky nebo se obdobným způsobem významné dotýká, a k tomuto zákazu přináší výjimky. Při aplikaci této právní úpravy bude obtížné určit, kdy má automatizované individuální rozhodnutí *„právní“* nebo *„obdobné účinky“*, což bylo ilustrováno na případě Facebookového feedu.[343]

Následně byla analyzována zásada přesnosti a nebezpečí spočívající zejm. v nereprezentativnosti tréninkových dat.[344] Nevhodně zvolená (tedy *nepřesná)* tréninková data mohou vést k diskriminačním rozhodnutím. I přes rozvoj řady nástrojů pro posouzení algoritmů neexistuje jednoduchá odpověď na otázku, jaké rozhodnutí je spravedlivé, když se skrze nové technologie vracíme zpět k tradiční právně-filosofické debatě.

V další části bylo dovozeno, že právo na vysvětlení v současné právní úpravě zřejmě není obsaženo, ovšem jeho zavedení by bylo pozitivním krokem pro práva subjektů údajů. Z tohoto důvodu bylo *de lege ferenda* doporučeno zakotvit zmíněné právo mezi právně závazné články GDPR, oproti současnému zařazení mezi recitály. S odkazem na technické obtíže spojené s vysvětlením automatizovaného rozhodnutí (black box) bylo doporučeno kombinovat srovnávací vysvětlení spolu s obecným vysvětlením fungování modelu.

Vzhledem k rozšiřujícímu se využívání algoritmů umožňující automatizované individuální rozhodování naráží úprava v tomto směru na přirozené limity možností kontroly ze strany dozorových úřadů.

[343] Dle rozvrhu práce pro roky 2019-2020 chystá Sbor pokyny ohledně cílení na uživatele sociální sítí, které by se mohly dotknout i výše zmíněného problému. Dle: THE EUROPEAN DATA PROTECTION BOARD. *Work program* [online]. [cit. 2019-02-19]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

[344] Pro stručný přehled dalších častých statistických omylů, které mohou ovlivnit funkčnost či správné chápání výsledků určitého modelu, vizte: GECKOBOARD. *Common Data Mistakes to Avoid* [online]. [cit. 2019-03-18]. Dostupné z: https://www.geckoboard.com/learn/data-literacy/statistical-fallacies/

5 Závěrečné zhodnocení, úvahy *de lege ferenda*

„The future is already here — it's just not very evenly distributed."[345]

Vzhledem k současnému stupni vývoje technologií a vzhledem k vlivu, které vybrané technologické společnosti mají na život jednotlivce, je příznačné, že se dnes již tolik nesetkáváme s názory volajícími po zdrženlivosti států při regulaci[346], ale naopak je patrný opačný trend.[347]

Na základě analýzy vybraných technologických aspektů lze konstatovat, že GDPR je správným a nutným krokem vpřed, s tím že základní principy se jeví být jako skutečně odolné (technologickým) změnám (*futureproof)*. Zároveň se domnívám, že neexistuje přesvědčivá argumentace pro opuštění nebo zmírnění těchto principů pod dojmem současného technologického vývoje. V tomto ohledu tedy plně souhlasím s Evropským inspektorem ochrany údajů, že není otázkou, jestli se na *big data*, ale i obecně na nové technologie, budou uplatňovat zásady ochrany osobních údajů, ale jakým způsobem se tyto zásady mají uplatnit.[348] Je legitimní vyžadovat, aby společnosti, které přicházejí s inovativními způsoby

[345] GIBSON, William. The Science in Science Fiction - interview with William Gibson. *National Public Radio* [online]. 1999 [cit. 2018-11-27]. Dostupné z: https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction

[346] Ve své době populární Deklarace nezávislosti kyberprostoru zpochybňovala autoritu států stejně jako reálnou možnost vymáhat právo v kyberprostoru. Toto smýšlení dobře vystihují hned úvodní věty Deklarace: *„Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."* Dle: BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. 8.2.1996 [cit. 2018-11-19]. Dostupné z: https://www.eff.org/cyberspace-independence

[347] Příkladem je nedávný projev CEO společnosti Apple, Tima Cooka, pronesený na The International Conference of Data Protection and Privacy Commissioners: *„Fortunately, this year, you've shown the world that good policy and political will can come together to protect the rights of everyone. We should celebrate the transformative work of the European institutions tasked with the successful implementation of the GDPR. (…) It is time for the rest of the world—including my home country—to follow your lead."*
Dle: COOK, Tim. Keynote address from Tim Cook, CEO, Apple Inc. *European Data Protection Supervisor - YouTube channel* [online]. [cit. 2018-11-19]. Dostupné z: https://www.youtube.com/watch?v=kVhOLkIs20A

[348] EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

zpracování osobních údajů, přicházely také s inovativními způsoby naplnění ochrany osobních údajů.

Přestože nelze GDPR v této oblasti upřít značný přínos, nelze se také domnívat, že jde o právní úpravu ideální a bezproblémovou. V jednotlivých oblastech jsou již dnes patrné jisté mezery. Pro právní úpravu *big data* a automatického individuálního rozhodování by, dle mého názoru, největší přínos přinesly následující dvě změny.

Právní úprava jednak v současné podobě neumožňuje plný výkon práv subjektů údajů, a to zejména vzhledem k nejasnému znění úpravy práva na vysvětlení. *De lege ferenda* se proto doporučuje přesunout úpravu práva na vysvětlení z preambule do některého z článků, a to i s vědomím technických obtíží spojených se zpětnou analýzou konkrétních rozhodnutí komplexních algoritmů. Pro naplnění účelu a smyslu tohoto práva se proto, s přihlédnutím právě ke zmíněným technickým potížím, navrhuje použití kombinace srovnávacího vysvětlení spolu s obecnými informacemi o fungování systému. Potvrzení zmíněného práva může vést k efektivnějšímu výkonu práv osob, a tím se může stát důležitým nástrojem v boji proti možné diskriminaci ze strany algoritmů.

Dále by měla existovat větší podpora pro systém umožňující subjektu údajů rozhodovat z jednoho místa o použití osobních údajů ve všech službách, které používá. Pro takový systém existuje vícero názvů *(personal data services, personal data store, personal cloud*), které označují, na kterou část takového systému se klade definičně větší důraz. Dle mého názoru by vhodnou kombinací tzv. *sticky policies* a *dashboardu* vznikl skutečně efektivní a intuitivní systém, naplňující smysl a účel právní normy. Právní podporou by bylo zavedení příslušného kodexu chování, respektive uznání tohoto kodexu jako všeobecně platného. Otázkou spíše ekonomickou, jejíž řešení si netroufám ani odhadovat, je, jakými pobídkami a jestli vůbec by měla Evropská unie motivovat společnosti k přijetí tohoto modelu.

K hodnocení GDPR obecně

Jednou z klíčových změn, které nová úprava přinesla, je volba odlišné formy právního předpisu, a to nařízení (oproti předchozí směrnicové úpravě). Je nesporné, že předchozí

směrnicová úprava vedla k často podstatným rozdílům mezi jednotlivými členskými státy, což narušovalo cíl zjednodušit pohyb dat v rámci EU. Přesto GDPR na mnoha místech dává překvapivě široký prostor členským státům pro odchýlení se od obecné úpravy, a to zejména skrze článek 23. Výsledkem by v souhrnu mohl být opět vznik více či méně rozdílných právních režimů v jednotlivých členských státech.[349] Současně je běžným omylem[350] označování GDPR za směrnici, což může spolu s výše naznačenou možností opětovného drolení právní úpravy dále přispět ke zmatení subjektů údajů, stejně jako správců. Přestože byla právní forma zvolena vzhledem k ambicím sjednotit právní režim vhodně, pro dosažení skutečně jednotícího účinku bude třeba také zdrženlivosti členských států v přijímání národních odchylek. V opačném případě je jednotící ambice ohrožena.

Důležitou součástí účinné ochrany osobních údajů je také znalost vlastních práv ze strany subjektů údajů. Blížící se datum účinnosti[351] předpisu doprovázela silná mediální pozornost, která je pro přijetí nového právního předpisu značně neobvyklá. Na jedné straně se tak zvýšilo právní vědomí občanů Evropské unie ohledně svých práv a povinností, na straně druhé „mediální zákonodárství" v mnoha ohledech pohled na věc zkreslilo, když docházelo ke zdůrazňování panující nejistoty ohledně GDPR a stejně tak ke zdůrazňování „hrozících likvidačních pokut"[352]. V tomto ohledu je třeba ocenit osvětovou roli Úřadu pro ochranu osobních údajů, který mj. kromě účasti na řadě debat[353] vytvořil mikroweb k GDPR[354], a také

[349] VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017, s. 184-185, ISBN 978-3-319-57959-7.

[350] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Desatero omylů ohledně GDPR* [online]. [cit. 2018-11-17]. Dostupné z: https://www.uoou.cz/desatero-omylu-o-gdpr/ds-4818/archiv=0&p1=3938

[351] GDPR používá místo „účinnosti" označení „použitelnost". Vzhledem k ustálenému používání termínu „účinnost" v teorii práva používám v práci právě tento termín, jinak obsahově shodný. Předpis nabyl účinnosti 25.5.2018.

[352] A oproti těmto „hrozícím likvidačním pokutám" pochopitelně následně mnozí jednotlivci nabízeli, za náležitý obnos, právní ochranu. Jak trefně poznamenal Morávek: *„Řada osob vycítila šanci vybrat od spoluobčanů hospodářské přebytky a (obrazně řečeno) prodává amulety a další propriety (směrnice, programy a další), které mají dotyčného ochránit před blížícím se strašákem, který dle legend, které o něj zejména nezasvěcení šíří, nejméně dští síru a přivodí dotyčnému (nebude-li podle stanoveného imperativu postupovat) útrapy, které si nezadají s deseti egyptskými ranami."* Dle: MORÁVEK, Jakub. Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?. *Právní rozhledy*. 2018(13-14), 487.

[353] Za rok 2018 šlo o bezmála 90 seminářů či konferencí. Dle: ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Úřad hostil diskuzi o GDPR za účasti amerických studentů* [online]. [cit. 2019-03-21]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=33442

[354] https://gdpr.uoou.cz/ . Naopak lze kritizovat to, že doménu gdpr.cz si Úřad nezajistil a ta slouží ke komerční prezentaci služeb spojených s GDPR, s tím, že vzhledem ke svému silnému doménovému jménu je to právě

se, skrze osobu ředitele Odboru pro styk s veřejností, JUDr. Jiřího Žůrka[355], podílel na vydání přehledné a kvalitní publikace, která má dle mého názoru potenciál zasáhnout i širší publikum. Kromě činnosti ÚOOÚ lze zmínit také prakticky orientovanou publikaci Ministerstva průmyslu a obchodu („*Příručka pro přípravu malých a středních firem na GDPR"*)[356] či celoevropsky vytvářené přehledy pro podniky i subjekty údajů. Zmíněné publikace jsou důležité i pro to, že lze předpokládat, že jen malá část správců a subjektů osobních údajů bude číst a porozumí přímo textu regulace.[357] Naopak negativně lze hodnotit zpoždění, se kterým jsou vydávány některé pokyny Sboru. Přestože je toto prodlení pochopitelné a je obvykle vyváženo precizní argumentací v pokynech, nezdá se mi z hlediska právní jistoty vhodné, aby některé důležité pokyny vycházely téměř s půlročním zpožděním oproti účinnosti předpisu.

