Jakub Míšek

MODERNÍ REGULATORNÍ METODY OCHRANY OSOBNÍCH ÚDAJŮ

MASARYKOVA UNIVERZITA

ACTA UNIVERSITATIS BRUNENSIS IURIDICA
EDITIO SCIENTIA

MUNI PRESS

MUNI LAW

MODERNÍ REGULATORNÍ METODY OCHRANY OSOBNÍCH ÚDAJŮ

Jakub Míšek

Masarykova univerzita
Brno 2020

Vzor citace
MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020, 279 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia, 694. ISBN 978-80-210-9736-0 (brož.), 978-80-210-9737-7 (online)

CIP - Katalogizace v knize

Míšek, Jakub
Moderní regulatorní metody ochrany osobních údajů / Jakub Míšek – 1. vydání. -- Brno: Masarykova univerzita, 2020. 279 stran. – Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia, sv. č. 694.
ISBN 978-80-210-9736-0 (brož.), 978-80-210-9737-7 (online)

342.721* 347.77/.78:004* 342.7* (048.8)*
- ochrana osobních údajů
- právo informačních technologií
- lidská práva
- monografie

342 – Ústavní právo. Správní právo [16]

Tato publikace vznikla na Masarykově univerzitě v rámci projektu Právo a technologie VIII č. MUNI/A/0989/2019 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2020.

Právní stav byl zohledněn ke dni 30. 6. 2020.

Recenzenti:
doc. JUDr. Pavel Mates, CSc.
JUDr. Tomáš Rychlý, Ph.D.

ISBN 978-80-210-9736-0
ISBN 978-80-210-9737-7 (online ; pdf)

Tato kniha, která je založena na výsledcích mého disertačního výzkumu, by nevznikla nebýt pomoci a působení celé řady lidí. Mé díky tak patří předně Radimu Polčákovi, za mnoho inspirujících diskuzí, validaci nápadů a za to, že ve mně podnítil lásku k teorii práva a snahu nahlížet na věci v jejich širším kontextu. Dále děkuji kolegům a přátelům z Ústavu práva a technologií. Předně mé díky patří Jakubu Haraštovi, který mi nabídl pomocnou ruku, když byla nejvíce potřeba. Děkuji Matějovi Myškovi za inspiraci a nasměrování, Pavlovi Loutockému za podporu na společné cestě studiem a Františku Kaslovi za jeho pronikavý pragmatismus, trefné postřehy a diskuze nad tématem ochrany soukromí a osobních údajů.

Děkuji Josefu Prokešovi, díky kterému jsem do světa ochrany osobních údajů mohl vstoupit, a který byl mým prvním průvodcem v něm.

Markétě Kleinové děkuji za korektury a Ivě Vávrové za jazykovou podporu.

Peregrinovi a Smělmírovi patří dík za vysoce funkční felinoterapii.

Anně pak tuto knihu věnuji a děkuji za nekonečnou podporu, trpělivost, shovívavost a výdrž.

OBSAH

Seznam zkratek ... 11

1 Úvod ... 13
1.1 Výzkumné otázky, cíle a metoda práce ... 16
1.2 Vymezení záběru monografie ... 22
1.3 Struktura publikace ... 24

2 Premisy ... 27
2.1 Soukromí, osobní údaje a informační sebeurčení ... 29
2.1.1 Pojem soukromí ... 29
2.1.2 Pojem osobní údaje ... 37
2.1.3 Právo na informační sebeurčení ... 39
2.1.4 Přehled pozitivně právní úpravy ochrany soukromí a osobních údajů ... 43
2.1.5 Právo na ochranu osobních údajů jako základní právo a jeho účel ... 47
2.2 Ochrana osobních údajů jako rámec pro probíhající zpracování ... 58
2.3 Práva subjektu údajů jako pojistka před zneužitím osobních údajů ... 71
2.3.1 Role práv subjektů v systému ochrany osobních údajů ... 71
2.3.2 Problémy aplikace práv subjektu údajů ... 83
2.4 Ochrana osobních údajů jako nástroj prevence ... 91
2.5 Shrnutí kapitoly ... 100

3 Minulost ochrany osobních údajů: Směrnice 95/46/ES a její problémy ... 103
3.1 IP adresy v kybernetické bezpečnosti ... 108
3.2 Rozhodnutí *Google Spain* a jeho následky ... 114
3.3 Hypertextové odkazy jako zpracování osobních údajů ... 119
3.4 Anonymizace a otevřená data ... 128
3.5 Shrnutí kapitoly ... 131

4 Zúžení interpretace definičních pojmů a nevymáhání povinností 133
4.1 Objektivní a subjektivní přístup k osobním údajům 133
4.2 Nevymáhání práva 140
4.3 Shrnutí kapitoly 144

5 Zásada odpovědnosti správce a regulace založená na riziku 147
5.1 Performativní regulace 148
5.2 Zásada odpovědnosti správce údajů 159
5.3 Jádro principu odpovědnosti: Rizikovost zpracování 169
5.4 Praktické dopady hodnocení rizik v Obecném nařízení 178
5.4.1 Oprávněný zájem správce 182
5.4.2 Vedení záznamů o zpracování 185
5.4.3 Povinnosti vyplývající z vyššího rizika 187
5.4.4 Práva subjektů údajů 191
5.5 Temporální aspekty 193
5.5.1 Odolnost právní úpravy osobních údajů vůči technologickým změnám 194
5.5.2 Změna hodnoty osobních údajů v čase a zapomínání 197
5.6 Shrnutí kapitoly 202

6 Moderní regulatorní metody ochrany osobních údajů: Syntéza a diskuze 205
6.1 Aplikace zásady accountability správce na modelové situace 208
6.2 Problémy performativní regulace v kontextu Obecného nařízení 212
6.2.1 Problém vymáhání povinností a sankce 213
6.2.2 Vysoké nároky na správce údajů 218

7 Závěr 221

Summary – Modern Regulatory Methods of Personal Data Protection 229

Literatura a další použité zdroje 235
Odborné monografie a články 235
Kapitoly knih 259
Další online zdroje 264
Doporučení, stanoviska a další dokumenty 265
Citované předpisy 270
Mezinárodní smlouvy 270
Evropské předpisy 270
České předpisy 271
Zahraniční předpisy 272
Citovaná rozhodnutí 272
Evropský soud pro lidská práva 272
Evropský soudní dvůr a Soudní dvůr Evropské unie 274
Ústavní soud 276
Nejvyšší soud 278
Nejvyšší správní soud 278
Zahraniční soudy 279
Rozhodnutí ÚOOÚ 279

SEZNAM ZKRATEK

ESLP	Evropský soud pro lidská práva
DPIA	Posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 Obecného nařízení o ochraně osobních údajů
SDEU	Soudní dvůr Evropské unie
Obecné nařízení	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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)
Sbor	Evropský sbor pro ochranu osobních údajů
SME	Střední a malé podniky s méně než 250 zaměstnanci
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
Úmluva 108	Sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat
WP 29	Pracovní skupina zřízená dle článku 29 směrnice 95/46/ES

1 ÚVOD*

Ochrana osobních údajů představuje i vzhledem k stále probíhající reformě právní úpravy[1] velice aktuální a silně diskutované téma zejména v kontextu střetu základních práv[2] s technologickou realitou. Dynamický vývoj informačních a komunikačních technologií posledních let znamenal pro ochranu osobních údajů zásadní a nevratnou paradigmatickou změnu. Došlo totiž k výraznému nárůstu možností, jakými způsoby a v jakém rozsahu je možné osobní údaje zpracovávat a zároveň s tím i k celkovému navýšení množství zpracování, která jsou prováděna. Ačkoli je právo na ochranu osobních údajů součástí katalogu základních práv teprve relativně krátce,[3] principy, na kterých dodnes stojí, byly v mezinárodně relevantních dokumentech formulovány na samém počátku osmdesátých

* Tato monografie vychází z textu disertační práce nazvané „Osobní údaje v čase a prostoru: Role performativní regulace v ochraně osobních údajů", kterou jsem obhájil na Právnické fakultě Masarykovy univerzity v roce 2020.

1 Ačkoli účinnost nového Obecného nařízení [Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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)] nastala již více než před rokem a letošní jaro jsme se konečně dočkali i reakce českého zákonodárce v podobě zákonů č. 110/2019 Sb., o zpracování osobních údajů a na něj navazujícího změnového zákona č. 111/2019 Sb., proces stále není u konce vzhledem k probíhajícímu legislativnímu procesu tzv. ePrivacy nařízení, které v budoucnu nahradí současnou ePrivacy směrnici č. 2002/58/ES.

2 Jde zejména o právo na soukromí a právo na ochranu osobních údajů zakotvené v čl. 8 Evropské Úmluvy o ochraně lidských práv a základních svobod (viz Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb. m. s., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících), v čl. 7 a 8 Listiny základních práv EU (Dokument č. 2010/C 83/02) a v čl. 7, 10, 12 a 13 Listiny základních práv a svobod (Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů).

3 Právo na ochranu osobních údajů není přítomné v žádné z velkých lidskoprávních mezinárodních smluv a dokumentů, jako je Všeobecná deklarace lidských práv roku 1948, Mezinárodní pakt o občanských a politických právech z roku 1966 (Vyhláška MZV č. 120/1976 Sb. ze dne 10. 5. 1976 o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech), nebo Úmluva o ochraně lidských práv a základních svobod (Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících). Je zakotveno v článku 8 Listiny základních práv a svobod Evropské unie (dokument č. 2010/C 83/02), která nabyla účinnosti společně s Lisabonskou smlouvou. Text článku 8 je totožný s textem uvedeným v Chartě základních práv a svobod Evropské unie (dokument č. 2000/C 364/1). Na území České republiky bylo právo na ochranu osobních údajů uvedeno v Listině základních práv a svobod (ústavní zákon č. 23/1991 Sb.).

let[4] a cíl, k němuž uvedená právní úprava míří, tedy ochrana soukromí jedince, je aktivně zkoumán více než jedno a čtvrt století.[5] Motivaci pro sepsání svého dnes již ikonického textu našli Warren s Brandeisem právě v nových technologických a obchodních postupech, které umožnily do té doby nepoznaný zásah do soukromí člověka.[6] Technologický vývoj byl pak rovněž jednou z hlavních motivací pro vznik evropského nařízení č. 2016/679,[7] obecného nařízení o ochraně osobních údajů, známějšího možná pod akronymem GDPR (z anglického názvu předpisu *„General Data Protection Regulation"*, dále jen Obecné nařízení[8]).[9] Přijetí a účinnost Obecného nařízení je logickým zdrojem současného živého zájmu a diskuzí věnovaných ochraně osobních údajů, a to jak mezi odborníky mnoha profesí od právníků po informatiky a bezpečnostní experty,[10] tak i mezi

4 Srovnej Thirty years after, The OECD privacy guidelines. *OECD* [online]. 2011; dále též viz recitál 9 Obecného nařízení.

5 Viz například WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5; Ke vzniku základního práva na ochranu osobních údajů více dále např. GONZÁLEZ-FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Cham; New York: Springer, 2014.

6 Technologií, vůči které měli profesoři Warren a Brandeis potřebu se vymezit, byla instantní fotografie s možností jejího využití v bulvárních mediích, jejichž koncept v té době rovněž vznikal. Viz WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5, s. 195.

7 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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).

8 Pro tuto publikaci jsem se rozhodl používat zkrácený název „Obecné nařízení" místo možná používanějšího „GDPR". Hlavním důvodem je osobní preference užití českých názvů v případech, kdy je to možné a vzhledem k povaze pojmu i vhodné.

9 Viz bod 6 odůvodnění Obecného nařízení. Uvedené dále dokládají například slova tehdejší euro komisařky Viviane Reding: *„17 years ago less than 1% of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds… The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information."* Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. *Evropská komise* [online]. 2012, Press Release Database.

10 Jako příklad z vysokoškolského prostředí může posloužit řešení projektu CESNET *„Zpracování a pilotní ověření metodiky implementace GDPR v IT prostředí VVŠ"* (kód projektu 599/2017), ve kterém byla zapojena řada odborníků uvedených profesí.

laiky, jichž se nové normy nutně přímo dotýkají, ať už v pozici subjektů údajů nebo správců.[11]

Obecné nařízení se nachází v poměrně nesnadné pozici, kdy je obecnou normou zajišťující a upravující ochranu osobních údajů. Předně dopadá na zpracování osobních údajů, která provádí velké technologické společnosti, jako jsou Facebook a Google. Ty založily svoji obchodní strategii na analýze a monetizaci osobních údajů uživatelů jejich služeb.[12] Na rizika zpracování tzv. „big data" s osobními údaji uživatelů, která jsou předmětem „obchodu" („výměny" soukromí a osobních údajů za možnost užívat nové služby „zdarma" a nechat si nabízet přesně zacílené zboží) upozornila Shoshana Zuboff ve svém vlivném článku, ve kterém nazvala celý tento mechanismus *„Surveillance capitalism"*.[13] Obecné nařízení má být nástrojem, který by měl rizika, které Zuboff trefně identifikovala, alespoň zmírnit.[14] Vedle toho však to stejné Obecné nařízení dopadá na zpracování osobních údajů středními a malými podniky (dále jen „SME"), a dokonce i na jednotlivé fyzické osoby, pokud se dostanou do pozice správce osobních údajů. Stejný, ze své povahy veřejnoprávní, předpis tak musí být aplikovatelný na různé typy povinných subjektů s různými možnostmi zpracování osobních údajů a různou intenzitou jejich využívání ve své činnosti.

Obecné nařízení bylo přijato v dubnu 2016 po více než čtyřech letech legislativních prací. Když pak v květnu 2018 nabylo účinnosti, nahradilo

11 Stačí si vzpomenout na množství popularizačních a často bohužel velice nepřesných nebo strach nahánějících článků, které se vyrojily u příležitosti nabytí účinnosti Obecného nařízení. Některé z nich musel dokonce Úřad pro ochranu osobních údajů uvádět na pravou míru prostřednictvím svých webových stránek (viz např. Nepravdy o wi-fi v souvislosti s GDPR. *Úřad pro ochranu osobních údajů* [online]. 2018; Existují samozřejmě naopak i dobré popularizační zdroje, jako například KAMÍNEK, Petr. Návod jak na GDPR. *Weby Google* [online]. 2018.

12 Je to právě možnost efektivního vymáhání práva ochrany osobních údajů vůči těmto a dalším podobným technologickým gigantům, co tvořilo jednu z hlavních motivací přijetí Obecného nařízení včetně na první pohled velice tvrdé maximální výše sankcí v podobě 20 000 000 €, nebo 4 % celoročního obratu společnosti, podle toho, která hodnota je vyšší (čl. 83 odst. 6 Obecného nařízení).

13 ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology,* 2015, roč. 30, č. 1.