Nejde ovšem jen o znalost individuálních práv, ale také o to, jakou důležitost ochraně osobních údajů lidé přikládají a nakolik je pro ně náročné či naopak snadné se svých práv domoci. V řadě výše zmíněných případů bude fakticky existovat nerovnost v případném sporu. Jednotlivec nespokojený např. s podmínkami určité aplikace bude často vzhledem k časové náročnosti a povaze věci demotivován zabývat se podrobněji tímto problémem. Oproti tomu společnosti, pro které je sběr dat základem obchodního modelu, nemají problém vynaložit značné prostředky pro řešení takového sporu. Tento faktický problém řeší existence několika neziskových organizací, které se zabývají výlučně řešením takovýchto případů. Za všechny lze opětovně zmínit noyb, za kterou stojí známý „právní aktivista" Max Schrems.

Vzhledem k tzv. „bruselskému efektu"[358] je možné, že se GDPR stane „zlatým standardem" ochrany osobních údajů i ve světě. Tento vývoj jsme mohli v minulosti pozorovat i v jiných

stránka gdpr.cz, která se ve výsledcích vyhledávání na dotaz „GDPR" zobrazuje jako první. Obdobně ani stránka gdpr.eu není oficiálním zdrojem informací.

[355] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), s. 129, ISBN 978-80-7554-097-3.

[356] MINISTERSTVO PRŮMYSLU A OBCHODU. *Příručka pro přípravu malých a středních firem na GDPR* [online]. 27.4.2018 [cit. 2018-11-27]. Dostupné z: https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/podpurna-opatreni-mpo/prirucka-pro-pripravu-malych-a-strednich-firem-na-gdpr--236691/

[357] BLUME, Peter. Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*[online]. **2**(3), 130-136 [cit. 2018-11-18]. Dostupné z: https://academic.oup.com/idpl/article/2/3/130/660534?searchresult=1

[358] BRADFORD, Anu. The Brussels Effect. *Northwestern University Law Review* [online]. **107**(1) [cit. 2018-11-24]. Dostupné z:

odvětvích, předávání osobních údajů do zahraničí je navíc vzhledem k jejich povaze technicky snadné. K roku 2017 mělo 120 zemí právní úpravu ochrany osobních údajů, která odpovídá minimálním mezinárodním standardům, ještě v roce 2011 to bylo jen 76 zemí.[359] Většina těchto národních úprav je silně ovlivněna evropským přístupem k ochraně osobních údajů.[360] Některé státy pak přistupují k doslovnému kopírování vybraných částí GDPR.[361] Přestože lze do budoucna očekávat další rozšíření evropského standardu ochrany osobních údajů, bezprostředně po účinnosti GDPR jsme byli svědky také opačného trendu, kdy např. některé webové stránky blokovaly návštěvníky s evropskou IP adresou (kteří nejspíše tvořili zanedbatelné procento z celkových návštěv, a tedy i příjmů), když se jako výhodnější jevilo tyto návštěvníky blokovat, než se zabývat tím, jestli se GDPR bude aplikovat a jak případně dostát povinnostem z něj plynoucích. Nezbývá než doufat, že se toto překvapivé a nevhodné řešení stane věcí minulosti.[362]

Předpokládá se, že překotný vývoj moderních technologií bude pokračovat i nadále.[363] Další rozvoj technologií má jistě revoluční potenciál, mělo by jít ale o revoluci, která je konzistentní s evropskými hodnotami, mezi které patří mimo jiné právo na ochranu soukromého života a právo na ochranu osobních údajů. Pro naplnění tohoto cíle je nutné na evropské úrovni dosáhnout účinné a moderní právní úpravy. V tomto směru je GDPR dobrým a správným krokem, když, i přes některé zmíněné mezery, vhodně reaguje na dosavadní stupeň vývoje

https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1081&context=nulr

[359] GREENLEAF, Graham. Global Tables of Data Privacy Laws and Bills (5th Ed 2017). *Privacy Laws & Business International Report* [online]. 2017, (145) [cit. 2018-11-24]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986

[360] BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law* [online]. 2016, **6**(2), 77-78 [cit. 2018-11-24]. DOI: 10.1093/idpl/ipw006. ISSN 2044-3994. Dostupné z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw006

[361] Příkladem je návrh zákona „Privacy Act" ve státě Washington, který obsahuje formulaci „*Controllers that engage in profiling must disclose such profiling to the consumer at or before the time personal data is obtained, including* ***meaningful information about the logic involved and the significance and envisaged consequences of the profiling****."* Dle: Washington privacy act: Senate bill 5376. Dostupné z: http://lawfilesext.leg.wa.gov/biennium/2019-20/Htm/Bills/Senate%20Bills/5376.htm

[362] Jako příklad lze uvést deník Los Angeles Times, který k listopadu 2018 návštěvníky z EU stále blokuje. http://www.tribpub.com/gdpr/latimes.com/

[363] Dle tzv. Moorova zákona se počet tranzistorů na integrovaném obvodu, a tím i výkon, v pravidelném intervalu (co dva roky) znásobí. Podobně pak v komunikacích (Gilderův zákon). Dle: LASKY, Jack. Moore`s law. Salem Press Encyclopedia of Science [online]. 2017 [cit. 2018-11-26]. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds.

technologií. Principy ochrany osobních údajů jsou definovány dostatečně obecně na to, aby právní úprava byla skutečně odolná dalším změnám. Schopnost reagovat na budoucí technologické změny bude ale vyžadovat další práci, a to zejména vydávání stanovisek dozorových úřadů, stejně jako např. využívání kodexů chování pro nově vzniklé *„kategorie subjektů údajů“.*

Zdroje

Právní předpisy

Evropská úmluva o ochraně lidských práv ve znění Protokolů č. 11 a 14

Listina základních práv Evropské unie (Charta základních práv EU), vyhlášená pod č. 111/2009 Sb. m. s.

Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Francie)

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). [cit. 2018-10-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011

Směrnice 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

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

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

Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

Směrnice Rady 2004/113/ES ze dne 13. prosince 2004, kterou se zavádí zásada rovného zacházení s muži a ženami v přístupu ke zboží a službám a jejich poskytování

Smlouva o Evropské unii

Smlouva o fungování Evropské unie

The Constitution of the United States of America (ústava Spojených států amerických, USA)

Úmluva Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

Washington privacy act: Senate bill 5376. Dostupné z: http://lawfilesext.leg.wa.gov/biennium/2019-20/Htm/Bills/Senate%20Bills/5376.htm
Zákon č. 257/2016 Sb., o spotřebitelském úvěru

Zákon č. 101/2000 Sb., o ochraně osobních údajů

Dokumenty WP29 a úřadů

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation (WP 203)* [online]. [cit. 2018-10-29]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 05/2014 on Anonymisation Techniques* [online]. [cit. 2018-11-01]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* [online]. [cit. 2018-11-25]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* s. 15 [online]. [cit. 2018-11-25]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (WP221*), s. 2, [online]. [cit. 2018-11-15]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

CPVP - COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE. *Rapport Big Data* [online]. [cit. 2018-11-25]. Dostupné z: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf

DATATILSYNET. *Big Data - privacy principles under pressure*[online]. 2013 [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/big-data-engelsk-web.pdf

DATATILSYNET. *Artificial intelligence and privacy* [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Doporučení CM/Rec (2010) 13 Výboru ministrů členským státům o ochraně osob s ohledem na automatizované zpracování osobních údajů. [online]. [cit. 2018-11-23]. Dostupné z: https://www.uoou.cz/doporuceni-cm-rec-2010-13-vyboru-ministru-clenskym-statum-o-ochrane-osob-s-ohledem-na-automatizovane-zpracovani-osobnich-udaju/ds-1801

EUROPEAN COMMISSION. *Special Eurobarometer 431 - Data protection* [online]. [cit. 2018-11-05].

EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 7/2015: Meeting the challenges of big data*[online]. 19.11.2015 [cit. 2018-10-28]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *#BigData: Discrimination in data-supported decision making* [online]. (2018) [cit. 2018-10-28]. DOI: 10.2811/343905. Dostupné z: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

INFORMATION COMMISSIONER'S OFFICE (ICO). *Anonymisation: managing data protection risk code of practice* [online]. [cit. 2018-11-01]. Dostupné z: https://ico.org.uk/media/1061/anonymisation-code.pdf

INFORMATION COMMISSIONER'S OFFICE (ICO). *Big data, artificial intelligence, machine learning and data protection* [online]. [cit. 2018-10-29]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

INFORMATION COMMISSIONER'S OFFICE (ICO). *Data sharing code of practice* [online]. [cit. 2018-11-25]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

INFORMATION COMMISSIONER'S OFFICE (ICO). *Privacy in mobile apps: Guidance for app developers* [online]. [cit. 2018-11-25]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

MINISTERSTVO PRŮMYSLU A OBCHODU. *Příručka pro přípravu malých a středních firem na GDPR* [online]. 27.4.2018 [cit. 2018-11-27]. Dostupné z: https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/podpurna-opatreni-mpo/prirucka-pro-pripravu-malych-a-strednich-firem-na-gdpr--236691/

OFFICE OF FAIR TRADING. *Personalised Pricing: Increasing Transparency to Improve Trust*[online]. [cit. 2018-10-29]. Dostupné z: http://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*[online]. 2018, 6.2.2018 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro souhlas podle nařízení 2016/679 (WP259)* [online]. [cit. 2018-10-29]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

RADA VLÁDY PRO LIDSKÁ PRÁVA. *Zpráva o stavu lidských práv v České republice v roce 2015* [online]. [cit. 2018-11-21]. Dostupné z: https://www.vlada.cz/assets/ppov/rlp/dokumenty/zpravy-lidska-prava-cr/zprava-2015.pdf

Knihy

AGENTURA EVROPSKÉ UNIE PRO ZÁKLADNÍ PRÁVA. *Příručka evropského práva v oblasti ochrany údajů*. Lucemburk: Úřad pro publikace Evropské unie, 2015. ISBN 978-92-871-9933-1.

AMITAI, Etzioni a Christopher RICE. *Privacy in a Cyber Age: Policy and Practice*. Palgrave, 2015. ISBN 978-1-137-51396-0.

BAROCAS, Solon, Arvind NARAYANAN a Moritz HARDT. *Fairness and machine learning: Limitations and Opportunities* [online]. fairmlbook.org, 2018 [cit. 2019-03-21]. Dostupné z: https://fairmlbook.org/

BUYYA, Rajkumar, Rodrigo CALHEIROS a Amir Vahid DASTJERDI. *Big data: Principles and paradigms*. Cambridge, MA: Elsevier/Morgan Kaufmann, 2016. ISBN 978-012-8053-942.

CRAIG, Paul a Gráinne DE BÚRCA. *EU law: text, cases, and materials*. Sixth edition. New York: Oxford University Press, 2015. ISBN 9780198714927.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. Handbook on European data protection law. Lucemburk: Úřad pro publikace Evropské unie, 2018. ISBN 978-92-871-9849-5.

FORGÓ, Nikolaus, Stefanie HÄNOLD a Benjamin SCHÜTZE. The Principle of Purpose Limitation and Big Data. IN CORRALES, Marcelo, Mark FENWICK a Nikolaus FORGÓ. *'New Technology, Big Data and the Law*. Springer Singapore, 2017, s. 17-42. ISBN 978-981-10-5038-1.

JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

KUČEROVÁ, Alena a kolektiv. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání, Praha: C. H. Beck, 2012. ISBN 978-80- 7179-226-0

KÜHN, Zdeněk. Lidská práva v zajetí dvě stě let starých doktrín. AGHA, Petr a kol. *Budoucnost státu?.* Praha: Academia, 2017, s. 155-160. Společnost (Academia). ISBN 978-80-200-2681-1.

LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. Oxford studies in European law. ISBN 978-019-8718-239.

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.

NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.

NGUYEN, Carolyn a Jeffrey FRIEDBERG. A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy, IN: O'HARA, Kieron, Michael WAIDNER a Mireille HILDEBRANDT. *Digital Enlightenment Yearbook 2013*. IOS Press, 2013. ISBN 978-1-61499-295-0

NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

O`NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, 2016. ISBN 0553418815.

O`REILLY, Tim, Mike LOUKIDES, Julie STEELE a Colin HILL. *How Data Science Is Transforming Health Care*. O'Reilly Media, 2012. ISBN 9781449356187.

PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ, Michaela MILATOVÁ, Adéla PINKAVOVÁ, Dominik VÍTEK, Štefan KRÁĽ a Ferdinand FOŘT. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě - Komentář*. Praha: Leges, 2018. ISBN 978-80-7502-288-2.

SOLOVE, Daniel. *Understanding Privacy*. Harvard University Press, 2008. ISBN 978-0674027725.

TOMÁŠEK, Michal, Vladimír TÝČ, Jiří MALENOVSKÝ, et al. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017. Student (Leges). ISBN 978-80-7502-184-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017. ISBN 978-3-319-57959-7.

WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. ŠIMÍČEK, Vojtěch. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.

ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG), ISBN 978-80-7554-097-3.

Odborné publikace

ATHALYE, Anish, Logan ENGSTROM, Andrew ILYAS a Kevin KWOK. Synthesizing Robust Adversarial Examples. *ArXiv preprint* [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1707.07397.pdf

BAROCAS, Solon a Andrew SELBST. Big Data's Disparate Impact. *California Law Review* [online]. [cit. 2018-11-19]. Dostupné z: http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf

BELLOVIN, Steven M., Preetam K. DUTTA a Nathan REITINGER. Privacy and Synthetic Datasets. *Stanford Technology Law Review, Forthcoming* [online]. [cit. 2019-02-26]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3255766

BLUME, Peter. Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*[online]. **2**(3), 130-136 [cit. 2018-11-18]. Dostupné z: https://academic.oup.com/idpl/article/2/3/130/660534?searchresult=1

BORGESIUS, Frederik Zuiderveen. Discrimination, Artificial Intelligence and Algorithmic Decision-Making. *Council of Europe* [online]. [cit. 2019-03-18]. Dostupné z: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

BRADFORD, Anu. The Brussels Effect. *Northwestern University Law Review* [online]. **107**(1) [cit. 2018-11-24]. Dostupné z: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1081&context=nulr

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*[online]. 2016, **3**(1) [cit. 2018-11-24]. DOI: 10.1177/2053951715622512. ISSN 2053-9517. Dostupné z: http://journals.sagepub.com/doi/10.1177/2053951715622512

BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law* [online]. 2016, **6**(2), 77-78 [cit. 2018-11-24]. DOI: 10.1093/idpl/ipw006. ISSN 2044-3994. Dostupné z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw006

BYGRAVE, Lee A. Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. *Computer Law & Security Report* [online]. 2001, **17**, 67-76 [cit. 2018-11-23]. Dostupné z: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf

CALANDRINO, Joseph A., Ann KILZER, Arvind NARAYANAN, Edward W. FELTEN a Vitaly SHMATIKOV. "You Might Also Like: " Privacy Risks of Collaborative Filtering. *2011 IEEE Symposium on Security and Privacy* [online]. IEEE, 2011, 2011, , 231-246 [cit. 2019-02-26]. DOI: 10.1109/SP.2011.40. ISBN 978-1-4577-0147-4. Dostupné z: http://ieeexplore.ieee.org/document/5958032/

CRAWFORD, Kate. The Hidden Biases in Big Data. *Harvard Business Review* [online]. 2013 [cit. 2018-11-26]. Dostupné z: https://hbr.org/2013/04/the-hidden-biases-in-big-data

CUSTERS, Bart a Helena URŠIČ. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. DOI: 10.1093/idpl/ipv028. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipv028

GOODFELLOW, Ian, Jonathon SHLENS a Christian SZEGEDY. Explaining and harnessing adversarial examples. *ArXiv preprint* [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1412.6572.pdf

GOODMAN, Bryce a Seth FLAXMAN. European Union regulations on algorithmic decision-making and a ‘‘right to explanation’’. *AI Magazine* [online]. 2017, 38(3) [cit. 2018-10-27]. DOI: 10.1609/aimag.v38i3.2741. Dostupné z: https://ora.ox.ac.uk/objects/uuid:593169ee-0457-4051-9337-e007064cf67c/download_file?safe_filename=euregs.pdf&file_format=application%2Fpdf&type_of_work=Journal+article

GREENLEAF, Graham. Global Tables of Data Privacy Laws and Bills (5th Ed 2017). *Privacy Laws & Business International Report* [online]. 2017, (145) [cit. 2018-11-24]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986

HILDEBRANDT, Mireille. Esclaus de les macrodades. O no? / Slaves to Big Data. Or Are We?. *IDP. Revista de Internet, Derecho y Política* [online]. [cit. 2018-11-15]. Dostupné z: https://idp.uoc.edu/articles/abstract/10.7238/idp.v0i17.1977/

KOSINSKI, Michal, David STILLWELL a Thore GRAEPEL. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* [online]. 2013, **110**(15), 5802-5805 [cit. 2018-11-24]. DOI: 10.1073/pnas.1218772110. ISSN 0027-8424. Dostupné z: http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110

KRAMER, Adam D. I., Jamie E. GUILLORY a Jeffrey T. HANCOCK. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National*

Academy of Sciences [online]. 2014, **111**(24), 8788-8790 [cit. 2018-11-26]. DOI: 10.1073/pnas.1320040111. ISSN 0027-8424. Dostupné z: http://www.pnas.org/cgi/doi/10.1073/pnas.1320040111

KUNER, Christopher, Dan SVANTESSON, Fred CATE, Orla LYNSKEY a Christopher MILLARD. Machine learning with personal data: is data protection law smart enough to meet the challenge?. *International Data Privacy Law*[online]. 2017, **7**(1) [cit. 2018-11-17]. Dostupné z: https://academic.oup.com/idpl/article/7/1/1/3782694

LEIBENGER, Dominik, Frederik MÖLLERS, Anna PETRLIC, Ronald PETRLIC a Christoph SORGE. Privacy Challenges in the Quantified Self Movement – An EU Perspective. *Proceedings on Privacy Enhancing Technologies* [online]. 2016, **2016**(4), 315-334 [cit. 2018-10-30]. DOI: 10.1515/popets-2016-0042. ISSN 2299-0984. Dostupné z: http://content.sciendo.com/view/journals/popets/2016/4/article-p315.xml

LYNSKEY, Orla. Deconstructing data protection: the 'added value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*. 2014, **63**(3), 569-597. DOI: 10.1017/S0020589314000244. ISSN 0020-5893. Dostupné také z: http://www.journals.cambridge.org/abstract_S0020589314000244

MAYER-SCHÖNBERGER, Viktor a Yann PADOVA. Regime Change? Enablig Big Data through Europe`s new data protection regulation. *The Columbia Science & Technology Law Review* [online]. **17** [cit. 2018-11-15]. Dostupné z: http://stlr.org/download/volumes/volume17/SchonbergerPadova.pdf

MCDONALD, Aleecia a Lorrie CRANOR. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* [online]. [cit. 2018-11-16]. Dostupné z: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

MOEREL, Lokke a Corien PRINS. Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things. *SSRN Electronic Journal* [online]. [cit. 2018-11-24]. DOI: 10.2139/ssrn.2784123. ISSN 1556-5068. Dostupné z: http://www.ssrn.com/abstract=2784123

MORÁVEK, Jakub. Když dva dělají totéž, není to totéž, aneb GDPR jako přestupková amnestie?. *Právní rozhledy*. **2018**(13-14), 487.

MUNIR, Abu Bakar, Siti Hajar Mohd YASIN a Firdaus MUHAMMAD-SUKKI. Big Data: Big Challenges to Privacy and Data Protection. *International Journal of Computer and Information Engineering* [online]. **9**(1) [cit. 2018-10-31]. Dostupné z: https://waset.org/publications/10000669/big-data-big-challenges-to-privacy-and-data-protection

NARAYANAN, Arvind a Vitaly SHMATIKOV. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)* [online]. 2008 [cit. 2018-10-30]. Dostupné z: https://arxiv.org/pdf/cs/0610105.pdf

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* [online]. [cit. 2018-11-16]. Dostupné z: https://www.uclalawreview.org/pdf/57-6-3.pdf

PEARSON, Siani a Marco CASASSA-MONT. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. *Computer* [online]. 2011, **44**(9), 60-68 [cit. 2018-11-26]. DOI: 10.1109/MC.2011.225. ISSN 0018-9162. Dostupné z: http://ieeexplore.ieee.org/document/5959137/

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* [online]. 2018, **10**(1), 40-81 [cit. 2019-02-26]. DOI: 10.1080/17579961.2018.1452176. ISSN 1757-9961. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

RHOEN, Michiel a Qing Yi FENG. Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science. *International Data Privacy Law*. 2018, 8(2), 140-159. DOI: 10.1093/idpl/ipy005. ISSN 2044-3994. Dostupné také z: https://academic.oup.com/idpl/article/8/2/140/5045225

ROSSI, Francesca. Artificial Intelligence: Potential Benefits and Ethical Considerations. *European Parliament: Briefing* [online]. [cit. 2018-10-27]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf

ROUVROY, Antoinette. "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. *Council of Europe, Directorate General of Human Rights and Rule of Law* [online]. [cit. 2018-11-16]. Dostupné z: https://works.bepress.com/antoinette_rouvroy/64/

RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law* [online]. **3**(2) [cit. 2018-11-01]. Dostupné z: https://academic.oup.com/idpl/article/3/2/74/709082#12469607

SALEIRO, Pedro, Benedict KUESTER, Abby STEVENS, Ari ANISFELD, Loren HINKSON, Jesse LONDON a Rayid GHANI. Aequitas: A Bias and Fairness Audit Toolkit. *Center for Data Science and Public Policy - University of Chicago* [online]. [cit. 2018-11-20]. Dostupné z: https://arxiv.org/pdf/1811.05577.pdf

SEAVER, Nick. Captivating algorithms: Recommender systems as traps. *Journal of Material Culture* [online]. 2018 [cit. 2019-02-19]. DOI: 10.1177/1359183518820366. ISSN 1359-1835. Dostupné z: http://journals.sagepub.com/doi/10.1177/1359183518820366

SELBST, Andrew a Julia POWLES. Meaningful information and the right to explanation. International Data Privacy Law [online]. 2017, 7(4), 233-242 [cit. 2018-10-29]. DOI: 10.1093/idpl/ipx022. ISSN 2044-3994. Dostupné z: http://academic.oup.com/idpl/article/7/4/233/4762325