14 Hodnocení, zda se tak opravdu děje, leží mimo záběr této publikace.

směrnici 95/46/ES.[15] Byť přineslo řadu dílčích novinek, ve svých principech a základních stavebních blocích přímo navazuje na své přímé a ideové předchůdce v podobě směrnice 95/46/ES, Úmluvy Rady Evropy č. 108[16] a pravidel Organizace pro hospodářskou spolupráci a rozvoj, o ochraně soukromí a přeshraničních tocích osobních údajů.[17] Jde zejména o základní zásady, jako je princip zákonnosti, odpovědnosti a transparentnosti, princip omezení účelem zpracování a princip minimalizace údajů.[18] Judikatura i doktrinální práce, které se vztahovaly k předchozí právní úpravě, jsou tak po patřičné (a zpravidla minimální) korekci stále použitelné. Obecné nařízení je navíc podobně jako směrnice 95/46/ES vystavěno jako technologicky neutrální předpis v tom smyslu, že předem nijak neomezuje a neurčuje využití konkrétních technologií, a proto by mělo obstát i ve zkoušce časem vzhledem k příchodu nových technologií a nových způsobů zpracování osobních údajů.[19] Vzhledem k výše uvedenému je možné říct, že pokud nenastane nějaký zcela nepředvídatelný vývoj událostí, minimálně pro příští dvě desetiletí bude Obecné nařízení regulovat právní úpravu ochrany osobních údajů a v tomto smyslu je nezbytné s celým systémem ochrany osobních údajů pracovat.

1.1 Výzkumné otázky, cíle a metoda práce

Hlavním cílem této publikace je prozkoumat, jestli a jakým způsobem připouští ustanovení Obecného nařízení interpretaci, která umožňuje rozlišit mezi povinnostmi správců podle povahy probíhajícího zpracování a schopnosti plnit požadavky předepsané nařízením. Hlavní obecnou výzkumnou otázku je tak možné zformulovat následovně: *Obsahuje Obecné nařízení mechanismy, které zajistí škálovatelnost a granularitu povinností správců osobních údajů lepším*

15 Viz směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

16 Viz sdělení ministerstva zahraničních věcí č. 115/2001 Sb., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

17 Viz OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online].

18 Viz odst. 7–10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, čl. 5 Úmluvy 108 a čl. 6 směrnice 95/46/ES a čl. 5 Obecného nařízení.

19 Viz HILDEBRANDT, Mireille a Laura TIELEMANS. Data protection by design and technology neutral law. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5.

způsobem než směrnice 95/46/ES tak, aby nedocházelo k nepřiměřenému zatížení správců údajů a zároveň byla zachována dostatečná ochrana práv subjektů údajů?

Škálovatelností a granularitou povinností je myšlena taková konkrétní interpretace právní úpravy, která umožní, aby vzhledem k charakteru konkrétního probíhajícího zpracování osobních údajů a povaze konkrétního správce byly povinnosti správce adekvátní v tom smyslu, že jej nebudou nepřiměřeně zatěžovat a zároveň bude nadále zachována nezbytná úroveň ochrany práv subjektů údajů. Důležitou součástí granularity a škálovatelnosti povinností je umožnění správci údajů pružně reagovat na změny, které se v průběhu zpracování údajů stanou. Granularitou povinností je myšlena aplikace specifických povinností správce údajů dle toho, zda jsou v konkrétním případě vzhledem k povaze zpracování opravdu nezbytné. Škálovatelností je pak myšleno nastavení způsobu plnění konkrétní povinnosti, včetně míry investované snahy a prostředků, dle toho, jak je to v konkrétním případě zpracování vzhledem k jeho povaze a okolnostem přiměřené.

K zodpovězení hlavní výzkumné otázky je nejprve nutné upřesnit ji do podoby dílčích výzkumných otázek, u kterých je pak nezbytné dále specifikovat, jakým způsobem na ně budu hledat odpověď. Tato publikace si tak postupně klade za cíl odpovědět na násl. dílčí otázky: i) jaké byly z hlediska granularity a škálovatelnosti povinností hlavní nedostatky směrnice 95/46/ES? ii) jaká jsou možná řešení těchto nedostatků? iii) obsahuje Obecné nařízení takovou právní úpravu, která umožňuje překonat problémy identifikované v případě směrnice 95/46/ES, a pokud ano, jak funguje jejich regulatorní metoda? iv) Jakou roli ve výše uvedeném hraje aspekt plynoucího času?

Konkrétní důvody volby výběru těchto otázek jsou rozebrány v následujících odstavcích.

První dílčí výzkumná otázka směřuje ke zhodnocení toho, jak bývalá právní úprava dokázala reagovat na výzvy v podobě nových druhů zpracování osobních údajů, tedy zda nabízela dostatečnou škálovatelnost a granularitu povinností správce údajů. Při hodnocení této otázky vychází publikace jak z textu hodnocené směrnice, tak její české národní implementace v podobě zákona č. 101/2000 Sb. Hodnocení je provedeno prostřednictvím čtyř případových studií. Pro případové studie byly vybrány situace zpracování osobních

údajů se zapojením nových technologií, které argumentačně testovaly hranici výkladu pravidel obsažených ve směrnici 95/46/ES. Konkrétně byla provedena analýza zpracování IP adres v kontextu kybernetické bezpečnosti, zpracování osobních údajů internetovými vyhledávači, užití hypertextových odkazů v kontextu zpracování osobních údajů a zpracování anonymizovaných osobních údajů v kontextu poskytování informací veřejného sektoru a otevřených dat. Objektem zkoumání těchto případových studií je míra škálovatelnosti a granularity povinností správce.[20] Byť vybrané případy sdílejí charakteristiku zapojení nových technologií do procesu zpracování, nedochází k jejich přímému porovnání a jedná se tak o čtyři samostatné jednopřípadové studie. Tyto případy zpracování byly vybrány na základě toho, že v jejich aplikaci šíře definice základních aplikačních pojmů (vymezení pojmu osobní údaj nebo zpracování osobních údajů) přesahuje nebo přesahovala jejich běžný rozsah.[21]

Druhá dílčí otázka směřuje k identifikaci možných řešení, které by mohly napomoci překonání nedostatků aplikace právní úpravy ochrany osobních údajů v kontextu nízké škálovatelnosti a granularity povinností správce. Obecně je možné identifikovat tři základní varianty, které mohou být

20 Viz KOSAŘ, David a Jan PETROV. Jak vybrat „případy" do případové studie a pracovat s nimi v právu: poznatky z výzkumu na pomezí práva a politologie. *Jurisprudence*, 2016, roč. 25, č. 6, s. 22.

21 Jde tedy o tzv. deviantní případy, viz Ibid., s. 24. Uvedenou „běžnou šíři rozsahu interpretace" jsem určil subjektivně na základě probíhajících debat, ze kterých vyplývala výjimečnost daného případu. Příkladem mohou být texty odmítající vymezení IP adresy jako osobních údajů (viz LUNDEVALL-UNGER, Patrick a Tommy TRANVIK. IP Addresses – Just a Number? *International Journal of Law and Information Technology* [online]. 2011, roč. 19, č. 1; TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken a Anna-Maria TALIHÄRM (eds.). *International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010) a vzrušené diskuzní příspěvky, které následovaly po rozhodnutí *Google Spain* (např. ALSENOY, Brendan Van et al. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?* [online]. Rochester, NY: Social Science Research Network, 2013 [cit. 30. 6. 2020]; NONNEMANN, František. Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google. *Právní rozhledy*, 2014, roč. 22, č. 13–14). Případ, že by hypertextový odkaz mohl být zpracováním osobních údajů, se zdá na první pohled nepravděpodobným a nepanuje shoda, že to tak opravdu je (v tomto směru děkuji Zsoltu Baloghovi a Andreasi Wiebemu za plodnou diskuzi na 4th Göttinger Research Forum on Law and ICT/IP 2015 a Radimu Polčákovi za debatu při příležitosti konání setkání iSysel v březnu 2019). Konečně v případě anonymizace se jedná o problém daný vývojem technologie, která neustále posunuje hranici toho, co je možné za anonymizované považovat (viz OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 2009, roč. 57, č. 6).

v tomto směru využity. První je interpretační zúžení definičních pojmů, které vymezují aplikovatelnost právní úpravy ochrany osobních údajů. Díky němu by došlo k vyloučení aplikace právní úpravy v případech, ve kterých by byla z hlediska splnitelnosti povinností ze strany správce nepřiměřená.[22] Druhou variantou je systematické rozhodnutí kompetentních orgánů dozoru takové hraniční případy nevymáhat.[23] Konečně třetí variantou je vnitřní systémová škálovatelnost a granularita povinností.

První část třetí dílčí otázky směřuje k identifikaci regulatorního přístupu, který ze své podstaty nabízí povinným subjektům dostatečnou možnost zvolit si variantu splnění svých povinností, která odpovídá konkrétnímu případu. Cílem druhé části třetí dílčí otázky je ověřit, zda Obecné nařízení obsahuje takovou právní úpravu, která umožňuje překonat problémy identifikované v případě Směrnice 95/46/ES, a pokud ano, jaké jsou mechanismy jejího fungování.

Zpracování osobních údajů je proces probíhající v čase. Právní úprava ochrany osobních údajů nesmí být od dynamiky plynutí času odtržena, protože běh času při zpracování hraje významnou roli. To platí jak na úrovni konkrétního zpracování, jelikož význam zpracovávaných osobních údajů a konkrétní okolnosti daného zpracování se mohou v průběhu měnit,[24] tak na úrovni celého systému ochrany osobních údajů, neboť ten musí být schopný vyrovnat se technologickou změnou, kterou čas přináší.[25] Čtvrtá

22 Tuto variantu si můžeme představit jako „omezení na vstupu" do systému ochrany osobních údajů.

23 Tuto variantu si můžeme představit jako „omezení na výstupu" ze systému ochrany osobních údajů.

24 Srovnej např. KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law* [online]. Dordrecht: Springer Netherlands, 2015, Law, Governance and Technology Series, 20 [cit. 27. 10. 2016]; KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law* [online]. Dordrecht: Springer Netherlands, 2015, Law, Governance and Technology Series, 20 [cit. 27. 10. 2016].

25 Srovnej HERT, Paul de. The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents Editorial. *Utrecht Journal of International and European Law,* 2015, roč. 31, č. 80, s. 1; KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*, 2012, s. 14.

dílčí otázka proto směřuje k vyhodnocení, zda principy právní úpravy identifikované v průběhu třetí otázky obstojí v čase.

Cílem této publikace je zodpovědět výše položené otázky v prostředí regulatorní metody a norem Obecného nařízení a analyzovat v jejich světle práva a povinnosti správce a subjektu údajů.

Předkládaná publikace vychází ze čtyř předpokladů. Prvním z nich je, že právo na ochranu osobních údajů je samostatné základní právo, jehož cíle i metody regulace jsou odlišné od práva na ochranu soukromí, ačkoli se v určité části překrývají.[26] Druhým klíčovým východiskem je, že právo na ochranu osobních údajů má své kořeny v právu na informační sebeurčení, které je realizováno skrze jednotlivá dílčí práva náležející subjektům údajů, která tak hrají v celém systému úpravy klíčovou roli.[27] Krom toho však právní úprava ochrany osobních údajů má silnou nedistributivní část,[28] kdy reguluje

---

26 Srovnej GUTWIRTH, Serge. *Privacy and the information age*. Lanham, Md: Rowman & Littlefield Publishers, 2002, s. 30. Citováno dle FINN, Rachel L., David WRIGHT a Michael FRIEDWALD. Seven Types of Privacy. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 4; Dále též například CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site* [online]. 2016; GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5; GELLERT, Raphaël a Serge GUTWIRTH. Beyond Accountability, the Return to Privacy? In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 261–283; KOOPS, Bert-Jaap et al. A Typology of Privacy. *SSRN Scholarly Paper* [online]. ID 2754043. Rochester, NY: Social Science Research Network. 2016 [cit. 30. 6. 2020]; TZANOU, Maria. Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures. *Journal of Internet Law*. 2013, roč. 17, č. 3.

27 Základ pro právo na informační sebeurčení byl založen Německým spolkovým ústavním soudem v rozsudku ze dne 15. 12. 1983, sp. zn. BvR 209/83, BVerfGE 65. Dále k informačnímu sebeurčení viz ROUVROY, Antoinette a Yves POULLET. The Right to Informational Self-Determination and the Value of Self-Development. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009; LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3; POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, s. 327; POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 21; WAGNEROVÁ, Eliška. Čl. 10. In: WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012. Dostupné z: ASPI [Právní informační systém].

28 Viz POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, s. 341–345.

a chrání prostředí, v němž se subjekty údajů pohybují.[29] Třetím předpokladem je, že právní úprava ochrany osobních údajů neslouží výhradně k ochraně práv subjektů údajů, ale stejně tak má za cíl umožnit správcům osobních údajů s údaji nakládat. Cílem právní úpravy ochrany osobních údajů je tak v praxi umožnit korektní nakládání s osobními údaji tak, aby toto zpracování bylo pro subjekty údajů pokud možno co nejvíc bezpečné.[30] Čtvrtým předpokladem, ze kterého vychází tato kniha, je potom fakt, že systém ochrany osobních údajů je primárně preventivním nástrojem, jehož cílem je předcházet vzniku zásahu do práv fyzických osob nesprávným zpracováním jejich údajů.[31] Tento princip prevence se implicitně promítá do rozhodovací praxe Soudního dvora Evropské unie (dále „SDEU“). Ten s argumentem nezbytnosti zajištění ochrany práv subjektů údajů rozhoduje tak, že definice pojmů, které jsou podmínkou pro aplikaci právní úpravy, je třeba vykládat široce, a naopak veškeré výjimky maximálně úzce.[32]

---

29 Viz HOOD, Christopher, Henry ROTHSTEIN a Robert BALDWIN. *The government of risk: understanding risk regulation regimes*. Oxford; New York: Oxford University Press, 2001; GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law* [online]. 2015, roč. 5, č. 1.

30 Viz například BYGRAVE, Lee A. The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal,* 2001, roč. 24, č. 1, s. 282; HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: *Reinventing data protection*? Dordrecht: Springer, 2009, s. 3; ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 245.

31 Srovnej například CAVOUKIAN, Ann. Privacy by Design: Leadership, Methods, and Results. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 192; LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3.

32 Jako příklad je možné uvést rozhodnutí rozšiřující pojem osobní údaj (rozsudek Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer,* C-582/14, a rozsudek Soudního dvora Evropské unie ze dne 20. 12. 2017 ve věci *Nowak,* C-434/16), rozšiřující pojem zpracování osobních údajů (rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01), rozšiřující pojem správce osobních údajů (rozsudek Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein,* C-210/16; rozsudek Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan Todistajat,* C-25/17; a rozsudek Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci *Fashion ID*, C-40/17), nebo naopak rozsudek zužující výklad výjimky zpracování pro osobní potřebu (rozsudek Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13).

V této publikaci jsou využity klasické textově analytické metody normativní právní vědy,[33] potažmo právní hermeneutiky.[34] Kniha vychází z pragmatického přístupu, který se dle Polčáka jeví být pro technologické obory práva ideálním metodologickým východiskem, protože si všímá okamžitého užitku a umožňuje tak pružně reagovat na specifika daná aplikovanou technologií.[35] Pragmatický přístup byl zvolen jako metodologické východisko proto, že umožňuje interpretovat analyzované ustanovení v souladu s jeho účelem[36] a v kontextu reálného fungování použitých technologií.[37] Tato publikace nemá motivaci ani snahu nijak hlouběji čerpat z dalších vědních oborů, jako je sociologie, psychologie nebo ekonomie a aplikovat jejich metodologická východiska.