SCHWARTZ, Paul a Daniel SOLOVE. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *N.Y.U. Law Review* [online]. **86**(6) [cit. 2018-10-31]. Dostupné z: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs

SU, Jiawei, Danilo Vasconcellos VARGAS a Kouichi SAKURAI. One Pixel Attack for Fooling Deep Neural Networks. *ArXiv*[online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1710.08864.pdf

THE ROYAL SOCIETY. *Machine learning: the power and promise of computers that learn by example* [online]. [cit. 2018-11-17]. ISBN 978-1-78252-259-1. Dostupné z: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf

TZANOU, Maria. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law* [online]. **3**(2) [cit. 2018-12-06]. Dostupné z: https://academic.oup.com/idpl/article/3/2/88/709116?searchresult=1

VEALE, Michael, Reuben BINNS a Lilian EDWARDS. Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* [online]. 2018, **376**(2133) [cit. 2019-02-26]. DOI: 10.1098/rsta.2018.0083. ISSN 1364-503X. Dostupné z: http://rsta.royalsocietypublishing.org/lookup/doi/10.1098/rsta.2018.0083

VEALE, Michael a Lilian EDWARDS. Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review* [online]. 2017, **16**(18) [cit. 2019-02-20]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

WACHTER, Sandra a Brent MITTELSTADT. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review* [online]. [cit. 2019-02-20]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

WARREN, Samuel a Louis BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. **4**(5) [cit. 2018-12-06]. Dostupné z: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

WACHTER, Sandra. Privacy: Primus Inter Pares: Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights. *The Alan Turing Institute* [online]. [cit. 2019-02-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514

WACHTER, Sandra, Brent MITTELSTADT a Luciano FLORIDI. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, 7(2), 76-99. DOI: 10.1093/idpl/ipx005. ISSN

2044-3994. Dostupné také z: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005

WACHTER, Sandra, Brent MITTELSTADT a Chris RUSSELL. Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal of Law & Technology* [online]. (forthcoming) [cit. 2018-11-24]. Dostupné z: https://arxiv.org/pdf/1711.00399.pdf

WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law School Legal Scholarship Repository* [online]. [cit. 2018-12-06]. Dostupné z: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.cz/&httpsredir=1&article=1647&context=fss_papers

YOM-TOV, Elad a Shaul LEV-RAN. Adverse Reactions Associated With Cannabis Consumption as Evident From Search Engine Queries. *JMIR Public Health and Surveillance* [online]. 2017, 3(4) [cit. 2018-10-30]. DOI: 10.2196/publichealth.8391. ISSN 2369-2960. Dostupné z: http://publichealth.jmir.org/2017/4/e77

ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* [online]. **47**(2) [cit. 2018-11-15]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646#

ZARSKY, Tal. The Privacy–Innovation Conundrum. Lewis & Clark Law Review, [online]. 19(1) [cit. 2018-10-29]. Dostupné z: https://law.lclark.edu/live/files/19418-lcb191art4zarskyfinalpdf

ZARSKY, Tal. Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society. *University of Miami Law Review* [online]. 2004, **58**(4) [cit. 2018-11-27]. Dostupné z: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1398&context=umlr

ZARSKY, Tal. Transparent Predictions. *University of Illinois Law Review* [online]. 2013, 2013(4), 1503-1570 [cit. 2018-11-26]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324240

ŽLIOBAITĖ, Indrė. Measuring discrimination in algorithmic decision making. *Data Mining and Knowledge Discovery* [online]. 2017, 31(4), 1060-1089 [cit. 2018-10-28]. DOI: 10.1007/s10618-017-0506-1. ISSN 1384-5810. Dostupné z: http://link.springer.com/10.1007/s10618-017-0506-1

Kvalifikační práce

NOVÁK, Daniel. *Problémy ochrany soukromí a osobních údajů v právu EU*, Brno, 2011. Disertační práce. Právnická fakulta Masarykovy univerzity. Vedoucí práce Filip Křepelka**.**

Internetové zdroje

AMERICAN CIVIL LIBERTIES UNION. 5 Problems with national ID cards [online]. [cit. 2018-12-06]. Dostupné z: https://www.aclu.org/other/5-problems-national-id-cards

APPLE. *Human Interface Guidelines: Requesting Permission* [online]. [cit. 2018-11-25]. Dostupné z: https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/

Audit-AI. *GitHub* [online]. [cit. 2018-11-21]. Dostupné z: https://github.com/pymetrics/audit-ai

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. 8.2.1996 [cit. 2018-11-19]. Dostupné z: https://www.eff.org/cyberspace-independence

Blue Feed, Red Feed. *The Wall Street Journal* [online]. [cit. 2018-11-23]. Dostupné z: http://graphics.wsj.com/blue-feed-red-feed/#/immigration

BROCKELL, Gillian. Dear tech companies, I don't want to see pregnancy ads after my child was stillborn. *The Washington Post* [online]. [cit. 2019-02-19]. Dostupné z: https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/?noredirect=on&utm_term=.b2d2ffc8da03

COOK, Tim. Keynote address from Tim Cook, CEO, Apple Inc. *European Data Protection Supervisor - YouTube channel* [online]. [cit. 2018-11-19]. Dostupné z: https://www.youtube.com/watch?v=kVhOLkIs20A

CROLL, Alistair. Big data is our generation's civil rights issue, and we don't know it: What the data is must be linked to how it can be used. *Radar* [online]. [cit. 2018-10-29]. Dostupné z: http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html

CROCKETT, Emily. How Twitter taught a robot to hate. *Vox*[online]. [cit. 2018-11-17]. Dostupné z: https://www.vox.com/2016/3/24/11299034/twitter-microsoft-tay-robot-hate-racist-sexist

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters* [online]. [cit. 2018-11-17]. Dostupné z: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

DEEPMIND. *DeepMind Ethics & Society* [online]. [cit. 2018-11-25]. Dostupné z: https://deepmind.com/applied/deepmind-ethics-society/

DIFFERENTIAL PRIVACY TEAM. Learning with Privacy at Scale. *Apple Machine Learning Journal* [online]. **1**(8) [cit. 2018-11-21]. Dostupné z: https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html#DMNS06

DUHIGG, Charles. How Companies Learn Your Secrets. *New York Times* [online]. [cit. 2018-11-01]. Dostupné z: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0

EUROPEAN DIGITAL RIGHTS. *Comparison of the Parliament and Council Text on the General Data Protection Regulation* [online]. [cit. 2018-11-23]. Dostupné z: https://edri.org/files/EP_Council_Comparison.pdf

EVROPSKÁ KOMISE. *Jednotný digitální trh* [online]. [cit. 2018-11-18]. Dostupné z: https://ec.europa.eu/commission/priorities/digital-single-market_cs

FairML. *GitHub* [online]. [cit. 2018-11-21]. Dostupné z: https://github.com/adebayoj/fairml

FELTRON, Nicholas. *Annual reports* [online]. [cit. 2018-10-30]. Dostupné z: http://feltron.com/index.html

FEW, Stephen. Dashboard Confusion Revisited. *Perceptual Edge* [online]. [cit. 2018-11-26]. Dostupné z: https://www.perceptualedge.com/articles/visual_business_intelligence/dboard_confusion_revisited.pdf

FLACY, Mike. HAPIfork tracks your eating habits, encourages healthier eating. *Digital Trends* [online]. [cit. 2018-10-29]. Dostupné z: https://www.digitaltrends.com/home/hapifork-tracks-your-eating-habits-encourages-healthier-eating/

FORBRUKERRÅDET - NORWEGIAN CONSUMER COUNCIL. *Deceived by design* [online]. [cit. 2018-11-25]. Dostupné z: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

FRANKEL, Joseph. One Coffee? Your Total Is Some Personal Data. *New York Magazine - Intelligencer* [online]. 2018 [cit. 2018-11-26]. Dostupné z: http://nymag.com/intelligencer/2018/08/shiru-cafs-offer-students-free-coffee-for-harvested-data.html

GARUN, Natt. Egg Minder smart tray lets you remotely check the freshness of your eggs. *Digital Trends* [online]. [cit. 2018-10-29]. Dostupné z:

https://www.digitaltrends.com/home/egg-minder-smart-tray-lets-you-remotely-check-the-freshness-of-your-eggs/

GECKOBOARD. *Common Data Mistakes to Avoid* [online]. [cit. 2019-03-18]. Dostupné z: https://www.geckoboard.com/learn/data-literacy/statistical-fallacies/

GIBSON, Lydialyle. A Rosetta Stone for Earthquakes. In: *Harvard Magazine* [online]. 2017 [cit. 2018-11-19]. Dostupné z: https://harvardmagazine.com/2017/11/earthquakes-around-the-world

GIBSON, William. The Science in Science Fiction - interview with William Gibson. *National Public Radio* [online]. 1999 [cit. 2018-11-27]. Dostupné z: https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction

CHANNEL 4. *Your Data* [online]. [cit. 2018-11-25]. Dostupné z: https://www.channel4.com/4viewers/your-data

KAMARINOU, Dimitra, Christopher MILLARD a Jatinder SINGH. Machine Learning with Personal Data. *Queen Mary University of London, School of Law - Legal Studies Research Paper* [online]. 2016 [cit. 2018-11-18]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811

KOUBSKÝ, Petr. Hrnečku, vař! řekl Mark Zuckerberg. *Deník N* [online]. [cit. 2019-02-23]. Dostupné z: https://denikn.cz/66855/hrnecku-var-rekl-mark-zuckerberg/?ref=tit
KOUBSKÝ, Petr. Kořeny digitálního světa. *067.cz* [online]. [cit. 2018-11-26]. Dostupné z: https://067.cz/archiv/14/koreny-digitalniho-sveta.html

KOUBSKÝ, Petr. Mysl je slepenec improvizací. *067.cz*[online]. [cit. 2018-11-27]. Dostupné z: https://067.cz/archiv/58/mysl-je-slepenec-improvizaci.html

KOUBSKÝ, Petr. Poznámky k digitalizaci člověka. *067.cz* [online]. [cit. 2018-10-30]. Dostupné z: https://067.cz/archiv/33/poznamky-k-digitalizaci-cloveka.html

KUNER, Christopher. A Chekhovian view of privacy for the internet age. *Oxford University Press Blog* [online]. 2015 [cit. 2018-12-08]. Dostupné z: https://blog.oup.com/2015/10/chekhov-privacy-internet-age/

KURFÜRSTOVÁ, Jana. Strojové učení kouzla zbavené. *EDTECH KISK* [online]. [cit. 2018-11-17]. Dostupné z: https://medium.com/edtech-kisk/strojov%C3%A9-u%C4%8Den%C3%AD-kouzla-zbaven%C3%A9-e066d79ebe51

LASKY, Jack. Moore`s law. *Salem Press Encyclopedia of Science* [online]. 2017 [cit. 2018-11-26]. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds.

LARSON, Jeff, Surya MATTU, Lauren KIRCHNER a Julia ANGWIN. How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica* [online]. [cit. 2018-11-19]. Dostupné z: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

LEE, Peter. Learning from Tay's introduction. *Official Microsoft Blog*[online]. [cit. 2018-11-17]. Dostupné z: https://secure.wikimedia.org/wikipedia/cs/wiki/Hlavn%C3%AD_strana

LENAERTS, Koen. *The General Data Protection Regulation five months on* [online]. [cit. 2018-12-18]. Dostupné z: https://www.youtube.com/watch?v=fZaKPaGbXNg

LINN, Allison. Microsoft researchers win ImageNet computer vision challenge. *Official Microsoft Blog* [online]. [cit. 2018-11-18]. Dostupné z: https://blogs.microsoft.com/ai/microsoft-researchers-win-imagenet-computer-vision-challenge/

LOMAS, Natasha. YouTube under fire for recommending videos of kids with inappropriate comments. *TechCrunch* [online]. [cit. 2019-02-19]. Dostupné z: https://techcrunch.com/2019/02/18/youtube-under-fire-for-recommending-videos-of-kids-with-inappropriate-comments/

MITTELSTADT, Brent, Sandra WACHTER, David SUTCLIFFE a Chris RUSSELL. Could Counterfactuals Explain Algorithmic Decisions Without Opening the Black Box?. *Oxford Internet Institute* [online]. [cit. 2018-11-24]. Dostupné z: https://www.oii.ox.ac.uk/blog/could-counterfactuals-explain-algorithmic-decisions-without-opening-the-black-box/

MOEREL, Lokke. *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof* [online]. [cit. 2018-11-13]. Dostupné z: https://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf

Netflix Prize - Frequently Asked Questions: Is there any customer information in the dataset that should be kept private? [online]. 2009 [cit. 2018-10-30]. Dostupné z: https://www.netflixprize.com/faq.html

NOYB - EUROPEAN CENTER FOR DIGITAL RIGHTS. *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook* [online]. [cit. 2018-11-25]. Dostupné z: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

PEARSON, Jordan. Why An AI-Judged Beauty Contest Picked Nearly All White Winners. *Vice - Motherboard*[online]. 2016 [cit. 2018-11-19]. Dostupné z: https://motherboard.vice.com/en_us/article/78k7de/why-an-ai-judged-beauty-contest-picked-nearly-all-white-winners

PFEFFER, Jan a Hana GAWLASOVÁ. Big Data právním pohledem. *Hospodářské noviny* [online]. [cit. 2018-10-29]. Dostupné z: https://ihned.cz/c1-60126320-big-data-pravnim-pohledem

Pokyny k uplatňování směrnice Rady 2004/113/ES v pojišťovnictví s ohledem na rozsudek Soudního dvora Evropské unie ve věci C-236/09 (Test-Achats) [online]. [cit. 2019-3-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52012XC0113(01)&from=GA

RASMUSSEN, Anders Fogh. The West's dangerous lack of tech strategy. *Politico* [online]. [cit. 2019-03-22]. Dostupné z: https://www.politico.eu/article/opinion-the-wests-dangerous-lack-of-tech-strategy/

ROSER, Max a Hannah RITCHIE. Technological Progress. In: *Our World in Data* [online]. [cit. 2018-11-17]. Dostupné z: https://ourworldindata.org/technological-progress

RYGE, Leif. *ImageNet Roulette* [online]. [cit. 2019-03-22]. Dostupné z: https://imagenet-roulette.paglen.com/

SZYMIELEWICZOVÁ, Katarzyna. Your digital identity has three layers, and you can only protect one of them. *Quartz* [online]. [cit. 2019-02-19]. Dostupné z: https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

STŘEDOČESKÝ KRAJ. *Hlášení závad - Středočeský kraj* [online]. [cit. 2018-11-26]. Dostupné z: https://musimetoopravit.cz/

THE EUROPEAN DATA PROTECTION BOARD. *Work program* [online]. [cit. 2019-02-19]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

TOKMETZIS, Dimitri, Maurits MARTIJN, Riffy BOL a Foeke POSTMA. Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app. *De Correspondent* [online]. [cit. 2018-12-17]. Dostupné z: https://decorrespondent.nl/8481/heres-how-we-found-the-names-and-addresses-of-soldiers-and-secret-agents-using-a-simple-fitness-app/412999257-6756ba27

TOONDERS, Joris. Data is the new oil of the digital economy. *Wired* [online]. [cit. 2018-10-27]. Dostupné z: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/

Uber drivers demand their data. *The Economist* [online]. [cit. 2019-03-22]. Dostupné z: https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Desatero omylů ohledně GDPR* [online]. [cit. 2018-11-17]. Dostupné z: https://www.uoou.cz/desatero-omylu-o-gdpr/ds-4818/archiv=0&p1=3938

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Práva subjektů údajů: Základní příručka k GDPR* [online]. 5.3.2018 [cit. 2018-10-27]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Tisková zpráva: Nařízení o ePrivacy jako doplněk k GDPR* [online]. [cit. 2018-12-19]. Dostupné z: https://www.uoou.cz/tiskova-zprava-narizeni-o-nbsp-eprivacy-jako-doplnek-k-nbsp-gdpr/d-27454/p1=1017

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Úřad hostil diskuzi o GDPR za účasti amerických studentů* [online]. [cit. 2019-03-21]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=33442

VARSHNEY, Kush. Introducing AI Fairness 360. *IBM* [online]. 2018 [cit. 2018-11-20]. Dostupné z: https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

VEALE, Michael a Lilian EDWARDS. *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling* [online]. 2018, **34**(2), 398-404 [cit. 2018-11-26]. DOI: 10.1016/j.clsr.2017.12.002. ISSN 02673649. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S026736491730376X

VINCENT, James. Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech. *The Verge*[online]. [cit. 2018-11-19]. Dostupné z: https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai

VOLNÁ, Eva. *Neuronové sítě 1* [online]. Vydání druhé. Ostrava: Ostravská univerzita v Ostravě, 2008 [cit. 2018-10-28]. Dostupné z: http://www1.osu.cz/~volna/Neuronove_site_skripta.pdf

WEINBERGER, David. Playing with AI Fairness. *What-If Tool*[online]. [cit. 2018-11-21]. Dostupné z: https://pair-code.github.io/what-if-tool/ai-fairness.html

Judikatura, rozhodování dozorových úřadů, stanoviska generálních advokátů

DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS). *Investigation into the combining of personal data by Google: Report of Definitive Findings* [online]. 2013 [cit. 2018-11-25]. Dostupné z: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf

DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS). *Summary of investigation report; Microsoft Windows 10 Home and Pro investigation by the Autoriteit Persoonsgegevens (Dutch DPA), August 2017: Public version,* [online]. [cit. 2018-11-25]. Dostupné z: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf

Komise pro veřejné služby v. Pollak, 343 U.S. 451, 467 (1952) (soudce William O. Douglas, separátní votum). Dostupné z: https://supreme.justia.com/cases/federal/us/343/451/

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, 94/2011 Sb.

Planned Parenthood v. Casey, 505 U.S. 833 (1992). Dostupné z: https://supreme.justia.com/cases/federal/us/505/833/

Roe v. Wade, 410 U.S. 113 (1973). Dostupné z: https://supreme.justia.com/cases/federal/us/410/113/

Rozhodnutí EKLP ze dne 11. 7. 1980 ve věci Deklerck v. Belgie, stížnost č. 8307/78.

Rozsudek ESLP ze dne 24. 6. 2004 ve věci von Hannover v. SRN, stížnost č. 59320/00

Rozsudek ESLP ze dne 28. 1. 2003 ve věci Peck v. Spojené království, stížnost č. 44647/98.

Rozsudek Soudního dvora ze dne 1. března 2011. Test-Achats. Věc C-236/09, ECLI:EU:C:2011:100. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=80019&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3975414#Footnote*

Rozsudek Soudního dvora ze dne 6. listopadu 2003. Trestní řízení proti Bodil Lindqvist. Žádost o rozhodnutí o předběžné otázce: Göta hovrätt - Švédsko. Věc C- 101/01, ECLI:EU:C:2003:596. Dostupné z: http://curia.europa.eu/juris/liste.jsf?num=C-101/01

Rozsudek Soudního dvora ze dne 8. dubna 2014. Digital Rights Ireland a další. Spojené věci C-293/12 a C-594/12, ECLI:EU:C:2014:238. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN

Rozsudek Soudního dvora ze dne 9. listopadu 2010. Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3584200

Rozsudek Soudního dvora ze dne 12. listopadu 1969. Erich Stauder v City of Ulm, Sozialamt, Věc C-29/69, ECLI:EU:C:1969:57. Dostupné z: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=29-69&td=ALL

Rozsudek Soudního dvora ze dne 13. května 2014. Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD),Mario Costeja González, Věc C-131/12, ECLI:EU:C:2014:317. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A62012CJ0131

Rozsudek Soudního dvora ze dne 20. prosince 2017. Peter Nowak v. Data Protection Commissioner, Věc C-434/16, ECLI:EU:C:2017:994. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=13042823

Rozsudek Soudního dvora ze dne 29. ledna 2008. Productores de Música de España (Promusicae) v. Telefónica de España SAU, Věc C-275/06, ECLI:EU:C:2008:54. Dostupné z: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06

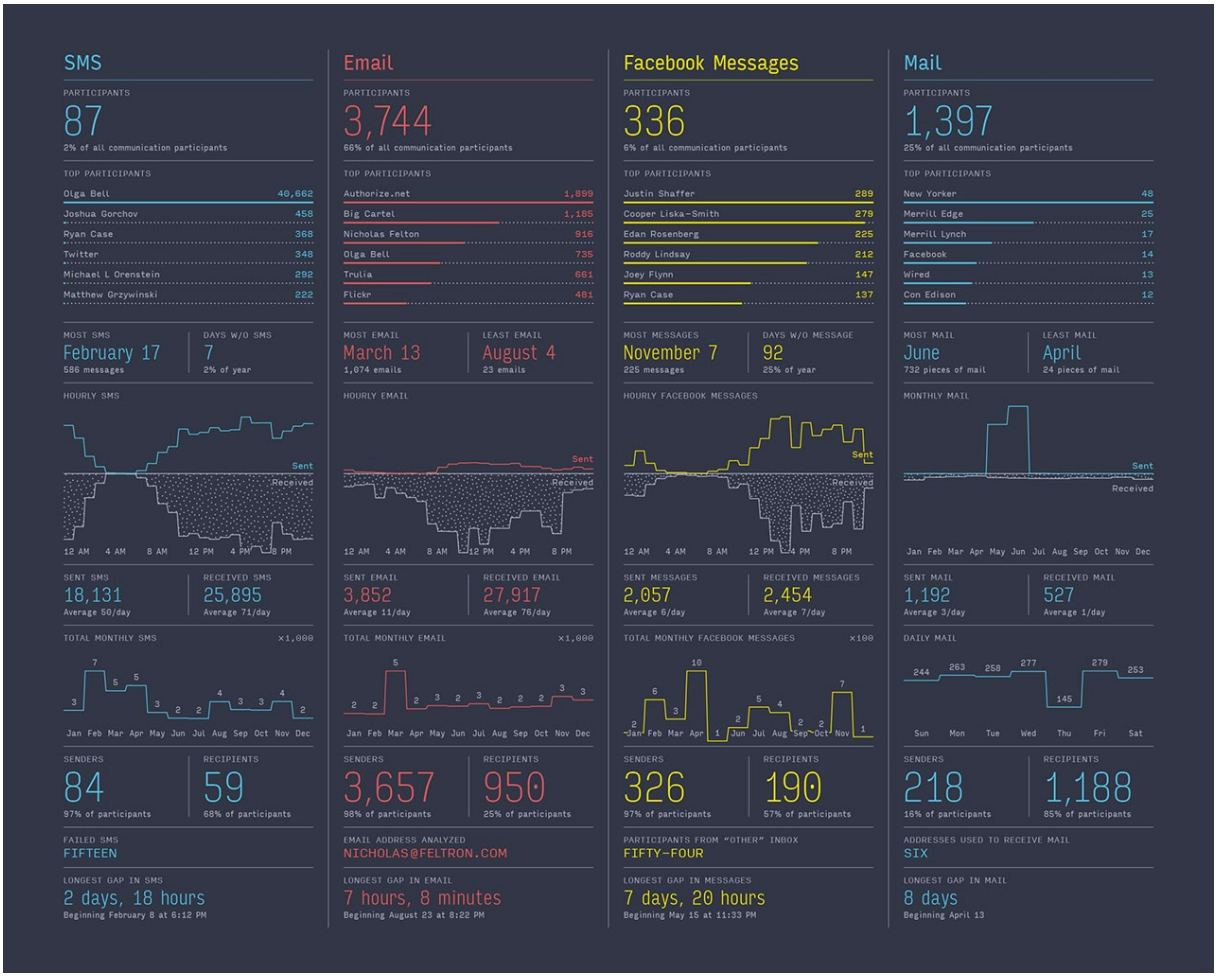
Silverman v. United States, 365 U.S. 505 (1961). Dostupné z: https://supreme.justia.com/cases/federal/us/365/505/