1.2 Vymezení záběru monografie

Tato publikace se zabývá obecnou právní úpravou ochrany osobních údajů z pohledu evropského a českého práva. Toto zaměření proto vymezuje základní záběr celé monografie. Z mezinárodněprávních dokumentů text pracuje zejména se základními lidskoprávními úmluvami a specifickými nástroji ochrany osobních údajů. Těžiště knihy leží na úrovni práva Evropské unie. V kontextu evropského práva se publikace v rámci primárního práva věnuje toliko ustanovením, která se zabývají ochranou osobních údajů (čl. 16 Smlouvy o fungování EU a čl. 8 Listiny základních práv EU). Účelem této publikace není však jejich hlubší analýza. Jejich využití je převážně argumentační. V kontextu sekundárního práva se publikace analyticky zaměřuje

33 Srovnej SMITS, Jan M. *The mind and method of the legal academic*. Cheltenham, UK: Edward Elgar, 2012, s. 58 a násl.; HOECKE, Mark Van. Legal Doctrine: Which Method(s) for What Kind of Discipline? In: HOECKE, Mark van (ed.). *Methodologies of legal research: which kind of method for what kind of discipline?* Oxford, Portland: Hart, 2011, s. 1–18, European Academy of Legal Theory monograph series.

34 Viz HLOUCH, Lukáš. *Teorie a realita právní interpretace*. Plzeň: Aleš Čeněk, 2011, s. 78; HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 289 a násl.

35 POLČÁK, Radim. *Internet a proměny práva. Téma*. Praha: Auditorium, 2012, s. 76–81; POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 5.

36 K významu účelu v právu viz klasická publikace Rudolfa von Jheringa *Zweck im Recht* (citováno dle anglického překladu JHERING, Rudolf von. *Law as a means to an end*. Přel. HUSIK, Isaac. Boston: The Boston book company, 1913).

37 Více k právnímu pragmatismu viz např. POSNER, Richard A. *Law, pragmatism, and democracy*. Cambridge, Mass: Harvard University Press, 2003, s. 57–96.

na Obecné nařízení. Zcela mimo její zájem leží směrnice č. 2002/58/ES,[38] směrnice č. 2016/680[39] a nařízení č. 2018/1725.[40] Případné zmínky o těchto předpisech jsou pouze ilustrační. Ustanovení zrušené směrnice 95/46/ES jsou analyzovány z hlediska komparace s ustanoveními Obecného nařízení. V kontextu českého práva publikace vychází zejména z obecných předpisů ochrany osobních údajů v podobě již zrušeného zákona č. 101/2000 Sb. a nového zákona č. 110/2019 Sb. Detailní analýza jejich ustanovení však není těžištěm tohoto textu, blíže je jim věnována pozornost převážně pro srovnání s úpravou evropskou. Obzvláště otázky harmonizace národní úpravy s Obecným nařízením v podobě zákona 110/2019 Sb. leží za hranicí této publikace.

V textu jsou argumentačně využity rozhodnutí ESLP, SDEU a vrcholných českých soudů.

Monografie vychází z českých i zahraničních doktrinálních textů, a to včetně prací z oblasti angloamerického práva, které přes rozdílnost právních systémů slouží jako dobrý zdroj inspirace a nikoli jako objekt komparativní analýzy. V oblasti *soft law* vychází monografie zejména z doporučení a stanovisek Pracovní skupiny zřízené dle článku 29 (WP 29), Evropského sboru pro ochranu osobních údajů, Evropského inspektora ochrany osobních údajů a Úřadu pro ochranu osobních údajů.

Při zpracování textu publikace jsem dospěl k závěru, že je vzhledem k výzkumným otázkám nadbytečné provádět extenzivní analýzu a návrhy *de lege ferenda*. Obecné nařízení vstoupilo v účinnost v květnu 2018, a pokud můžeme soudit na základě zkušenosti se směrnicí 95/46/ES, alespoň po dvě další desetiletí není příliš pravděpodobné očekávat zásadnější legislativní změnu obecného rámce právní úpravy ochrany osobních údajů. Tato

38 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

39 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 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.

40 Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. 10. 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.

kniha se tak soustředí více na současnou úpravu a jak zajistit její smysluplnou interpretaci.

Právní stav byl zohledněn ke dni 30. 6. 2020.

1.3 Struktura publikace

Tato publikace je členěna do sedmi kapitol, které zahrnují rovněž její Úvod a Závěr.

Druhá kapitola nazvaná Premisy je věnována historickému a systematickému kontextu práva na ochranu osobních údajů. Shrnuje stav současného poznání, zabývá se jeho vztahem k právu na soukromí a k právu na informační sebeurčení a vymezuje základní předpoklady, na kterých právní úprava ochrany osobních údajů spočívá. První premisou je, že právo na ochranu osobních údajů je formulováno jako samostatné právo, které se již zcela oddělilo od práva na soukromí, a to jak v účelech a cílech, tak metodách regulace. Navazující část druhé kapitoly přednáší druhou premisu, přistupuje ke zpracování osobních údajů z pohledu správce údajů a vymezuje pragmatický předpoklad vhodnosti a nezbytnosti probíhajícího zpracování osobních údajů pro fungování moderní společnosti. Právní úprava ochrany osobních údajů tak právně rámuje prostor, v němž zpracování údajů probíhá. Umožňuje jej a zároveň stanoví jeho limity. Třetí část druhé kapitoly se zaměřuje na práva subjektů údajů. Popisuje významnou roli pozitivně formulovaných práv subjektů údajů, která jsou v analyzované právní úpravě obsažena a uvádí jako třetí premisu systému ochrany osobních údajů, že subjektivní pozitivní práva plní významnou funkci v zajištění kontroly správce údajů po celou dobu probíhajícího zpracování. Druhá a třetí premisa stojí ve vzájemném napětí, když odpovídají dvěma základním účelům, které právní úprava ochrany osobních údajů má plnit. Jsou jimi zajištění ochrany fyzických osob (subjektů údajů) před zneužitím jejich osobních údajů[41] a umožnění využití osobních údajů pro zpracování, která jsou v širokém slova smyslu přínosná pro společnost. Konečně poslední, čtvrtá, premisa je přednesena ve čtvrté části druhé kapitoly a spočívá v nezbytnosti preventivního přístupu k ochraně osobních údajů. Ten se prakticky projevuje při

41 Touto širokou formulací účelu právní úpravy mám na mysli projev jak distributivní, tak nedistributivní součásti práva na ochranu osobních údajů.

interpretaci předpisů upravujících ochranu osobních údajů tak, že definiční ustanovení zakládající působnost těchto předpisů je třeba vykládat extenzivně a ustanovení zakládající výjimky naopak restriktivně. Na těchto premisách jsou postaveny následující části této publikace.

Třetí a čtvrtá kapitola se zabývají stavem systému ochrany osobních údajů v minulosti. Třetí kapitola je věnována popisu výsledků případových studií, které poukazují na nedostatečnost předchozí právní úpravy (směrnice 95/46/ES a zní vycházejícího zákona č. 101/2000 Sb.) ve směru potřeby pružně reagovat na výzvy, které před ni stavěl technologický vývoj. Z tohoto pohledu spočíval její hlavní problém v absenci nástroje, který by dokázal zajistit dostatečnou granularitu a škálovatelnost povinností správce údajů. Čtvrtá kapitola představuje dva přístupy, kterými se v minulosti pokoušely dozorové orgány a soudy překonat nedostatky popsané v kapitole třetí. První metodou byla restriktivní interpretace klíčových definičních pojmů tak, aby na tyto problematické případy právní úprava osobních údajů vůbec nedopadla. Druhou metodou pak bylo *ad hoc* rozhodnutí dozorových úřadů nevymáhat takto problematické případy.

Pátá kapitola tvoří argumentační jádro této publikace. Představuje moderní regulatorní metodu v podobě performativních pravidel, která silně spočívá na teleologických normách. Její podstata spočívá v tom, že regulovaným subjektům určí pouze cíl (který může být jak velmi konkrétní, tak velmi abstraktní), kterého mají dosáhnout, ale již konkrétně neurčuje, jak se to má stát. Metodu performativních pravidel zvolil evropský zákonodárce jako základní regulatorní způsob pro Obecné nařízení. První část páté kapitoly proto detailně popisuje principy performativních pravidel, stejně jako další moderní regulatorní metody. Performativní regulace je v Obecném nařízení provedena prostřednictvím zásady odpovědnosti správce (český pojem má obsahově odpovídat anglickému pojmu *„accountability"*), která v obecnosti stanoví, že správce je odpovědný (ve smyslu *accountable*) za zpracování, které provádí. Té se detailně věnuje druhá část páté kapitoly. Třetím diskutovaným prvkem, nové podoby regulace ochrany osobních údajů, je přístup postavený na riziku, kterému se věnuje třetí část páté kapitoly. Tento přístup propojuje koncept hodnocení rizika se zásadou odpovědnosti, což v konečném důsledku umožňuje granularitu a škálovatelnost povinností

správce. Čtvrtá část páté kapitoly přináší praktické příklady aplikace performativních pravidel v kontextu Obecného nařízení. Pátá část páté kapitoly se pak věnuje otázkám plynoucího času, a zkoumá, zda performativní regulace může zlepšit odolnost právní úpravy ochrany osobních údajů vůči technologickým změnám a zda může pomoci při řešení výzvy v podobě práva být zapomenut.

Šestá kapitola přináší syntézu a diskuzi poznatků a myšlenek představených v předchozích kapitolách. Po rekapitulaci základních argumentů této publikace testuje aplikaci performativních pravidel na případy, kterým byla věnována třetí kapitola a poukazuje na výsledné odlišnosti. V závěru šesté kapitoly je identifikován základní problém regulace ochrany osobních údajů využívající performativních pravidel, zásady odpovědnosti (*accountability*) správce a přístupu postaveném na riziku. Jsou jimi vysoké nároky, které tato metoda regulace klade na správce osobních údajů a na orgány veřejné správy, které povinnosti vyplývající z Obecného nařízení vymáhají.

V závěrečné kapitole publikace jsou zodpovězeny výzkumné otázky, pojmenovány limity tezí představených v rámci jejího textu a naznačeny možné cesty dalšího výzkumu.

2 PREMISY

Právní úprava ochrany osobních údajů je svými cíli přirozeně úzce spjatá s právní úpravou soukromí. Vyplývá to ze samotných předpisů upravujících ochranu osobních údajů,[42] ze soudních rozhodnutí[43] i doktrinálních prací.[44] Maria Tzanou vhodně poznamenává, že mezi těmito právy panuje až rodinný vztah, kdy právo ochrany osobních údajů je potomkem práva na soukromí.[45] Pokud bychom ovšem měli její příměr dovézt do konce, je třeba dodat, že právo ochrany osobních údajů již odrostlo, od svého rodiče se odstěhovalo a začalo si poměrně čile žít vlastním životem. Dokládá to jednak přítomnost samostatného práva na ochranu osobních údajů mezi základními právy Listiny základních práv Evropské unie,[46] dále odkaz na ochranu osobních údajů v dalším ustanovení primárního unijního práva, konkrétně v čl. 16 Smlouvy o fungování EU (bývalý článek 286 Smlouvy o ES) a konečně,

42 Úmluva 108 v čl. 1 uvádí: *„Účelem této Úmluvy je zaručit… každé fyzické osobě… úctu k jejím právům a základním svobodám a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují (‚ochrana údajů').“*, směrnice 95/46/ES pak v bodu 2 odůvodnění zmiňuje, že při zpracování osobních údajů musí být dodržovány základní svobody a práva, zejména právo na soukromí a dnes již zrušený zákon 101/2000 Sb., o ochraně osobních údajů uváděl v § 1, že práva a povinnosti v něm obsažené jsou upraveny za cílem *„naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí“*.

43 Pro příklad je možné uvést rozhodnutí ESLP (Rozsudek Evropského soudu pro lidská práva ze dne 28. 10. 1994 ve věci *Murray vs. Spojené království*, stížnost č. 14310/88; Rozsudek Evropského soudu pro lidská práva ze dne 4. 5. 2000 ve věci *Rotaru vs. Rumunsko*, stížnost č. 28341/95; a Rozsudek Evropského soudu pro lidská práva ze dne 27. 6. 2017 ve věci *Satakunnan Markkinapörssi Oy a Satamedia Oy vs. Finsko*, stížnost č. 931/13), SDEU (Rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist,* C-101/01; Rozsudek Evropského soudního dvora ze dne 29. 1. 2008 ve věci *Promusicae,* C-275/06; a Rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2015, C-362/14) i Ústavního soudu (Nález Ústavního soudu ze dne 18. 8. 2009, sp. zn. I.ÚS 557/09, č. N 188/54 SbNU 325; a Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625).

44 Pro příklad je možné uvést českou komentářovou literaturu k zákonu č. 101/2000 Sb., kdy Alena Kučerová ani Daniel Novák cíle právní úpravy ochrany osobních údajů vzhledem k ochraně soukromí nikterak neproblematizují. Viz NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. In: *ASPI* [Právní informační systém, text aktuální k 1. 7. 2017]; KUČEROVÁ, Alena. § 1. In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář.* Praha: C. H. Beck, 2012, s. 1–2, Beckova edice komentované zákony.

45 TZANOU, Maria. Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures. *Journal of Internet Law,* 2013, roč. 17, č. 3, s. 23.

46 Srovnej Čl. 8 listiny základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

ačkoli to může působit jen jako pouhé gesto, v naprosto precizním a důsledném vynechání byť jediné zmínky o ochraně soukromí v Obecném nařízení.[47] Rozsah aplikace práva na ochranu osobních údajů je v současné době vůči právu na ochranu soukromí na jednu stranu věcně širší (protože se aplikuje i na případy, kdy k žádnému zásahu do soukromí nedochází),[48] na druhou stranu je však omezen na specifickou výseč informačního soukromí (protože se aplikuje toliko na data).[49] Jakkoli lze proto souhlasit s názorem, že ve většině konkrétních situací není vždy smysluplné právo na soukromí a ochranu osobních údajů od sebe striktně oddělovat,[50] koncepční oddělení na abstraktní úrovni je naopak velmi užitečné pro jejich poznání.

Tato kapitola představuje základní premisy, na kterých spočívá zbytek výkladu této knihy. První její část se věnuje vztahu práva na ochranu osobních údajů a práva na soukromí s akcentem na jeho informační aspekt a komparuje jejich vzájemné postavení a rozsah úpravy s cílem zakotvit právo na ochranu osobních údajů jako samostatné základní právo.[51] Zároveň stanoví pro uvedená práva jako východisko právo na informační sebeurčení. Cílem druhé části této kapitoly je ustanovit jako východisko fakt, že zákonodárce uznává zájmy správců údajů na probíhajícím zpracování osobních údajů a zajištění volného toku osobních údajů v rámci Evropské unie. Právní úprava ochrany osobních údajů v principu obecně zpracování osobních údajů nezakazuje,

47 Přesvědčivá argumentace oddělení obou práv viz též HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 3–44.

48 Srovnej např. POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 330, Téma.

49 K překryvu práva na soukromí a ochranu osobních údajů více viz GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 526.