Stanovisko generální advokátky Eleanor Sharpston ve věci spojených věcí C-92/09 a C-93/09 Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:62009CC0092&from=GA

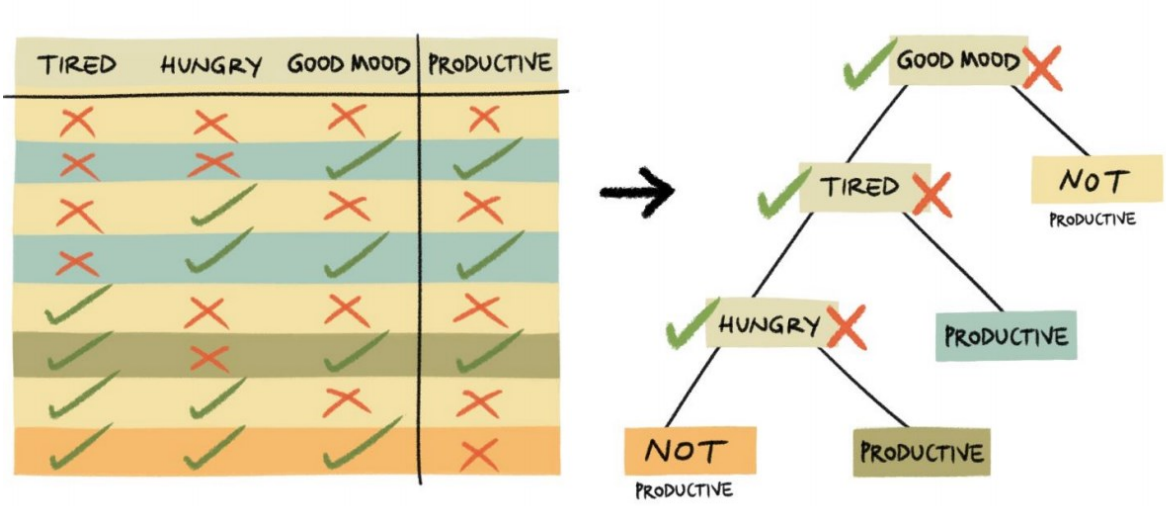
Stanovisko generální advokátky Juliane Kokott ve věci C‑ 236/09 Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=82589&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=3975414#Footnote49

Přílohy

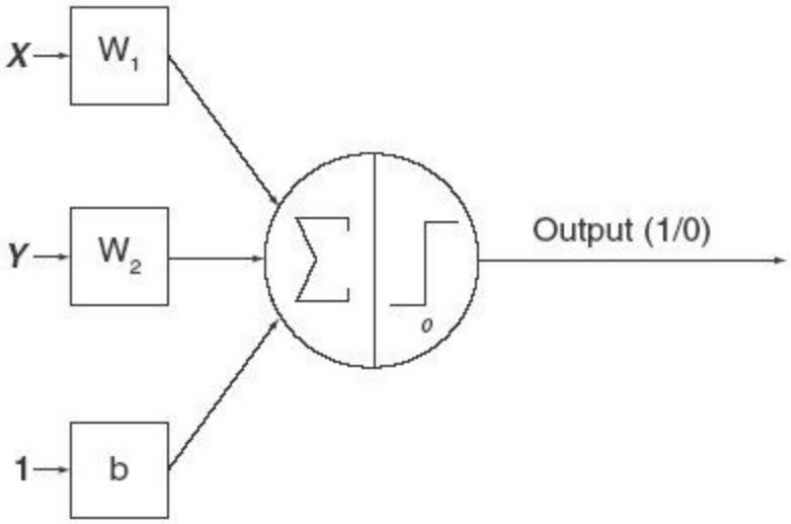
Příloha 1 - Ukázka z "výročních zpráv" ze života Nicholase Feltrona. Jeho výroční zprávy ilustrují možnosti digitalizace a kvantifikace lidského života. Zdroj: FELTRON, Nicholas. Annual reports [online]. [cit. 2018-10-30]. Dostupné z: http://feltron.com/index.html



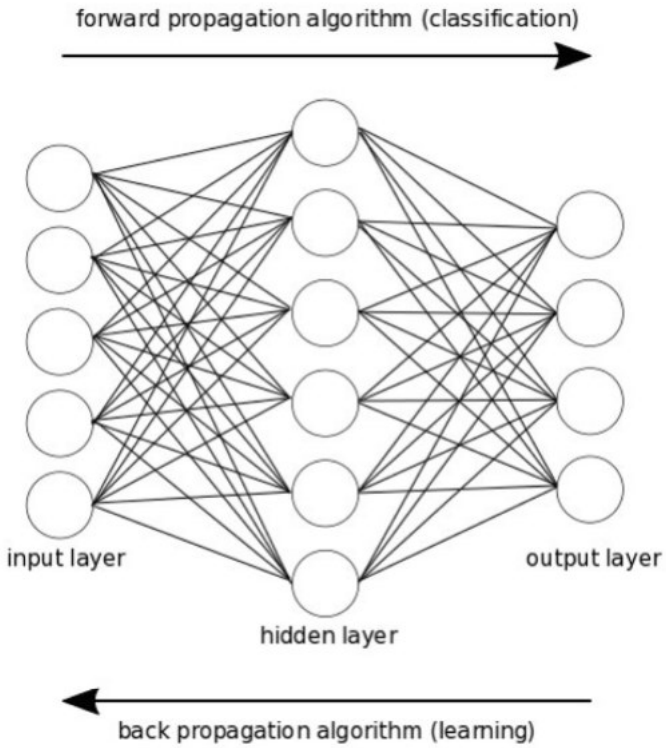
Příloha 2 - Ukázka z "výročních zpráv" ze života Nicholase Feltrona. Jeho výroční zprávy ilustrují možnosti digitalizace a kvantifikace lidského života. Zdroj: FELTRON, Nicholas. Annual reports [online]. [cit. 2018-10-30]. Dostupné z: http://feltron.com/index.html



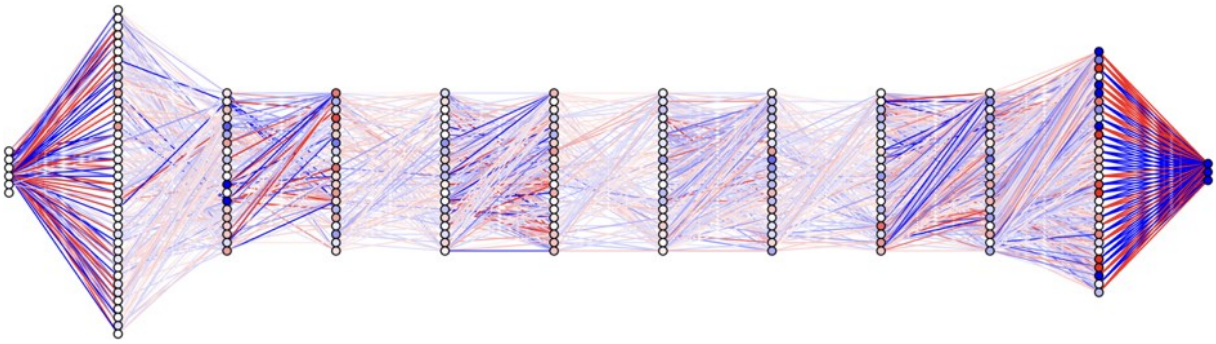
Příloha 3 - Ukázka jednoduchého rozhodovacího stromu, který na základě vstupních dat určuje, zda-li je jedinec produktivní. Proces rozhodování začíná otázkou ohledně dobré nálady (good mood) a postupuje na základě odpovědí směrem dolů. Zdroj: DATATILSYNET. Artificial intelligence and privacy [online]. [cit. 2018-11-17]. Dostupné z: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf



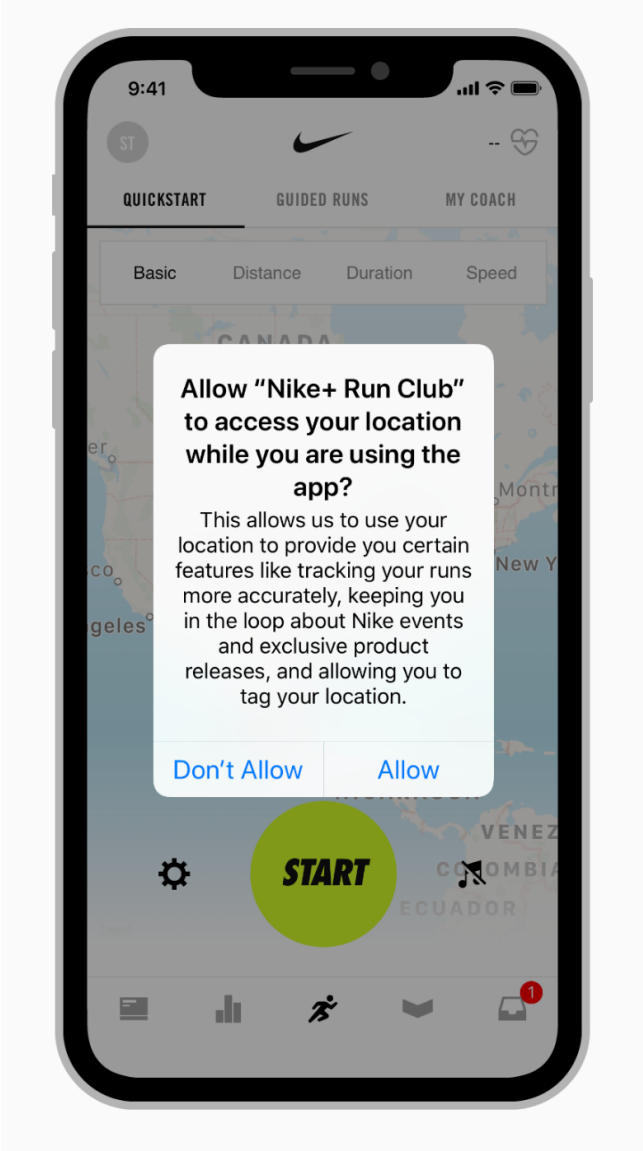
*Příloha 4 - Perceptron, formální neuron. Jednotlivé vstupy jsou x a y, ty násobíme vahou W1 a W2. Prahová hodnota pro sepnutí je 1. Mějme x = 2, y = 1, Wx = 2 a Wy = -2. Vážený součet vstupů je pak x*Wx + y*Wy = 2*2 - 1*2 = 2. Tento výsledek je větší než prahová hodnota, neuron tedy sepne. Obrázek i popis dle: KOUBSKÝ, Petr. Mysl je slepenec improvizací. 067.cz[online]. [cit. 2018-11-27]. Dostupné z: https://067.cz/archiv/58/mysl-je-slepenec-improvizaci.html*