50 Viz například KASL, František. Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 401.

51 Shodně například dále CANNATACI, Joseph A. a Jeanne Pia MIFSUD-BONNICI. Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information & Communications Technology Law* [online]. 2005, roč. 14, č. 1; Samostatnou monografii tématu věnovala Gloria Gonzalez Fuster (GONZÁLEZ-FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Cham, New York: Springer, 2014), opačně argumentuje například Bart van der Sloot (SLOOT, Bart van der. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 19–27).

ale pouze předepisuje, aby probíhalo korektně a co nejvíce šetřilo práva subjektů údajů. To vyplývá například z poměrně širokého množství právních titulů pro zpracování osobních údajů,[52] případně z toho, že volný pohyb osobních údajů mezi členskými státy Evropské unie je jedním z přiznaných cílů právní úpravy ochrany osobních údajů.[53] Třetí část této kapitoly představuje koncept tzv. *„right based approach"*, tedy přístupu založeného na právech,[54] a zaměřuje se na práva subjektů údajů, která jim právní úprava ochrany osobních údajů přiznává. Identifikuje je jako faktický způsob, jakým mohou vůči správci údajů vykonávat své právo na informační sebeurčení. Třetí část tak stojí v myšlené kontrapozici k části druhé, když vymezuje práva subjektů údajů jako limity výkonu zpracování osobních údajů. Konečně, čtvrtá část této kapitoly na základě rozhodovací praxe SDEU zakotvuje princip prevence jako jeden ze základních stavebních kamenů právní úpravy ochrany osobních údajů.

2.1 Soukromí, osobní údaje a informační sebeurčení

2.1.1 Pojem soukromí

Pojem soukromí je nesnadné vymezit. Judith Thomson v polovině sedmdesátých let uvedla: *„Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."*[55] Dodnes jde o velice těžko uchopitelný pojem, který není možné svázat do jedné pevné a trvalé definice.[56] Svědčí o tom

52 Viz čl. 6 odst. 1 Obecného nařízení.

53 Směrnice 95/46/ES byla přijata na základě čl. 100a smlouvy o Evropské unii (nynější čl. 114 smlouvy o fungování Evropské unie), který zmocňuje k vydání legislativy za cílem zajištění fungování vnitřního trhu Unie. Uvedené je dále patrné z bodu 9 odůvodnění směrnice 95/46/ES a ze samotného názvu Obecného nařízení. Více viz LYNSKEY, Orla. From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 60–63.

54 Více viz GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review*, 2016, roč. 2, č. 4.

55 THOMSON, Judith Jarvis. The Right to Privacy. *Philosophy & Public Affairs,* 1975, roč. 4, č. 4, s. 295.

56 Shodně s odkazem na rozhodnutí ESLP ve věci *Marper proti Velké Británii.* NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; Dále viz POLČÁK, Radim a Dan Jerker B. SVANTESSON. *Information sovereignty: data privacy, sovereign powers and the rule of law*. Cheltenham, UK: Edward Elgar Publishing, 2017, s. 90–91.

i velké množství pokusů, které v tomto směru byly učiněny,[57] k čemuž Serge Gutwirth trefně píše *„The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive."*[58] Někteří autoři, jako například výše citovaná Thomson, rovnou došli k závěru, že vůbec nemá smysl pokoušet se soukromí vymezit a vzhledem k jeho instrumentální povaze se soustředit na primární práva, která jsou s jeho ochranou spojena, jako například právo vlastnit majetek.[59]

Pravděpodobně prvními v dlouhé řadě autorů, kteří se o vymezení pojmu soukromí pokusili, byli Samuel D. Warren a Louis D. Brandeis, kteří tak učinili ve svém průlomovém textu The Right to Privacy. V něm o soukromí s odkazem na soudce Thomase McIntyrea Cooleyho hovoří jako o *„right to be left alone"*.[60] Z dalších pokusů o vymezení pojmu je možné uvést Alana Westina,[61] který na konci šedesátých let klasifikoval soukromí do čtyř sfér na spektru od naprosté samoty (*solitude*), při které má člověk možnost být sám se sebou a svými myšlenkami, přes stav intimity (*intimacy*) umožňující navázání rodinných a přátelských vztahů, stav anonymity (*anonymity*), umožňující člověku zůstat skryt v davu, až po rezervaci (*reserve*), při které si *„jedinec upraví své jednání navenek tak, aby s okolím nesdílel o sobě některé informace, které považuje za příliš osobní, citlivé nebo rouhavé."*[62] Je to tak právě úroveň rezervace, na které

57 Srovnej rovněž např. SOBEK, Tomáš. Svoboda a soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, s. 39 a násl., Ediční řada Sborníky, 50.

58 GUTWIRTH, Serge. *Privacy and the information age*. Lanham, Md: Rowman & Littlefield Publishers, 2002, s. 30. Citováno dle FINN, Rachel L., David WRIGHT a Michael FRIEDWALD. Seven Types of Privacy. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 4.

59 Nutno dodat, že Thompson měla k právu na soukromí silně redukcionistický přístup. Viz THOMSON, Judith Jarvis. The Right to Privacy. *Philosophy & Public Affairs,* 1975, roč. 4, č. 4, s. 303; V tomto kontextu lze uvést komentář Rogera Clarka, který vytýkal na konferenci CPDP 2017 Bertu-Jaap Koopsovi, že jeho koncept chápání soukromí ve vztahu k dalším právům, představený v článku A Typology of Privacy, je natolik široký, že by se za soukromí dalo označit už úplně všechno, a tudíž jde o prázdný pojem.

60 WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5, s. 195; Ústavní soud uvedené vyjádření přeložil jako „právo být ponechán sám sobě" (bod 27 nálezu Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625), lépe se však vžil překlad „právo být ponechán o samotě" (viz POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, s. 328–329.

61 WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967.

62 Viz KASL, František. Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 397.

se pohybujeme, když se zabýváme otázkami informačního soukromí a jeho ochrany.[63] Westin k němu přistupoval ze statické pozice, dle které je možné informace ovládat a vykonávat nad nimi kontrolu, což na konci šedesátých let vzhledem ke stavu většinové technologie opravdu stále bylo.[64]

Dále je možné uvést přístup Rogera Clarka, který obecně navázal na Warrena s Brandeisem. Vymezil soukromí jako zájem jedince na zachování osobního prostoru, ve kterém bude uchráněn před zásahy jiných lidí a organizací.[65] Clarke identifikuje jako součást soukromí pět sfér, kterými jsou osobní soukromí (*privacy of the person*), soukromí chování (*privacy of personal behaviour*), soukromí komunikací (*privacy of personal communications*), osobní údaje (*privacy of personal data*). Pátou sféru přidal při přepracování svého textu v reakci na technologicko-společenský vývoj a je jí soukromí osobní zkušenosti (*privacy of personal experience*).[66] Přímo na Clarka pak navázali Finn, Wright a Friedewald, kteří navrhli typů soukromí hned sedm.[67] Dalším příkladem je Daniel Solove, který ve svém textu *Conceptualizing Privacy* navrhl šest kategorií soukromí.[68] Jsou jimi i) právo být nechán o samotě; ii) umožnění omezení přístupu k vlastní osobě; iii) možnost určení a zachování tajemství; iv) kontrola nad osobními informacemi;[69] v) ochrana osobnosti jako

63 Na Westina a kontext soukromí jako možnost nakládání s informacemi ideově navázali například Rachels (RACHELS, James. Why Privacy is Important. *Philosophy & Public Affairs*, 1975, roč. 4, č. 4, s. 326) a Reiman (REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 1976, roč. 6, č. 1, s. 31); V české doktríně, o více než půlstoletí později ve velmi proměněném kontextu informačního soukromí a nových technologií viz FIALOVÁ, Eva. *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges, 2016, s. 52; MATEJKA, Ján, Alžběta KRAUSOVÁ a Vojen GÜTTLER. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 17, s. 101.

64 Srovnej též WEITZNER, Daniel J. et al. Information Accountability. *Communications of the ACM* [online]. 2008, roč. 51, č. 6, s. 87.

65 CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site* [online]. 2016.

66 Ibid.

67 Jde o následující: i) osobní soukromí; ii) soukromí chování a akce (*privacy of behaviour and action*); iii) soukromí komunikací; iv) soukromí datové a osobního obrazu (*privacy of data and image*); v) soukromí myšlenek a pocitů; vi) soukromí místa a prostoru (zahrnuje právo nebýt sledována na veřejnosti); vii) soukromí shromažďování. In FINN, Rachel L., David WRIGHT a Michael FRIEDWALD. Seven Types of Privacy. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 7–10.

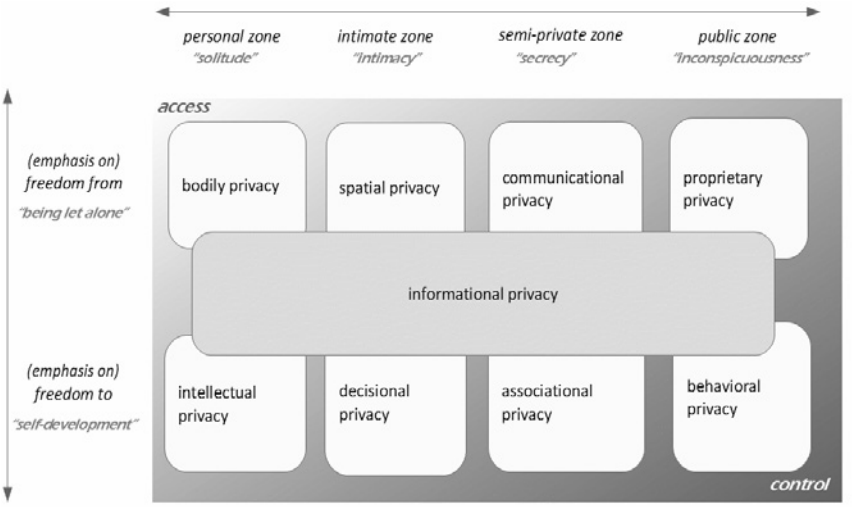
68 SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review* [online]. 2002, roč. 90, č. 4.

69 Solove tedy specificky a výslovně vyčleňuje jako konkrétní druh informační soukromí.

individuality, důstojnosti a autonomie člověka; a vi) intimita.[70] Možné druhy zásahu do informačního soukromí pak Solove systematizoval ve svém navazujícím článku *A Taxonomy of Privacy*.[71]

Poslední typologií, kterou na tomto místě uvádím, je práce Bert-Jaap Koopse a jeho týmu. Ve svém důkladném textu představili celkem devět dimenzí soukromí, z nichž osm je odlišených a devátá je překrývá.[72] Osm základních dimenzí je rozřazeno do prostoru podle dvou os. První je osa navazuje na Westinovy typy soukromí a postupuje od stavu nejniternějšího soukromí (samoty), přes intimitu, tajemství, až po soukromí v rámci veřejného prostoru. Druhá osa má dvě polohy, kterými jsou akcent na ochranu daného práva (právo být nechán o samotě) a akcent na svobodu konání. Devátou Koopsovou sférou soukromí je informační soukromí, které zasahuje všech osm zbývajících, jak přehledně znázorňuje následující obrázek.[73]

Obrázek 1: KOOPS et al. Typologie soukromí



70 Z uvedených kategorií je zcela zřejmý akcent na aspekt faktické možnosti sebeurčení, ať už informačního nebo fyzického.

71 SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review* [online]. 2006, roč. 154, č. 3.

72 KOOPS, Bert-Jaap et al. A Typology of Privacy. *SSRN Scholarly Paper* [online]. ID 2754043. Rochester, NY: Social Science Research Network, 2016 [cit. 30. 6. 2020].

73 Ibid., s. 68.

Koops zmiňuje jako příklad tělesné soukromí, které krom fyzického rozměru omezení přístupu nežádoucích osob k tělu člověka obsahuje rovněž omezení nakládání s informacemi, které s ním souvisí. Doslova pak uvádí: *„Despite the frequency at which informational privacy has been classified as a separate type of privacy alongside (and thus on the same level as) other types, we think it should be represented instead as an overarching aspect… After all, each ideal type of privacy contains an element of informational privacy – that is, a privacy interest exists in restricting access or controlling the use of information about that aspect of human life.“*[74] Koncipováním informačního soukromí jako zvláštní kategorie překrývající ostatní sféry se tak Koopsova typologie odlišuje například od Clarkovy, který umístil rovnítko mezi informační soukromí a osobní údaje a přiřadil jim kategorii nezávislou na ostatních.[75]

Na příkladech uvedených typologií je možné demonstrovat postupný vývoj rozšiřování chápání pojmu a konceptu soukromí, které probíhalo v závislosti na technologickém vývoji. Dominantní postavení pak mezi nimi zaujímá postupně se vynořivší informační soukromí. Domnívám se, že Koopsovo nahlížení na informační soukromí je velice dobře a přesvědčivě koncepčně uchopeno a chápání informačního soukromí jako virtualizovaného[76] informačního odrazu ostatních sfér je vhodnější než jeho konceptualizace jako sféry zcela samostatné. Soukromí je často prezentováno jako zcela esenciální právo, které umožňuje zajištění vlastní autonomie, výkon dalších práv a vůbec fungování jedince v demokratické

74 Ibid., s. 70–71.

75 Clarke uvádí: *„Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.“* CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site* [online]. 2016; Shodně pak rovněž viz FINN, Rachel L., David WRIGHT a Michael FRIEDWALD. Seven Types of Privacy. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 7.

76 K virtualizaci např. LÉVY, Pierre. *Becoming virtual: reality in the Digital Age*. New York: Plenum Trade, 1998.

společnosti.[77] Je to ale právě jeho informační složka, která v uvedeném hraje naprosto klíčovou úlohu. Uvedené je možné demonstrovat na třech příkladech. Za prvé, možnost ovlivnit kdo má přístup k jakým informacím o člověku se přímo odráží na možnosti navazovat sociální vztahy a tím na faktické možnosti zapojení daného člověka ve společnosti.[78] Za druhé, lidé žijící ve společnosti vystavené neustálému sledování se přestávají chovat svobodně, protože se pod vlivem tzv. *„chilling effect"* začínají automaticky přizpůsobovat své chování vyžadované společenské normě („normalizují se").[79] Tento příklad pak úzce souvisí s příkladem třetím, který spočívá v informačním aspektu toho, co Westin nazývá samotou a Koops tělesným[80] a intelektuálním soukromím.[81]

---

77 Srovnej např. WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, s. 53–54, Ediční řada Sborníky, 50; O klíčovosti práva na soukromí pro moderní liberální demokracii se vyjádřil Ústavní soud například v nálezu ze dne 2. 11. 2009, sp. zn. II.ÚS 2048/09, č. N 232/55 SbNU 181, kdy v bodě 19 uvádí: *„Zcela zvláštní respekt a ochranu požívá v liberálních demokratických státech základní právo na nerušený soukromý život osoby (čl. 10 odst. 2 Listiny). Právo na nedotknutelnou soukromou sféru je úhelným kamenem liberální tradice, na které stojí základy moderní politiky i moderního práva, která rovněž stála u zrodu moderních idejí základních práv a svobod. Zajištění autonomní sféry jednotlivce je nejspolehlivější zárukou individuální nezávislosti a lidské svobody."*

78 Jako příklad si můžeme vzít prostou praktickou zkušenost, že jinak se člověk chová a jiné informace o sobě sděluje v různých prostředích a různých společenských kontextech. Druhým příkladem pak je zahlazení jako institut trestního práva, které umožňuje ukrytím informace, že byl jedinec trestán, jeho snadnější zapojení zpět do společnosti. Více srovnej například RACHELS, James. Why Privacy is Important. *Philosophy & Public Affairs*, 1975, roč. 4, č. 4, s. 326.