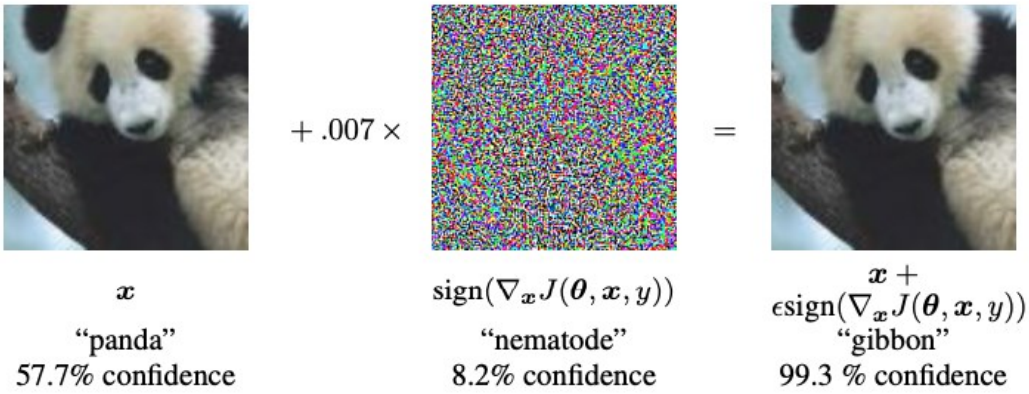
Příloha 5 - Zjednodušený model neurální sítě. Vlevo vstupní vrstva, následuje jedna skrytá vrstva a model končí vpravo generováním výsledku skrze výstupní vrstvu. Nahoře je naznačeno, jakým směrem model rozhoduje, dole pak směr nejrozšířenějšího typu učení (backpropagation). Zdroj: BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society [online]. 2016, 3(1) [cit. 2018-11-24]. DOI: 10.1177/2053951715622512. ISSN 2053-9517. Dostupné z: http://journals.sagepub.com/doi/10.1177/2053951715622512



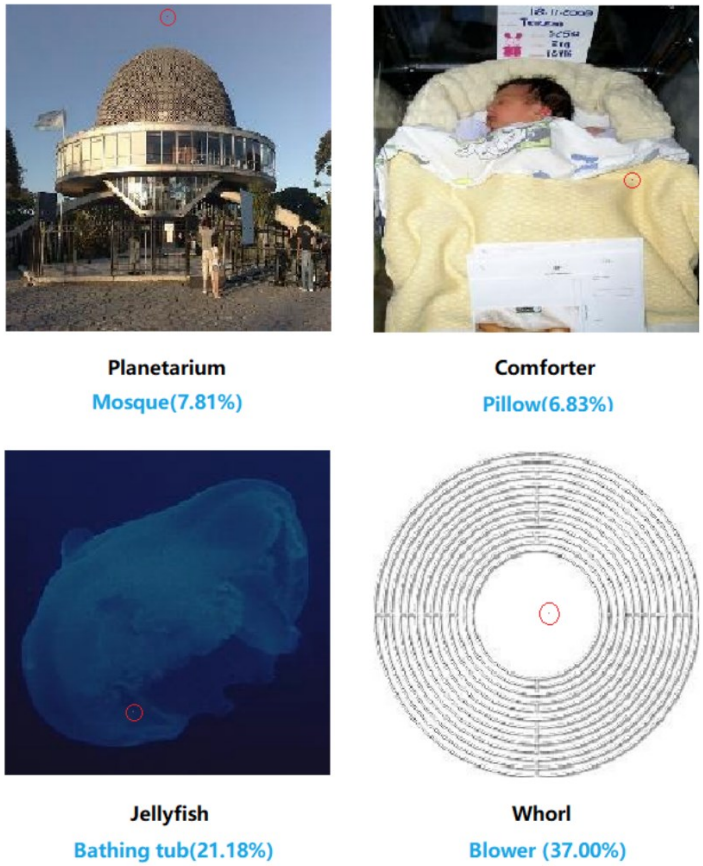
Příloha 6 - Vizualizace skutečné neurální sítě; v tomto případě sloužící k detekci zemětřesení. Zdroj: GIBSON, Lydialyle. A Rosetta Stone for Earthquakes. In: Harvard Magazine [online]. 2017 [cit. 2018-11-19]. Dostupné z: https://harvardmagazine.com/2017/11/earthquakes-around-the-world



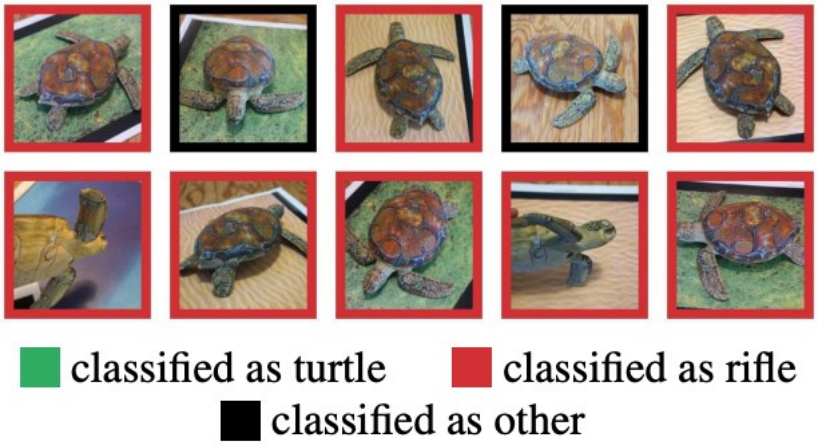
Příloha 7 - Příklad vhodného přístupu k informování a žádání o souhlas uživatelů mobilních aplikací, který ilustruje postup just-in-time. Data z mobilních aplikací jsou často jedním ze zdrojů pro následnou analýzu big data. Zdroj: APPLE. Human Interface Guidelines: Requesting Permission [online]. [cit. 2018-11-25]. Dostupné z: https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/



Příloha 8 - Ukázka útoku na neurální síť rozpoznávající obrázky. Zde síť na základě přidaného šumu chybně klasifikuje pandu jako gibbona. Dle: GOODFELLOW, Ian, Jonathon SHLENS a Christian SZEGEDY. Explaining and harnessing adversarial examples. ArXiv preprint [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1412.6572.pdf



Příloha 9 - Ukázka útoku na neurální síť rozpoznávající obrázky. Zde síť na základě změny jediného pixelu (na obrázcích změna označena červeným kroužkem) chybně klasifikuje původně správně rozpoznané obrázky. Původní výsledek znázorněn černou barvou, nový – chybný – barvou modrou. Dle: SU, Jiawei, Danilo Vasconcellos VARGAS a Kouichi SAKURAI. One Pixel Attack for Fooling Deep Neural Networks. ArXiv [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1710.08864.pdf



Příloha 10 - Příklad útoku na neurální síť rozpoznávající obrázky. Zde síť rozpoznává reálný objekt (želvu vytištěnou pomocí běžně dostupné 3D tiskárny), který je záměrně upraven tak, aby jej systém chybně rozpoznal. Dle: ATHALYE, Anish, Logan ENGSTROM, Andrew ILYAS a Kevin KWOK. Synthesizing Robust Adversarial Examples. ArXiv preprint [online]. [cit. 2019-02-26]. Dostupné z: https://arxiv.org/pdf/1707.07397.pdf