79 Více k chilling efektu například PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal* [online]. 2016, roč. 31, č. 1, s. 125–129; PENNEY, Jonathon. Chilling effects and transatlantic privacy. *European Law Journal* [online]. 2019, roč. 25, č. 2, s. 126–128; SLOOT, Bart van der. Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, s. 422–425.

80 Koops ho identifikuje následovně: *„… individuals' interest in the privacy of their physical body. The emphasis here is on negative freedom: being able to exclude people from touching one's body or restraining or restricting one's freedom of bodily movement."* KOOPS, Bert-Jaap et al. A Typology of Privacy. *SSRN Scholarly Paper* [online]. ID 2754043. Rochester, NY: Social Science Research Network, 2016, s. 69 [cit. 30. 6. 2020].

81 To Koops vymezuje takto: *„… person's interest in privacy of thought and mind, and the development of opinions and beliefs. While this can have important associational aspects, it is suitable as an ideal type of the personal zone, as the mind is where people can be most themselves."* Ibid., s. 70.

Soukromí je nezbytným předpokladem toho, aby člověk vnímal svoji identitu, své já. Uvedenou myšlenku přednáší Reiman, když interpretuje soukromí a jeho respektování jako společenský rituál. Tím že uznáváme soukromí jiného člověka, uznáváme zároveň jeho osobnost a lidství jako takové. Na základě práce Ervinga Goffmana[82] dochází k závěru, že aby člověk měl morální vlastnictví svého těla, a tedy mohl vnímat svoji identitu jako vlastní, musí být naplněny dvě podmínky. Za prvé je to kontrola nad vlastním tělem, tedy možnost určit, jak s ním bude nakládáno. Za druhé je to informační úroveň kontroly nad vlastním tělem, kterou je myšlena na jedné straně jistota člověka, že prožitky, zkušenosti a vzpomínky jsou opravdu jeho (bez vnějšího zásahu, sledování nebo podsouvání) a na straně druhé možnost sám rozhodnout o tom s kým a za jakých okolností budou sdíleny.[83] Informační úroveň kontroly soukromí jedince může fungovat jen za předpokladu, že ji respektují ostatní členové společnosti, a že uznávají, že by bylo špatně ji narušovat. Reiman doslova uvádí: *„The right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as mine… The right to privacy, then, protects the individual's interest in becoming, being, and remaining a person."*[84] Právo na soukromí a jeho informační složka jsou nezbytnou ochranou identity člověka.[85] Konceptuální chápání informačního soukromí jako druhé strany mince ostatních sfér soukromí je tak klíčové[86] a v kontextu

82 Goffman se v Reimanem citované studii zabýval tím, jak fungují tzv. totální instituce, mezi které řadil např. sirotčince, sanatoria a psychiatrické léčebny, věznice, tábory válečných zajatců, koncentrační tábory, kasárna, lodě, pracovní tábory, ale i kláštery a řádové školy. Mezi základní rysy totálních institucí patří, že všechny činnosti jedince probíhají na stejném místě pod dozorem stejné autority, že je jedinec neustále ve společnosti velkého množství dalších osob a za třetí, že všechny denní činnosti navazují jedna za druhou pod neustálou kontrolou autority. Viz GOFFMAN, Erving. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. 1961, s. 5–7. Goffman uvádí příklady, kdy dochází k nabourávání osobnosti chovanců v totální instituci porušováním jejich soukromí, a to včetně zneužití soukromí informačního například využíváním informací o soukromém životě chovance ze strany dozorového personálu totálních institucí. Ibid., s. 24.

83 REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 1976, roč. 6, č. 1, s. 40–43.

84 Ibid., s. 43.

85 O základní potřebě identity jedince viz též ČERMÁK, Vladimír. *Otázka demokracie. svazek 1*. 2. vyd. Praha: Centrum pro studium demokracie a kultury, 2017, s. 233–238.

86 Reiman svoji myšlenku ještě dále rozvíjí, když uvádí, že totalitní stát je totální instituce na státní úrovni. V tomto směru je možné připomenout ztrátu soukromí jako základní atribut společností v obou základních dystopických románech dvacátého století – Orwellově *1984* i Huxleyho *Konec civilizace: aneb Překrásný nový svět*.

kyberprostoru, ve kterém jde zcela převážně o soukromí informační, pak zcela nezbytné.[87]

Zajímavý přístup k informačnímu soukromí navrhla Helen Nissenbaum, která se pokoušela překonat tradiční dichotomii mezi soukromým a veřejným prostorem či sférou[88] a současně s ní i problém obtížně vyjádřitelného oprávněného očekávání soukromí, které působí jako jedna z kategorií při poměřování, zda došlo nebo nedošlo k zásahu do soukromí.[89] Jako možné východisko vidí koncept kontextové integrity. Problém totiž často nespočívá v tom, že někdo pracuje s informacemi soukromého charakteru vztahující se k člověku, ale v tom, jakým způsobem s nimi pracuje. Postavení právní úpravy ochrany informačního soukromí na rámci kontextů a vztahů v nich obsažených umožňuje překonat problém často nejasného vymezení veřejné a soukromé sféry života. Kontextem Nissenbaum myslí strukturované

87 Reiman na téma navázal roku 1995 článkem, ve kterém identifikuje rizika ztráty soukromí v kontextu nových technologií, které umožňují neustálý dohled nad jedincem (v daném případě šlo o systém sledování cest řidičů projíždějících inteligentními dálničními branami). Při myšlenkové konstrukci svého „informačního panoptikonu" se inspiroval konceptem Jeremyho Benthama a identifikoval 4 rizika, která neustálý dohled (nebo jeho pouhá možnost) může způsobit: i) riziko externí ztráty svobody (ztráta rozhodovací svobody vlivem sociálního tlaku okolí); ii) riziko interní ztráty svobody (když člověk ví, že je sledován, automaticky vkládá do svého rozhodování pohled sledujícího a dle toho upravuje své chování); iii) symbolická rizika (jedná se o symbolickou ztrátu sebe sama ve smyslu výše zmiňovaného Reimanova konceptu soukromí jako nástroje k identifikaci se svým já, svoji identitou. Sledování odebírá člověku právo rozhodnout o svém sebeurčení); iv) riziko psycho-politické proměny (člověk bez soukromí nikdy nemůže dospět v plnohodnotnou samostatnou individuální lidskou bytost, protože nemůže mít dostatečně bohatý vnitřní život, aby si utvořil vlastní názory). REIMAN, Jeffrey H. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer and High-Technology Law Journal*, 1995, roč. 27, č. 1.

88 Byť Nissenbaum vychází z amerického právního prostředí, je tato dichotomie ve formě různých sfér soukromí přítomná i v evropském, potažmo českém právním prostředí. Namátkou je možné uvést rozsudky ESLP ve věcech *Von Hannover* (ze dne 24. 6. 2004, stížnost č. 59320/00), *Von Hannover 2* (ze dne 7. 2. 2012, stížnosti č. 40660/08 a 60641/08) a *Axel Springer* (7. 2. 2012, stížnost č. 39954/08), případně nález Ústavního soudu ze dne 17. 7. 2007, sp. zn. IV.ÚS 23/05, č. N 111/46 SbNU 41 (bod 33); K tématu rovněž například WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, s. 49–62; Více k tématu rovněž TIMAN, Tjerk, Bryce Clayton NEWELL a Bert-Jaap KOOPS (eds.). *Privacy in public space: conceptual and regulatory challenges*. Cheltenham, UK: Edward Elgar Publishing, 2017, Elgar law, technology and society series.

89 Viz NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010, s. 89–126.

sociální prostředí, které se vyvinulo v průběhu času a je určeno svým účelem, místem, kulturou, historií a dalšími charakteristikami.[90] Konkrétně je kontext utvářen rolemi zúčastněných osob, aktivitami, které jsou v kontextu vykonávány, normami ať už právními nebo mimoprávními, které chování v daném kontextu regulují, a hodnotami, které se v rámci kontextu aplikují.[91] Tok soukromých informací v určitém kontextu je pak pro zúčastněné snadno představitelný a umožňuje preciznější zakotvení regulace soukromí. Snadno si představíme kontext univerzitního výzkumu, kontext obchodního vztahu s klientem, nebo kontext návštěvy lékaře. Dokud je zpracování a přenos soukromých informací v souladu s kontextem, ke kterému je dotčená osoba poskytla, nebo ve kterém jejich užití očekává, je zachována integrita kontextu a taková činnost je v pořádku. Problematickým se celý proces stává v okamžiku, kdy dojde k překročení očekávaného kontextu.[92]

2.1.2 Pojem osobní údaje

Oproti pojmu soukromí je pojem osobních údajů velice snadno vymezitelný i vzhledem k existenci poměrně jasné zákonné definice. Ochrana osobních údajů se vztahuje na data (byť Obecné nařízení uvádí pojem informace),[93] která mohou přímo nebo nepřímo vést k identifikaci fyzické osoby. Tu právní úprava označuje jako subjekt údajů. Není předmětem této publikace detailně pojednat o problematice vztahu konceptů data a informace. Přesto alespoň

90 Ibid., s. 130.

91 Ibid., s. 133–134.

92 Ibid., s. 148–150. Je vhodné upozornit na podobnost s institutem ochrany osobních údajů, kterým je princip limitace účelem. Zejména v kontextu aplikace Obecného nařízení je kontextová integrita dle Nissenbaum tomuto principu velice blízká.

93 Zákonodárce v případě osobních údajů používá v zásadě ekvivalentně pojmy „data" (potažmo v českém překladu „údaje") a „informace" a nerespektuje tak základní rozlišení těchto pojmů ať už v jakémkoli kontextu teorií informační vědy. K teoretickému konceptu informace viz ADRIAANS, Pieter. Information. In: ZALTA, Edward N. (ed.). *The Stanford Encyclopedia of Philosophy* [online]. Stanford: Metaphysics Research Lab, Stanford University, 2013 [cit. 30. 6. 2020]; SHANNON, Claude Elwood a Warren WEAVER. *The mathematical theory of communication*. [online]. Urbana: University of Illinois Press, 1949 [cit. 27. 7. 2019]; BUCKLAND, Michael Keeble. Information as a Thing. *Journal of the American Society for Information Science and Technology*. 1991, roč. 42, č. 5; FLORIDI, Luciano. *Information: a very short introduction*. Oxford; New York: Oxford University Press, 2010, Very short introductions, 225; K právní úpravě informací a dat více viz např. BYGRAVE, Lee A. Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxford Journal of Legal Studies,* 2015, roč. 35, č. 1; POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13; TELEC, Ivo. Držba informací. *Právní rozhledy*, 2014, roč. 22, č. 4.

na obecné rovině je třeba uvést, že jedním ze základních (a jak uvádí Floridi, nejméně kontroverzních) vysvětlení pojmu informace je, že se jedná o data, která nesou význam.[94] Informace jsou tedy vyšší sémantickou úrovní dat. V kontextu ochrany osobních údajů můžeme vidět paralelu s obecnou definicí informace, protože osobní údaje jsou data, která v patřičném kontextu vedou k identifikaci fyzické osoby a nesou tedy význam. Již zde je nutné předeslat, že cílem ochrany osobních údajů ovšem není ochrana dat jako takových, ale skrze regulaci nakládání se specifickými daty (která je možné zasadit do takového kontextu, že budou identifikovat fyzickou osobu, a jsou proto osobními údaji) zajistit, že na vyšších sémantických úrovních (informace, znalost) nedojde k jejich zneužití, které by mohlo vyústit až k porušení možnosti rozhodování (a tedy autonomie) člověka.[95] Tento kontext bohužel nebyl evropským zákonodárcem respektován a pojmy data, údaje a informace jsou volně zaměňovány. Pro přehlednost výkladu a snížení rizika zmatení je v této publikaci dodržena terminologie Obecného nařízení, na sémantický vztah pojmů data a informace je však dobré pamatovat.

Osobními údaji jsou tedy všechny identifikátory fyzické osoby jako unikátní čísla osob, jméno, příjmení, adresa, ale rovněž také veškeré další informace zasazené do takového kontextu, který umožní identifikaci dané osoby. Z uvedeného je zřejmé, že překryv právní úpravy osobních údajů a informačního soukromí je poměrně značný. Osobní údaje jsou ale zcela oddělitelné od subjektu údajů,[96] k němuž se váží, a jejich regulace tak bude v obecných rysech stejná, ať už například půjde o osobu veřejného zájmu či nikoli, což v případě ochrany soukromí hraje roli.[97] Cílem právní úpravy osobních údajů je ochrana lidí před neoprávněným zpracováním (sběrem, ukládáním, užitím a šířením) jejich osobních údajů. Subjekty údajů však svá data nevlastní

94 Floridi tuto definici označuje jako „obecnou definici informace". Viz FLORIDI, Luciano. *Information: a very short introduction*. Oxford; New York: Oxford University Press, 2010, s. 22, Very short introductions, 225.

95 Shodně viz ALBERS, Marion. Realizing the Complexity of Data Protection. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 222. Uvedené je detailněji rozebráno ve zbytku této kapitoly.

96 Viz např. POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 330, Téma.

97 Srovnej například Rozsudek Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci *Von Hannover vs. Německo* (No. 2), stížnosti č. 40660/08 a 60641/08.

a nemohou ve velkém množství případů ani zcela vyloučit jejich zpracování, protože právní úprava pragmaticky předpokládá, že zpracování osobních údajů je potřeba.[98] Stejně jako informační soukromí je ochrana osobních údajů zakořeněná v právu na informační sebeurčení.[99]

2.1.3 Právo na informační sebeurčení

Informační rozměr soukromí a ochrana osobních údajů jsou zejména v německém a českém prostředí úzce propojeny s konceptem práva na informační sebeurčení, které bylo poprvé formulováno německým Spolkovým ústavním soudem roku 1983 v případě zabývajícím se sčítáním lidu.[100] Zajímavostí je, že vzhledem k absenci přímo zakotveného konceptu ochrany soukromí v německé ústavě vyšel při formulaci tohoto práva Spolkový ústavní soud z konceptů ochrany lidské důstojnosti a sebeurčení.[101] Právo na informační sebeurčení spočívá v možnosti člověka stanovit si zda a jakým způsobem mají být zveřejněny informace, které se ho týkají.[102] Vzhledem k tomu, že německá judikatura je častým zdrojem inspirace pro český Ústavní soud, není překvapením, že koncept práva na informační sebeurčení převzal[103]

98 Viz HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 3–4.

99 Detailnější srovnání obou režimů regulace je přítomné na konci této části knihy.

100 Rozhodnutí německého Spolkového ústavního soudu ze dne 15. 12. 1983, sp. zn. BvR 209/83, BVerfGE 65.

101 Srovnej LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 572; Dále též HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 14. Autoři rovněž uvádějí, že obdobně byla například ve Francii ochrana osobních údajů vzhledem k absenci jiných možností založena na konceptu svobody.

102 V tomto případě jde o původní tzv. pasivní složku informačního sebeurčení. Aktivní složka informačního sebeurčení, tedy právo na možnost komunikovat s okolím, byla později vyjádřena například českým Ústavním soudem v nálezu ze dne 7. 4. 2010, sp. zn. I.ÚS 22/10, č. N 77/57 SbNU 43. Více viz POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 21.

103 Ústavní soud uvádí ve svých rozhodnutích jako základ práva na informační sebeurčení buď čl. 10 odst. 3 listiny (bod 83 nálezu Ústavního soudu ze dne 12. 12. 2017, sp. zn. Pl.ÚS 26/16 a bod 301 nálezu Ústavního soudu ze dne 27. 11. 2012, sp. zn. Pl.ÚS 1/12, č. N 195/67 SbNU 333), nebo poměrně zajímavě kombinaci čl. 4 odst. 1 a čl. 2 odst. 2 (bod 27 nálezu Ústavního soudu ze dne 1. 12. 2008, sp. zn. I.ÚS 705/06, č. N 207/51 SbNU 577).

a aplikoval jej v řadě svých rozhodnutí.[104] Právo na informační sebeurčení vytváří ideové pozadí subjektivních pozitivních práv vyjádřených jak instituty práva na ochranu osobnosti a soukromí (resp. jeho informační složky),[105] tak zejména práva na ochranu osobních údajů.[106] To potvrzuje rovněž ESLP, který tento koncept do své judikatury poprvé zahrnul v rozhodnutí ve věci Atakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku. V něm identifikoval právo na informační soukromí jako součást práva na respektování rodinného a soukromého života dle čl. 8 Evropské úmluvy o ochraně lidských práv.[107] ESLP propojuje právo na informační sebeurčení s ochranou osobních údajů a uvádí, že toto právo zaručuje jedincům ochranu poskytovanou čl. 8 Úmluvy, když dochází ke zpracování osobních údajů způsobem porušujícím záruky zajištěné čl. 8 a to i tehdy, když předmětné osobní údaje

104 V bodě 30 rozhodnutí Data retention I Ústavní soud uvádí: *„Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními."* Viz nález Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625; Mezi další významná rozhodnutí, ve kterých se Ústavní soud informačnímu sebeurčení věnoval, patří například nález Ústavního soudu ze dne 12. 12. 2017, sp. zn. Pl. ÚS 26/16 (nález ve věci *EET*), nález Ústavním soudu ze dne 21. 4. 2009, sp. zn. II.ÚS 703/06 a nález Ústavním soudu ze dne 17. 7. 2007, sp. zn. IV.ÚS 23/05, č. N 111/46 SbNU 41; K problematice data retention více viz HARAŠTA, Jakub a Matěj MYŠKA. Budoucnost data retention. *Trestněprávní revue,* 2015, roč. 14, č. 10; MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů*. Brno: Masarykova univerzita, 2013, Acta Universitatis Brunensis Iuridica, 456, Edice S.

105 Viz § 84 a násl. zákona č. 89/2012 Sb., občanský zákoník.

106 Jde o práva subjektu údajů jako právo na opravu (čl. 16 Obecného nařízení), právo na výmaz (čl. 17 Obecného nařízení), právo na přenositelnost údajů (čl. 20 Obecného nařízení) a zprostředkovaně rovněž o právo na informace o zpracování (čl. 13–15 Obecného nařízení), protože bez znalosti o probíhajícím zpracování nebo možnosti být informován subjekt nemůže svá další práva vykonávat. K tomu více např. SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review*, 2007, roč. 44.

107 V Čechách přijato a ratifikováno až na počátku devadesátých let 20. století. Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb. m. s., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

jsou samy o sobě neutrální.[108] K širšímu porozumění práva na informační sebeurčení dospěl Radim Polčák, když uvádí, že *„lze chápat pojem informačního sebeurčení jako relativně neurčitý a stále se vyvíjející komplex jednotlivých vzájemně souvisejících distributivních informačních práv, jehož konkrétní rozsah a obsah se mění mimo jiné na základě vývoje informačních technologií… V současné době je možno… označit za integrální součást práva na informační sebeurčení následující instituty: svoboda projevu, ochrana soukromí, právo na vzdělání, ochrana osobních údajů a právo na informace veřejného sektoru.“*[109] Uvedený přístup dobře rámuje různá distributivní informační práva do uchopitelného celku. V kontextu této publikace je však, vzhledem k jejímu zaměření, právo na informační sebeurčení uvažováno pouze v jeho původním úzkém rozsahu, tedy ve smyslu práva na informační soukromí a ochranu osobních údajů.

Vhodný komentář k právu na informační sebeurčení přinesli Rouvrouy a Poullet, když vycházejí z úvahy, že právo na informační sebeurčení je bytostně provázané s autonomií jedince, v čemž můžeme spatřit stejnou linii úvah, jako u výše zmiňovaného Reimana. Rouvrouy a Poullet doslova uvádí: *„What the expression 'informational self-determination' means is rather that an individual's control over the data and information produced about him is a… precondition for him to live an existence that may be said 'self-determined'.“*[110] Souhlasím s nimi, že interpretace chápající právo na informační sebeurčení toliko jako technicky realizované právo k datům a informacím o osobě, by byla nepřiměřeně zužující. Nemá být jen pouhým nástrojem umožňujícím faktickou kontrolu a ovládání informací a osobních údajů vztahujících se k člověku,[111] ale je třeba ho chápat abstraktněji jako nástroj umožňující výkon

108 Shodně ESLP postupoval i v dalších rozhodnutích, viz bod 103 rozsudku Evropského soudu pro lidská práva ze dne 24. 4. 2018 ve věci *Benedik vs. Slovinsko*, stížnost č. 62357/14 a bod 87 rozsudku Evropského soudu pro lidská práva ze dne 28. 6. 2018, ve věcech *M.L. a W.W. vs. Německo*, stížnosti č. 60798/10 a 65599/10.

109 POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 327, Téma.

110 ROUVROY, Antoinette a Yves POULLET. The Right to Informational Self-Determination and the Value of Self-Development. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 51.

111 Zde je nutné upozornit na to, že faktická kontrola informací je navíc z principu nedosažitelná. Viz např. POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 331 a násl.

dalších práv.[112] Jejich výklad je navíc v souladu s původní interpretací německého spolkového i českého Ústavního soudu, které rovněž interpretují právo na informační sebeurčení (a tedy zprostředkovaně rovněž právo na ochranu osobních údajů a v patřičné míře rovněž informační aspekt práva na soukromí) v základu jako právo instrumentální, tedy jako prostředek umožňující ochranu, případně dosažení, dalších základních práv.[113]

Proti chápání práva na informační sebeurčení jako nástroje k zajištění autonomie jedince se vymezuje Roosendaal, když upozorňuje na riziko v podobě „pasti autonomie". Tato past souvisí s nadužíváním souhlasu se zpracováním osobních údajů (a jeho bezmyšlenkovitého poskytování). Uživatelé internetových služeb se do ní dostávají tím, že de iure svým jednáním rozhodují o svých osobních údajích (a tedy o svém informačním sebeurčení), avšak reálně se to neděje, protože jejich rozhodnutí nejsou fakticky dostatečně informovaná a vědomá.[114] Roosendaalova kritika však míří dle mého názoru mimo cíl, který zamýšleli Rouvrouy s Poulletem. Roosendaal zaměnil právo na informační sebeurčení s právem na ochranu osobních údajů a vytýkal jeho konkrétní aplikační problém. Právo na informační sebeurčení však není možné limitovat na konkrétní zpracování osobních údajů. Jedná se o širší, relativně abstraktní koncept, který má za cíl umožnit jedinci naplnit

112 Ke konceptu informačního sebeurčení jako k nástroji garantujícímu možnost se rozhodovat obdobně viz LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 591; FIALOVÁ, Eva. *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges, 2016, s. 57.

113 Viz výše citované rozhodnutí Data retention I., nebo na něj navazující nález Pl.ÚS 26/16 v jehož bodě 83 k právu na informační sebeurčení Ústavní soud uvádí: *„Jednou z primárních funkcí práva a státu v demokracii podle Ústavního soudu je totiž zajišťování prostoru pro rozvoj a seberealizaci individuální osobnosti. Vedle tradičního prostorového chápání soukromí (ochrana obydlí) a možnosti vytvářet sociální vztahy nerušené veřejnou mocí je právo na respekt k soukromému životu i garancí na sebeurčení ve smyslu rozhodování jednotlivce o sobě samém."*

114 Viz ROOSENDAAL, Arnold. We Are All Connected to Facebook… by Facebook! In: GUTWIRTH, Serge et al. (eds.). *European data protection: in good health?* New York: Springer, 2012, s. 14–15; Více k problematice souhlasu se zpracováním viz BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network. 2013 [cit. 30. 6. 2020]; MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9.

autonomii jeho vůle, a jehož je ochrana osobních údajů jedním z projevů.[115] Je přitom důležité zdůraznit, že právo na informační sebeurčení není právem absolutním, protože v mnoha případech je užití určitých informací vázaných k člověku vzhledem k jejich povaze nezbytné (například při řádném výkonu veřejné správy) a není tak možné takový proces na základě vlastního uvážení vyloučit.[116]

2.1.4 Přehled pozitivně právní úpravy ochrany soukromí a osobních údajů

Tato podkapitola nabízí přehled pozitivně právní úpravy ochrany soukromí a osobní údajů, který vytvoří základ pro následující výklad. Na mezinárodně právní úrovni je právo na ochranu soukromého života, rodiny, obydlí a korespondence chráněno článkem 12 Všeobecné deklarace lidských práv roku 1948 a čl. 17 Mezinárodního paktu o občanských a politických právech z roku 1966.[117] Zejména je pak právo na soukromí obsaženo jako součást práva na respektování rodinného a soukromého života dle čl. 8 Evropské úmluvy o ochraně lidských práv.[118] Samotný text čl. 8 obsahuje čtyřlístek garantovaných práv v podobě práva na respektování rodinného a soukromého života, obydlí a korespondence. Jak ale uvádí ESLP, jde o otevřené

115 Je třeba dodat, že na první pohled dochází ke sloučení konceptů osobních údajů a informačního sebeurčení. Shodně viz rovněž Eliška Wagnerová (WAGNEROVÁ, Eliška. Čl. 10. In: WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář.* Praha: Wolters Kluwer, 2012. Dostupné z: ASPI [Právní informační systém]), když výklad věnovaný odst. 3 čl. 10 LZPS označuje jako právo na informační sebeurčení. Ze samotného textu však vyplývá akcent na hodnoty přesahující pouhé osobní údaje. Wagnerová uvádí: *„K potenci veřejné moci ve vztahu ke sběru dat týkajících se různých okruhů, v nichž se odstupňovaně realizuje i soukromý život (k okruhům či sférám viz také body 33-36 nálezu IV.ÚS 23/05) jsme se již zmínili v úvodu. Tyto možnosti jsou způsobilé zmapovat ‚lidskoprávní genom' jednotlivce, který zahrnuje informace nejintimnější, ale i profesní a obchodní, jakož také účast na veřejném životě a společenské aktivity, prostě celý lidský profil. Je zřejmé, že technické a technologické možnosti dnes představují veliké riziko, ba skutečné ohrožení osobní soukromé sféry."*

116 Bygrave v tomto kontextu uvádí, že vedle úplného informačního sebeurčení („self-determination") tak jde mnohdy o informační spolu-určení („co-determination"). Viz BYGRAVE, Lee A. The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal,* 2001, roč. 24, č. 1, s. 2001.

117 Vyhláška MZV č. 120/1976 Sb. ze dne 10. 5. 1976 o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech. Nedodržování této mezinárodní smlouvy vytýkala Charta 77. Viz MOLEK, Pavel. *Politická práva*. 1. vyd. Praha: Wolters Kluwer, 2014, s. 40.

118 Bod 137 rozsudku Evropského soudu pro lidská práva ze dne 27. 6. 2017 ve věci *Satakunnan Markkinapörssi Oy a Satamedia Oy vs. Finsko*, stížnost č. 931/13.

kategorie, protože právo na ochranu soukromého života nemá a ani nemůže mít vyčerpávající definici.[119] Otevřené vymezení bylo autory Úmluvy zvoleno bez pochyb vědomě, protože pojem soukromý život je širší než pojem soukromí.[120] Ve výsledku je možné tvrdit, že právo na soukromý život, je tzv. soudní právo, tedy že jeho konkrétní obsah je fakticky určován judikaturou ESLP a národních vrcholných soudů (nejvyšších soudů a ústavních soudů). V současné době tak tento pojem zahrnuje například ochranu před odposlechy,[121] ochranu intimních aspektů identity jedince,[122] ochranu soukromí v kontextu jednání na veřejnosti[123] a řadu dalších oblastí včetně ochrany vlastního sebeurčení v souvislosti s ochranou osobní autonomie a možnosti osobního vývoje.[124] Právo na ochranu osobních údajů není sice v Evropské úmluvě výslovně obsaženo, ESLP jej však svojí rozhodovací praxí do kontextu čl. 8 zahrnul.[125]

Základním mezinárodněprávním dokumentem upravujícím ochranu osobních údajů tak je úmluva Rady Evropy o ochraně osob se zřetelem

119 Např. bod 33 rozsudku Evropského soudu pro lidská práva ze dne 4. 12. 2008 ve věci *S. a Marper vs. Spojené království*, stížnosti č. 30562/04 a 30566/04; Široká interpretace pojmu rodinný život byla potvrzena rovněž rozsudkem ze dne 2. 8. 1984 ve věci *Malone vs. Spojené království*, stížnost č. 8691/79.

120 Viz KRATOCHVÍL, Jan. Kapitola XVIII [čl. 8 EÚLP]. In: KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C. H. Beck, 2012, s. 867.

121 Viz např. rozsudek Evropského soudu pro lidská práva ze dne 1. 7. 2008 ve věci *Liberty a další vs. Spojené království*, stížnost č. 58243/00; nebo rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2015 ve věci *Roman Zakarov vs. Rusko*, stížnost č. 47143/06.

122 Viz např. bod 63 rozsudku Evropského soudu pro lidská práva ze dne 25. 3. 1992 ve věci *B. vs. Francie*, stížnost č. 13343/87.

123 Např. bod 57 rozsudku Evropského soudu pro lidská práva ze dne 25. 9. 2001 ve věci *P. G. a J. H. vs. Spojené království*, stížnost č. 44787/98; nebo body 58–59 rozsudku Evropského soudu pro lidská práva ze dne 28. 1. 2003 ve věci *Peck vs. Spojené království*, stížnost č. 44647/98.