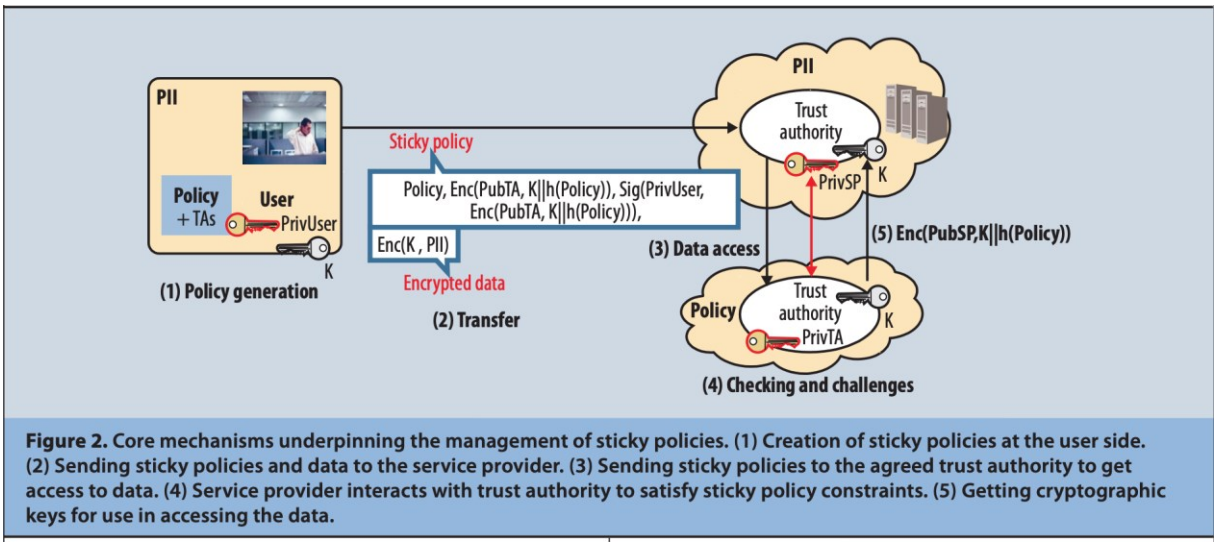
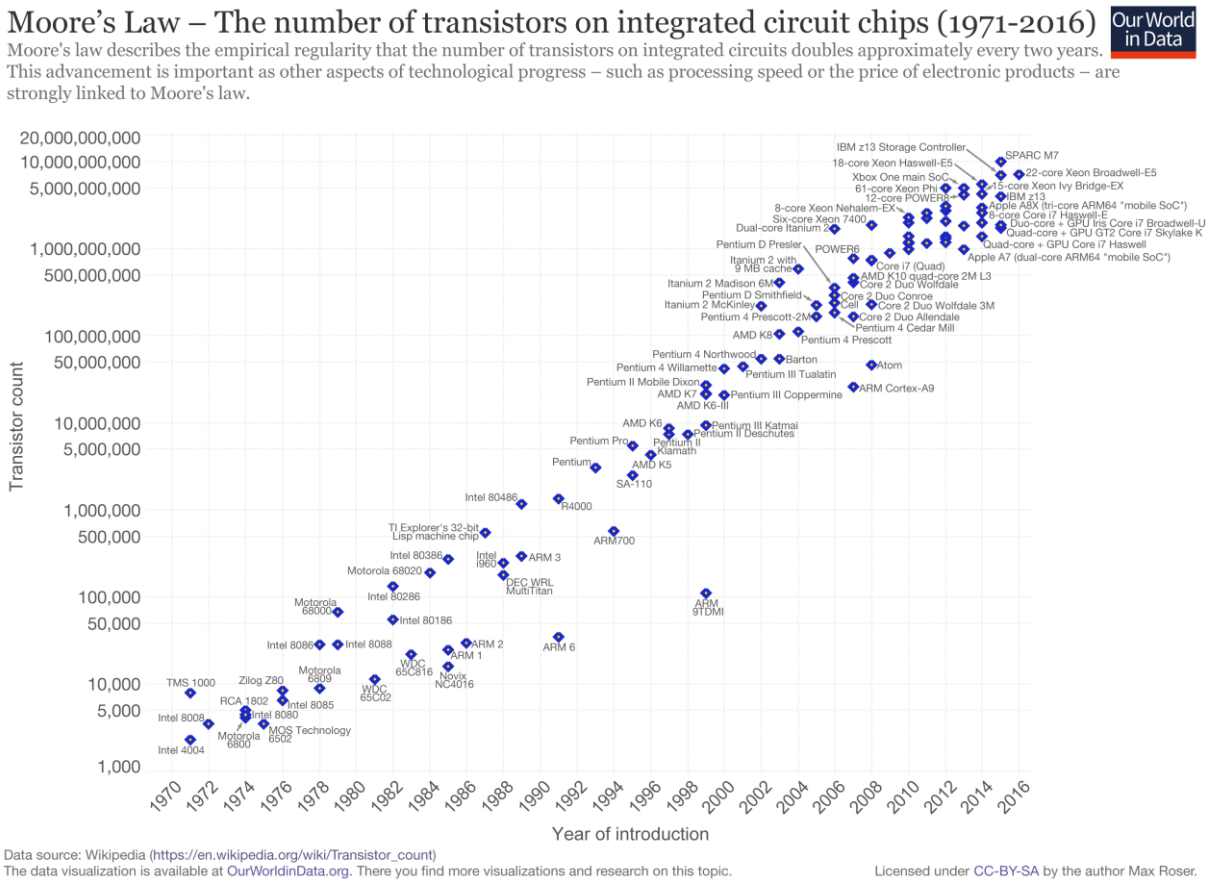
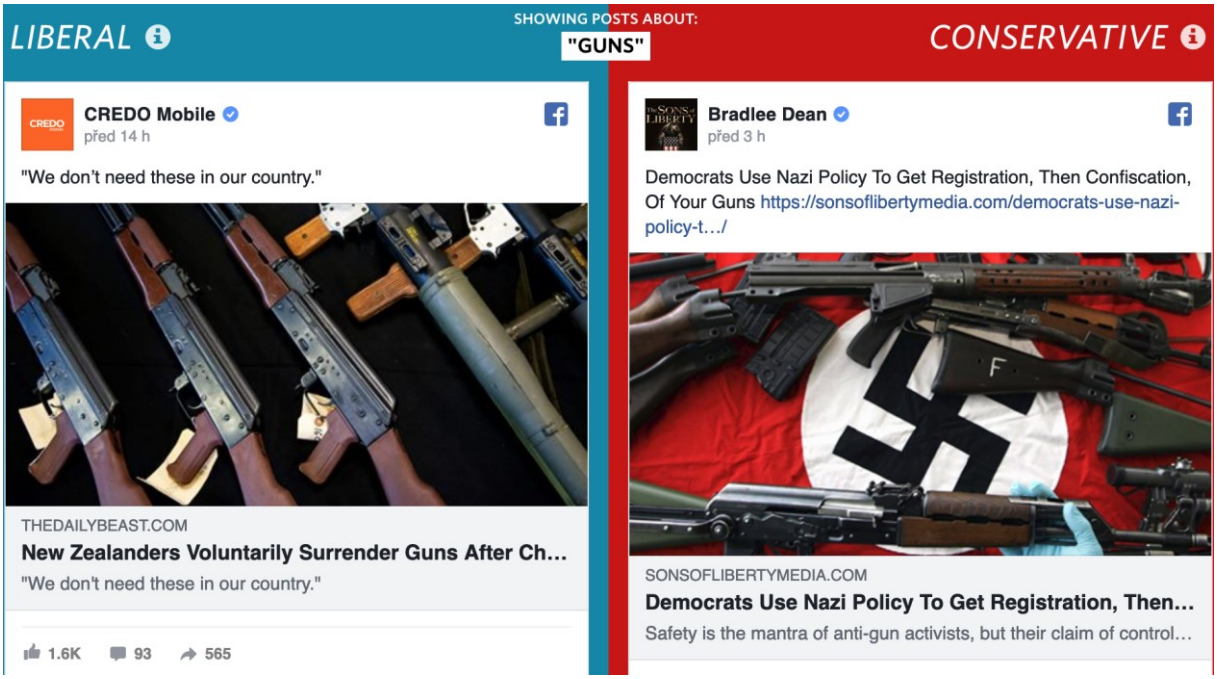


Figure 2. Core mechanisms underpinning the management of sticky policies. (1) Creation of sticky policies at the user side. (2) Sending sticky policies and data to the service provider. (3) Sending sticky policies to the agreed trust authority to get access to data. (4) Service provider interacts with trust authority to satisfy sticky policy constraints. (5) Getting cryptographic keys for use in accessing the data.

*Příloha 11 - Schématické znázornění fungování tzv. sticky policies spolu s vysvětlením jednotlivých kroků. Zdroj: PEARSON, Siani a Marco CASASSA-MONT. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer [online]. 2011, **44**(9), 60-68 [cit. 2018-11-26]. DOI: 10.1109/MC.2011.225. ISSN 0018-9162. Dostupné z: http://ieeexplore.ieee.org/document/5959137/*



Příloha 12 - Moorovo pravidlo. Zdroj: ROSER, Max a Hannah RITCHIE. Technological Progress. In: Our World in Data [online]. [cit. 2018-11-17]. Dostupné z: https://ourworldindata.org/technological-progress



Příloha 13 - Ukázka z projektu Blue Feed, Red Feed který ilustruje možnosti tvorby názorových bublin ze strany sociálních sítí. Má algoritmus třídící tzv. feed „právní" nebo „obdobné účinky"? Zdroj: http://graphics.wsj.com/blue-feed-red-feed/#/guns

Příloha 14 - Příklad genderové stereotypizace odrážející povahu datového setu. Dle: BAROCAS, Solon, Arvind NARAYANAN a Moritz HARDT. Fairness and machine learning: Limitations and Opportunities [online]. fairmlbook.org, 2018 [cit. 2019-03-21]. Dostupné z: https://fairmlbook.org/

Vybrané problémy technologické realizace evropské ochrany osobních údajů

Abstrakt

Tato diplomová práce se věnuje právní úpravě vybraných aspektů ochrany osobních údajů na evropské úrovni. Spolu s technologickým rozvojem nabírá tato oblast práva na důležitosti, s tím že využití osobních údajů může být jednak zdrojem inovací a ekonomického pokroku, jednak také může mít značný negativní efekt na práva jednotlivců. Diplomová práce analyzuje využití *big data* a automatizovaného individuálního rozhodování, s tím že oba tyto fenomény jsou nahlíženy skrze úpravu obsaženou v Obecném nařízení (GDPR). Cílem práce je pro tyto vybrané technologické fenomény zhodnotit funkčnost a perspektivy evropské právní úpravy.

Diplomová práce je, vyjma úvodu a závěru, členěna do tří kapitol. V první části je stručně představen koncept práva na ochranu osobních údajů a základní právní rámec evropské úpravy. Na tuto úvodní kapitolu navazuje kapitola týkající se *big data*, ve které je, po nutném technickém úvodu, rozebírán soulad současných postupů správců s jednotlivými zásadami ochrany osobních údajů. Zvláštní pozornost je také věnována úskalím anonymizace. Na konci této kapitoly je učiněn dílčí závěr, že všechny relevantní zásady je nutno aplikovat i na případy využití *big data*, a to přestože způsob dodržení těchto zásad nemusí být vždy zřejmý a snadný.

Navazující kapitola se týká příbuzného tématu, a to automatizovaného individuálního rozhodování. Po technickém úvodu, který představuje různé možnosti algoritmického rozhodování, je pozornost věnována souladu se zásadami přesnosti a transparentnosti. S druhou zmíněnou zásadou úzce souvisí otázka existence a povahy práva na vysvětlení. Ohledně tohoto práva byl učiněn závěr, že v současné právní úpravě zřejmě není obsaženo, ovšem jeho zavedení by bylo pozitivním krokem pro práva subjektů údajů. Z tohoto důvodu bylo *de lege ferenda* doporučeno zakotvit zmíněné právo mezi právně závazné články GDPR, oproti současnému zařazení mezi recitály. S odkazem na technické obtíže spojené s vysvětlením automatizovaného rozhodnutí (black box) bylo dále doporučeno kombinovat srovnávací vysvětlení spolu s obecným vysvětlením fungování modelu.

V závěrečné kapitole byl zhodnocen celkový přínos nové právní regulace, kdy bylo konstatováno, že GDPR je správným a nutným krokem vpřed, s tím že základní principy se jeví být jako skutečně odolné (technologickým) změnám (*futureproof),* jak ostatně bylo zamýšleno.

Klíčová slova:

ochrana osobních údajů, GDPR, Big Data, automatizované individuální rozhodování

Selected issues in technological realization of European data protection

Abstract

This thesis focuses on the legal regulation of selected aspects of the personal data protection at the European level. Fuelled by the technological progress, this area of legal regulation is becoming increasingly important, as the usage of personal data can be source of both innovation and economic progress, but it also has the potential to negatively impact individuals` rights ("chilling effect"). The thesis analyses the usage of *big data* and automated individual decision making; both phenomena are assessed through principles contained in GDPR. The aim of the thesis is to, as far as these two phenomena are concerned, evaluate functionality and perspectives of the European regulation.

The thesis is, apart from the introduction and the conclusion, divided into three chapters. The first part briefly introduces the concept of the right to the protection of personal data and the fundamental legal framework of the European regulation. This chapter is followed by a chapter focused on the big data, in which, after a necessary technical introduction is made, current practices of data controllers are contrasted with corresponding principles of data protection regulation. Particular attention is also paid to the pitfalls of anonymization. At the end of this chapter, it is concluded that all relevant principles of data protection should be applied when *big data* are used, even though it may not be obvious or easy to achieve compliance.

The following chapter then focuses on a related topic of automated individual decision making. After the technical introduction of different methods of algorithmic decision making is made, an analysis of compliance with the principles of accuracy and transparency follows. The latter mentioned principle relates closely to the question of the existence and nature of the right to explanation. Concerning this right, it was concluded that it is not incorporated in the current legislation, but its implementation would be a positive step forwards for the rights of data subjects. For this reason, it was, *de lege ferenda,* recommended to move the said right between legally binding GDPR articles, as it is now incorporated only in the form of legally not binding recital. Referring to the technical difficulties associated with explaining an automated

decision (black box), it was further recommended to combine a contrafactual explanation with a general explanation of the model's operation.

In the final chapter, the overall contribution of the new legal regulation was assessed, and it was concluded that GDPR is the right and necessary step forward and that basic principles contained in said regulation appear to be truly futureproof, as was intended.

Keywords:

data protection, GDPR, Big Data, automated individual decision-making