124 Uvedené dobře shrnují Gellert a Gutwirth, když odkazují na rozhodnutí ESLP ve věcech *Pretty vs. Spojené království* (stížnost č. 2346/02), *Evans vs. Spojené království* (stížnost č. 6339/05) a *Odièvre vs. Francie* (stížnost č. 42326/98). In: GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 524.

125 Například rozhodnutí ve věcech *Murray vs. Spojené království*, stížnost č. 14310/88, *Rotaru vs. Rumunsko*, stížnost č. 28341/95, *Satakunnan Markkinapörssi Oy a Satamedia Oy vs. Finsko*, stížnost č. 931/13 a dalších; Více k otázce ochrany osobních údajů v rozhodovací praxi ESLP viz např. KRATOCHVÍL, Jan. Kapitola XVIII [čl. 8 EÚLP]. In: KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C. H. Beck, 2012, s. 914–920; NARDELL QC, Gordon. Levelling up: Data Privacy and the European Court of Human Rights. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Data protection in a profiled world*. Dordrecht; New York: Springer, 2010, s. 43–52.

na automatizované zpracování osobních dat (Úmluva č. 108).[126] Obsahuje základní principy právní úpravy ochrany osobních údajů, které následně převzala právní úprava Evropské unie i jejích národních států a které jsou tak dodnes aktuální. K mezinárodnímu dni ochrany osobních údajů, tedy k 28. lednu 2019 došlo navíc k ohlášení modernizace této úmluvy, aby byla lépe způsobilá čelit výzvám, které přinesl technologický vývoj.[127]

Na úrovni primárního práva Evropské unie najdeme právní úpravu ochrany soukromí a osobních údajů obsaženou v Listině základních práv Evropské unie.[128] Její článek 7 chrání právo na respektování soukromého a rodinného života, obydlí a komunikace, přičemž jeho textace je doslova převzatá z Evropská úmluvy o ochraně lidských práv. Článek 8 však dává právní základ samostatné úpravě práva na ochranu osobních údajů.[129] Zmínit je vhodné rovněž čl. 16 Smlouvy o fungování EU (bývalý článek 286 Smlouvy o ES), který výslovně zakotvuje, že každý má právo na ochranu osobních údajů, které se jej týkají. Na úrovni evropského sekundárního práva mezi hlavní nástroje zaručující ochranu osobních údajů a soukromí patří Obecné nařízení o ochraně osobních údajů (nařízení č. 2016/679),[130] jakožto obecný předpis, směrnice č. 2016/680 (tzv. policejní směrnice) upravující zpracování osobních údajů v kontextu vyšetřování a stíhání trestné činnosti,[131] směrnice 2002/58/ES ve znění směrnice 2009/136/ES (tzv. e-Privacy směrnice)

126 Viz sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Úmluva 108 sama vychází z právně nezávazných, ale inspirativních pravidel Organizace pro hospodářskou spolupráci a rozvoj vydaných (OECD) roku 1980. Srovnej OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online].

127 COUNCIL OF EUROPE. Modernisation of the Data Protection "Convention 108". *Council of Europe* [online]. [cit. 30. 6. 2020].

128 Viz listina základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

129 Více ke vztahu práva na ochranu soukromí a práva na ochranu osobních údajů dále v této části.

130 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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).

131 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 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 rámco.vého rozhodnutí Rady 2008/977/SVV.

věnovaná ochraně soukromí v kontextu elektronických komunikací,[132] a nařízení 2018/1725, které upravuje zpracování osobních údajů orgány, institucemi a dalšími subjekty Evropské Unie.[133] Rozhodovací praxe Soudního dvora Evropské unie je takřka výlučně navázaná na starou směrnici 95/46/ES, která byla zrušena Obecným nařízením. Nicméně, vzhledem k tomu, že Obecné nařízení spočívá na stejných základech a principech jako zrušená směrnice, je obecně i nadále aplikovatelná. Právně nezávazným, avšak velice autoritativním zdrojem právních informací týkajících se práva na ochranu soukromí a osobních údajů na úrovni Evropské unie jsou stanoviska a doporučení bývalé Pracovní skupiny zřízené podle čl. 29 směrnice 95/46/ES („WP 29"), s účinností Obecného nařízení přetransformované do podoby Sboru pro ochranu osobních údajů.

V českém právním řádu je ochrana soukromí zakotvena na úrovni ústavního pořádku především čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 LZPS.[134] Je nezbytné explicitně upozornit na čl. 10 odst. 3 LZPS, který výslovně zakládá právo *„na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě."* Rozhodovací praxe Ústavního soudu následuje judikaturu ESLP a přistupuje ke konceptu soukromého a rodinného života se stejně rozšiřující tendencí.[135] Na úrovni předpisů právní síly zákona je ochrana soukromí přítomná zejména v § 86 Občanského zákoníku,[136] který specificky uvádí jako dimenze soukromí ochranu soukromých

132 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

133 Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. 10. 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Text s významem pro EHP).

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

135 Viz např. nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I.ÚS 453/03, č. N 209/39 SbNU 215.

136 Viz § 86 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

prostor, soukromého života a soukromých písemností.[137] Ochrana osobních údajů je upravena v zákoně 110/2019 Sb., o zpracování osobních údajů, který je harmonizačním předpisem Obecného nařízení a obsahuje rovněž implementaci směrnice 2016/680 a specifickou úpravu pro zpracování osobních údajů orgány veřejné moci mimo působnost Obecného nařízení (například jde o výkon k zajištění bezpečnosti státu a tajné služby). České soudy, zejména pak Ústavní a Nejvyšší správní, rovněž judikaturně zasáhly do oblasti ochrany osobních údajů. Byť tato rozhodnutí vykládají ustanovení již zrušeného zákona č. 101/2000, jsou do značné míry stále použitelná, podobně jako rozhodnutí SDEU vztahující se ke směrnici 95/46/ES.

2.1.5 Právo na ochranu osobních údajů jako základní právo a jeho účel

Právo na ochranu osobních údajů je vzhledem k právu na soukromí samostatným a nezávislým právem, byť obě z nich v základu sledují stejný cíl, kterým je ochrana soukromí člověka a zprostředkovaně následně rovněž i další základních práv. Pro přesvědčivé zakotvení práva na ochranu osobních údajů jako samostatného základního práva je vhodné obě práva porovnat a upozornit na rozdíly mezi nimi. Cílem této části je proto shrnout poznatky předchozích částí této podkapitoly a upozornit na rozdíly mezi jednotlivými právy.[138]

Obě práva se primárně liší v cílech, kterých má být jejich prostřednictvím dosaženo, a v předmětu své úpravy. Zatímco cílem práva na soukromí, jak

137 Ke vztahu práva na ochranu soukromí a práva na ochranu osobních údajů se v českém kontextu vyjádřili např. MAŠTALKA, Jiří. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*, 2010, roč. 18, č. 10; NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*, 2012, roč. 20, č. 13–14; Z komentářové literatury je možné uvést ze strany ochrany soukromí TŮMA, Pavel. § 86 [Právo člověka na soukromí]. In: LAVICKÝ, Petr (ed.). *Občanský zákoník: komentář*. 1. vyd. Praha: C. H. Beck, 2014, s. 51, Velké komentáře; Ze strany osobních údajů pak viz NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; KUČEROVÁ, Alena. § 1. In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 1–2, Beckova edice komentované zákony.

138 Jsou hodnoceny primárně hmotněprávní aspekty obou práv, protože procesní otázky nejsou podstatné z hlediska zakotvení práva na ochranu osobních údajů jako základního práva a tedy ani z hlediska této kapitoly.

je zakotveno v čl. 8 Evropské úmluvy o ochraně lidských práv, Listině základních práv EU a českém právním řádu, je výslovně ochrana před zásahem do čtyř aspektů soukromí (soukromý život, rodinný život, domov a korespondence),[139] cílem ochrany osobních údajů je ochrana před neoprávněným (škodlivým) zpracováním osobních údajů. Jak uvádí Gellert s Gutwirthem, ochranu osobních údajů můžeme chápat jako *„korektní nakládání s informacemi"*.[140] Peter Hustinx k systému ochrany osobních údajů uvádí: *„It was not designed to prevent the processing of such information or to limit the use of information technology per se."*[141] Z uvedeného vyplývá, že právní úprava ochrany osobních údajů obecně má probíhající zpracování osobních údajů za daný základ,[142] na rozdíl od právní úpravy ochrany soukromí, která obecně zásah do soukromí zapovídá, ledaže je možné aplikovat některou ze zákonných výjimek nebo souhlas dotčené osoby.[143] I v případě zpracování osobních údajů správce údajů potřebuje mít před jeho začátkem právní titul, který zpracování umožní a bez kterého by bylo protiprávní.[144] V tomto ohledu vypadá na první pohled ochrana osobních údajů funkčně ekvivalentní s ochranou soukromí.[145] Zásadní rozdíl však spočívá v šíři, v níž právní úprava ochrany osobních údajů zpracování umožňuje tím, že se správce může spolehnout na větší množství právních titulů, které mohou být poměrně

139 Je však třeba připomenout výše zmiňovaný rozšiřující výklad ESLP (a v jeho šlépějích kráčející Ústavní soud), který chápe ochranu soukromého života široce v kontextu zajištění svobody.

140 Viz GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 525; Dále též SLOOT, Bart van der. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 3.

141 HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 123, The collected courses of the Academy of European Law.

142 Srovnej např. body 4 a 5 odůvodnění Obecného nařízení.

143 Srovnej § 86 zákona č. 89/2012 Sb.

144 Viz čl. 6 odst. 1 Obecného nařízení.

145 Možná i tento fakt zmátl českého zákonodárce, když do zákona č. 101/2000 Sb. zakotvil odchylně od směrnice č. 95/46/ES jako základní právní titul souhlas subjektu údajů a ostatní právní tituly jako výjimky z něj. Více viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 29–30. Tento přístup samozřejmě respektovala i rozhodovací praxe českých soudů (např. viz odst. 19 rozsudku Nejvyššího správního soudu ze dne 19. 4. 2018, č. j. 2 As 107/2017-72).

široké (např. důvod oprávněného zájmu správce nebo třetí osoby).[146] Tento aspekt ochrany osobních údajů je možné demonstrovat příkladem směrnice 95/46/ES. Ta byla přijata k naplnění dvou cílů: a) dosažení jednotného trhu skrze umožnění volného pohybu osobních informací a b) ochrana základních práv a svobod obyvatel Evropského společenství, přičemž hlavní legislativní akcent ležel na prvním z nich.[147] Cílem ochrany osobních údajů je tak v jádru zajištění rovnováhy mezi zájmy správců a subjektů údajů.[148]

Na první pohled je zřejmé, že se krom cílů ochrany liší i její předmět. Ochrana soukromí včetně jejího informačního aspektu spočívá na materiální povaze osobnosti konkrétního člověka a její rozsah odpovídá jeho informační diskreci, tedy jak se svým soukromím nakládá.[149] Při konkrétním hodnocení otázky, jestli bylo nebo nebylo v určitém případě zasaženo do práv daného člověka, tak bude například hrát roli, zda jde o veřejně známou osobnost, zda se rozhodl vystoupit se svým soukromím na veřejnost, zda měl oprávněné očekávání soukromí a podobně. Oproti tomu v případě ochrany osobních údajů tyto otázky roli primárně nemají,[150] protože předmětem ochrany jsou právě osobní údaje vztahující se k danému člověku. Ochrana osobních údajů je tvořena specifickými pravidly vztahujícími se k nakládání s daty a k zajištění transparentnosti zpracování. Jde například o princip omezení účelem,[151] právo subjektu údajů na informace o zpracování a přístup k údajům, povinnost jejich zabezpečení a další.[152] Z uvedeného vyplývá rozdílný rozsah úpravy obou institutů. Zatímco právo na ochranu soukromí zahrnuje oproti právu na ochranu osobních údajů rovněž neinfor-

146 Viz čl. 6 odst. 1 písm. f) Obecného nařízení a s ním související body odůvodnění č. 47–49.

147 Srovnej First report on the implementation of the Data Protection Directive (95/46/EC). In: *EurLex* [online]. 2003, s. 3.

148 Srovnej BYGRAVE, Lee A. The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal*, 2001, roč. 24, č. 1.

149 Srovnej POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 330, Téma.

150 Mohou se projevit až uvnitř systému ochrany osobních údajů v konkrétních případech hodnocení internalizovaných testů proporcionality, jako je například hodnocení oprávněného zájmu správce údajů na zpracování osobních údajů.

151 Zde je možné však upozornit na blízkost tohoto principu s konceptem kontextové integrity Nissenbaum.

152 Srovnej HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 10.

mační aspekty soukromí,[153] ochrana osobních údajů se vztahuje i na takové případy zpracování osobních údajů, při kterých nedochází k zásahu do práva na soukromí, například vzhledem k nízké intenzitě zásahu do něj.[154] Oblast překryvu obou práv je tvořena oblastí informačního soukromí.[155] Právní úprava ochrany osobních údajů však prostřednictvím nastavení limitů nakládání s osobními údaji poskytuje ochranu subjektu údajů i v kontextu dalších základních práv,[156] jako je například právo na spravedlivý proces,[157]

153 Ve smyslu Koopsovy typologie jde o osm základních sfér soukromí.

154 Shrnutí relevantní rozhodovací praxe ESLP k této otázce nabízí například LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 585.

155 Zbývá dodat, že právo na informační sebeurčení v úzkém smyslu slova zahrnuje jak celou oblast práva na ochranu osobních údajů, tak specificky oblast informačního soukromí. Hlavní důvod pro zachování tohoto rozlišení vidím v tom, že byť se právo na ochranu osobních údajů a právo na soukromí z části překrývají (a je to právě část odpovídající oblasti informačního soukromí), není možné je vzhledem k odlišným regulačním nástrojům sloučit. Subjekt, kterému bylo chybným zpracováním osobních údajů zasaženo do práva na soukromý život, se může rozhodnout, zda bude své právo chránit instituty typickými pro ochranu soukromí (tedy primárně po linii soukromého práva prostřednictvím ochrany práva na soukromí požadovat odstranění závadného obsahu, případně prostřednictvím přímých nároků vyplývajících z Obecného nařízení, byť samozřejmě i v tomto případě je možné uvažovat o veřejnoprávní cestě v podobě trestněprávní sankce odpovídající některé ze skutkových podstat uvedených v Části druhé, Hlavě II, Dílu 2, zákona č. 40/2009 Sb., trestní zákoník), nebo po linii správního práva (tedy prostřednictvím státní autority v podobě Úřadu pro ochranu osobních údajů), nebo oběma variantami. Byť budou výsledky odlišné, jde v obou případech o výkon práva na informační sebeurčení.
Na zjevnou spojitost informačního soukromí a ochrany osobních údajů poukázal rovněž Jan Camenisch, když ve své studii věnované ochraně informačního soukromí online nabízí jako řešení metodu minimalizace osobních údajů a principy data protection by design a data protection by default. Viz CAMENISCH, Jan. Information privacy?! *Computer Networks* [online]. 2012, roč. 56, č. 18.

156 Gellert s Gutwirthem připomínají rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist,* C-101/01, kde soud v bodech rozhodnutí 97–99 sice konstatuje, že cílem směrnice 95/46/ES je *„zachování rovnováhy mezi volným pohybem osobních údajů a ochranou soukromého života"*, nicméně působnost její právní úpravy může být i širší. Viz GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 529.

157 Například protiprávního zpracování osobních údajů v kontextu vyšetřování trestné činnosti, nebo v kontextu výkonu veřejné správy. Za tímto účelem ostatně byla přijata směrnice EU 2016/680. Dalším příkladem je možnost zpracování osobních údajů za účelem zajištění důkazů v rámci civilního řízení. K tomuto více viz MAŘÁDEK, David. Pořízení zvukového záznamu soukromou osobou a obecné možnosti jeho použití jako důkazního prostředku v civilním soudním řízení. *Právní rozhledy*, 2015, roč. 23, č. 13–14.

právo mít majetek,[158] právo na informace a svobodu projevu,[159] ochrana před diskriminací[160] a další. Základní právo na ochranu osobních údajů tak připomíná deštník, který překrývá další základní práva. Podobně jako deštník chrání před bouří a promoknutím, působí ochrana osobních údajů jako prevence před zásahem do těchto dalších základních práv díky tomu, že je možné nástroje ochrany osobních údajů aplikovat dříve, než samotný zásah nastane.[161] Uvedené dobře shrnují Gellert s Gutwirthem, když tvrdí: *„… the fundamental right to personal data protection is bound to overlap with other rights because instead of granting a 'substantial' freedom (such as the secrecy of correspondence, freedom of speech, freedom of religion, etc.) it is limited to determine the extent to which an infringement on our (undetermined) liberty can go (in this case, the practice consisting in processing personal data). This contrasts starkly with other rights that both grant a 'substantial' freedom and provide for the means to determine the limits of such freedom."*[162] Zatímco tedy právo na ochranu soukromí garantuje ochranu člověka před zásahem do jeho soukromého a rodinného života, právo na ochranu osobních údajů tím, že předmětem jeho regulace jsou údaje a nikoli přímo člověk, vytváří limity nakládání s údaji a díky tomu zprostředkovaně chrání řadu

158 Například zpracování osobních údajů vedoucí ke krádeži identity a jejímu následnému zneužití, nebo protiprávním vytváření profilů, na jejichž základě je nabízeno zboží a služby za méně výhodných podmínek.

159 Jde o aspekt Clarkova soukromí zkušenosti. V případě protiprávního zpracování osobních údajů může docházet k nekontrolovatelnému zkreslování toho, k jakým informacím má subjekt údajů přístup, což nutně ovlivní i jeho právo na svobodu projevu. K tématu personalizovaných zpráv více např. ESKENS, Sarah. A right to reset your user profile and more: GDPR-rights for personalized news consumers. *International Data Privacy Law* [online]. 2019.

160 Příkladem může být automatizované rozhodování na základě sesbíraných dat bez vědomí subjektu údajů. Více k riziku skrytého rozhodování viz SOLOVE, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven Conn.: Yale University Press, 2013, s. 197; K vazbě mezi ochranou osobních údajů a antidiskriminačními předpisy viz MÉTAYER, Daniel Le. a Julien Le CLAINCHE. From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles. In: GUTWIRTH, Serge et al. (eds.). *European data protection: in good health?* New York: Springer, 2012, s. 323.

161 Teprve okamžikem porušení je často možné využít právních nástrojů charakteristických pro daná práva. Více k preventivnímu principu v poslední části této kapitoly.

162 GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 530.

dalších práv, včetně (primárně) práva na ochranu soukromí.[163] Jak ale připomíná Marion Albers, bylo by chybou na osobní údaje nahlížet jen úzkým pohledem technické regulace jejich zpracování: *„The goal of data protection is not the protection of data but of the individuals to whom the data refer. The object of protection, then, is not the personal data per se. We must expand this isolated view by including several elements: at a basic level the element of information; in the structural dimension knowledge; in the temporal dimension the flow of data and information; and in the broader context decisions and consequences of decision.“*[164] Při hodnocení účelů a cílů právní úpravy je třeba nezapomenout na to, že v konečném důsledku je cílem právní úpravy ochrana člověka před zásahy do jeho práv, které by mohly být způsobeny zpracováním jeho osobních údajů a to po celou dobu probíhajícího zpracování. Aspekt času je tak nesmírně klíčový.

Určité oddělení osobních údajů od člověka ukazuje další rozdíl mezi právem na soukromí a právem na ochranu osobních údajů. Právo na soukromí je typickým zástupcem distributivního práva, jelikož z něj plynou oprávnění konkrétním subjektům, které se ho mohou rovněž dovolat před soudem.[165] Oproti tomu právo na ochranu osobních údajů má vedle své distributivní složky rovněž silnou složku nedistributivní realizovanou v podobě dozorové činnosti nezávislého Úřadu pro ochranu osobních údajů.[166] Vzhledem

163 González Fuster s Gellertem ve svém článku označují právo na soukromí jako „pozitivní svobodu“ garantující člověku konkrétní práva (ve smyslu privilegia) a v kontrastu s ním identifikuje právo na ochranu osobních údajů jako „negativní svobodu“. V obdobném duchu Gabriela Zanfir označuje ochranu osobních údajů za „procesní právo“, které nemá samostatnou hodnotu, ale pomáhá s efektivním zajištěním dalších „hmotných“ práv. Viz ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 245–246; PURTOVA, Nadezhda. Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights. *Netherlands Quarterly of Human Rights,* 2010, roč. 28, č. 2, s. 183; Kriticky se k oddělení osobních údajů od člověka vyjadřuje Polčák například v POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014 [cit. 30. 6. 2020].

164 ALBERS, Marion. Realizing the Complexity of Data Protection. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 222.

165 Srov. POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, s. 303.

166 Nezávislost dozorového orgánu je jednou ze základních podmínek jak bývalé, tak současné evropské právní úpravy. Jejím porušením může být například předčasné ukončení mandátu orgánu dozoru, jako se to stalo v Maďarsku. Viz Rozsudek Soudního dvora Evropské unie ze dne 8. 4. 2014 ve věci *Komise vs. Maďarsko,* C-288/12.

k provázanosti ochrany osobních údajů s právem na soukromí, právem na informační sebeurčení a faktickým zajištěním možnosti realizace svobody jednotlivce a tím zprostředkované svobody celé liberální demokratické společnosti, existuje veřejný zájem na tom, aby nedocházelo k protiprávnímu zpracování osobních údajů, tedy například aby nevznikaly velké databáze plné osobních údajů (ať už v rámci činnosti veřejné správy nebo v soukromých rukách), které by mohly být v budoucnosti zneužitelné.[167]

Jako poslední argument hovořící ve prospěch samostatného základního práva na ochranu osobních údajů je jeho vývoj v souvislosti s přijetím Lisabonské smlouvy.[168] Směrnice 95/46/ES byla přijata na základě čl. 100a smlouvy o Evropské unii (nynější čl. 114 smlouvy o fungování Evropské unie), který zmocňuje k vydání legislativy za cílem zajištění fungování vnitřního trhu Unie. Vzhledem k tomu bylo hlavním legislativním cílem zajištění volného pohybu těchto dat v rámci Unie, byť dle jejího odůvodnění[169] i dle vyjádření Komise[170] byl druhý cíl, tedy ochrana osobních údajů zejména s ohledem na právo na soukromí, stejně důležitý. Přesto panovaly nejistoty, zda není akcent na ochranu základních práv směrnicí 95/46/ES překročením kompetencí založených primárními smlouvami.[171] Uvedené se odráží ve starší judikatuře Soudního dvora, která neklade akcent na právo

167 Srovnej body odůvodnění 2 a 4 Obecného nařízení. K rizikům zpracování velkých dat viz např. BERTOT, John Carlo et al. Big data, open government and e-government: Issues, policies and recommendations. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2014, roč. 19, č. 1/2; CUMBLEY, Richard a Peter CHURCH. Is "Big Data" creepy? *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5; NARAYANAN, Arvind, Joanna HUEY a Edward W. FELTEN. A Precautionary Approach to Big Data Privacy. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, s. 357–485; TENE, Omer a Jules POLONETSKY. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 2012, roč. 11.

168 Detailní zpracování vytváření ochrany osobních údajů jako základního práva viz GONZÁLEZ-FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Cham; New York: Springer, 2014.

169 Body 3–7 odůvodnění směrnice 95/46/ES.

170 Viz First report on the implementation of the Data Protection Directive (95/46/EC). In: *EurLex* [online]. 2003, s. 3.

171 Srovnej např. LYNSKEY, Orla. From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht, Springer Netherlands, 2013, s. 63.

na ochranu osobních údajů jako takové, ale právo na soukromý život zakotvený v čl. 8 Evropské úmluvy o ochraně lidských práv.[172] Soudní dvůr zároveň v dalších rozhodnutích aktivně akcentoval jako cíl směrnice harmonizaci jednotného trhu a nikoli ochranu základních práv.[173] Lisabonská smlouva přinesla z hlediska ochrany osobních údajů dvě zásadní změny. První bylo zakotvení ochrany osobních údajů do čl. 16 Smlouvy o fungování Evropské unie, díky čemuž zmizely pochybnosti o platnosti právního základu směrnice 95/46/ES a druhou bylo přiznání síly primárního unijního práva Listině základních práv Evropské unie[174] včetně jejího čl. 8, který právo na ochranu osobních údajů výslovně zakládá jako samostatné základní právo. S příchodem Obecného nařízení je pak právo na ochranu osobních údajů detailně upraveno na nejvyšší možné unijní úrovni. Změnu, kterou přinesla Lisabonská smlouva, samozřejmě reflektoval Soudní dvůr Evropské unie, který retrospektivně začal vykládat směrnici 95/46/ES tak, že jejím cílem je zajištění vysoké úrovně ochrany osobních údajů a soukromí občanů unie.[175] V rozsudku ve věci Coty Germany Soudní dvůr pak výslovně uvedl, že čl. 8 Listiny základních práv EU a směrnice 95/46/ES zaručují základní právo všech osob na ochranu osobních údajů.[176]

172 Například rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist,* C-101/01, a zejména pak rozsudek Evropského soudního dvora ze dne 20. 5. 2003 ve věci *Österreichischer Rundfunk a další,* C-465/00,. Viz HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 29–33.

173 Jde o rozsudek ze dne 16. 12. 2008 ve věci *Satakunnan Markkinapörssi a Satamedia*, C-73/07, ve kterém Soudní dvůr mimo jiné dospěl k závěru, že právo na výraz „výlučně pro účely žurnalistiky" je třeba chápat široce, což je jedna z mála výjimek, kdy Soudní dvůr upřednostnil jiné právo než ochranu osobních údajů; Dále jde o rozsudek ze dne 24. 11. 2011 ve věci *ASNEF*, C-468/10, ve kterém Soudní dvůr uvedl, že zpřísnění právních titulů ke zpracování osobních údajů národním právem je nepřijatelné z důvodu možného narušení volného trhu ve Společenství. Více viz LYNSKEY, Orla. From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht, Springer Netherlands, 2013, s. 72–73.

174 Listina základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

175 Srovnej například bod 66 rozsudku Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12), nebo bod 27 rozsudku Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13).

176 Bod 30 rozsudku Soudního dvora Evropské unie ze dne 16. 6. 2015, C-580/13.

Na základě výše uvedeného mám za to, že právo na ochranu osobních údajů musí být považováno za samostatné základní právo funkčně zcela nezávislé na právu na ochranu soukromí, případně dalších základních právech.[177] Vzhledem k tomu je nezbytné ptát se po jeho účelech, tedy po tom, k čemu má jeho aplikace vést. Důležitost účelu právní úpravy formuloval Rudolf von Jhering, když tvrdil, že stvořitelem celého práva je účel a není právní normy, která by nevděčila za svůj původ nějakému účelu, tedy praktickému motivu.[178] Na nejobecnější úrovni je pak účelem práva zajištění životních podmínek společnosti.[179] Gustav Radbruch identifikoval jako základní strukturu účelů práva tři prvky, kterými jsou spravedlnost, právní jistota a praktická užitečnost.[180] Radbruchovy kategorie účelů práva se nacházejí ve vzájemné kontrapozici. Kategorie praktické užitečnosti (obecného blaha) míří na zajištění hodnot, z nichž těží širší společnost, kategorie spravedlnosti pak v duchu kantovské centrality člověka chrání jedince ve střetu jeho zájmů se zájmy širší společnosti.[181] Účel právní jistoty pak celému systému dodává nezbytnou stabilitu. Radim Polčák ve svém starším textu věnovaném smyslu právní úpravy ochrany osobních údajů zmiňuje rovněž Lawrence Lessiga[182] a jeho základní pravidlo, že právo by mělo být takové, aby činilo

177 Shodně viz např. GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5; Opačný názor zastává SLOOT, Bart van der. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 3–30. Jeho hlavními argumenty jsou podpůrná funkce ochrany osobních údajů, kterou jsou chráněna další práva, a fakt, že ne všechna zpracování dosahují takové intenzity, aby mohla být předmětem ochrany základních práv, protože jsou v zásadě triviální (s. 21). Nemyslím si, že je možné rozsekávat abstraktní normativní úpravu základního práva na jednotlivé iterace jeho použití. Van der Slootův přístup je podobný, jako kdybychom tvrdili, že právo vlastnit majetek není základním právem, protože jednotlivé nákupy zeleniny na uvaření polévky jsou triviální, což je zjevně absurdní.

178 JHERING, Rudolf von. *Law as a means to an end*. Přel. HUSIK, Isaac. Boston: The Boston book company, 1913, s. liv.

179 Citováno dle HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 126.

180 Citováno dle POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 2; Pavel Holländer Radbruchovy kategorie prvků účelu práva uváděl jako spravedlnost, právní jistotu a obecné blaho (viz HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 132).

181 Více viz HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 132.

182 POLČÁK, Radim. Aims, methods and achievements in European data protection. *International Review of Law, Computers & Technology* [online]. 2009, roč. 23, č. 3, s. 179–180.

dobře, potažmo dobro (*„do good"*).[183] Tázat se po účelech základního práva na ochranu osobních údajů je nezbytné i z toho důvodu, že formulace účelů právní úpravy umožňuje zajištění koherence jeho interpretace. Při aplikaci práva v kontextu nových technologií je vhodné vycházet z pragmatického přístupu, protože tento přístup umožňuje flexibilně reagovat na konkrétní situaci.[184] Pro pragmatickou aplikaci práva je poznání účelu právní úpravy zcela zásadní, protože teleologická intepretace umožňuje překlenout napětí mezi textem právní normy a technologickou realitou.[185]

V návaznosti na předchozí části této podkapitoly jsem identifikoval následující účely právní úpravy ochrany osobních údajů. S těmito účely na mysli je pak konstruován rovněž zbytek této publikace. Právní úprava ochrany osobních údajů sleduje dva hlavní účely. Můžeme o ní tedy říct, že má duální povahu.[186]

Prvním účelem je zajištění ochrany fyzických osob (subjektů údajů) před zneužitím jejich osobních údajů. Tomuto cíli odpovídá čl. 1 odst. 2 Obecného nařízení, který stanoví, že Obecné nařízení *„chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů"*.[187] Je třeba si povšimnout odklonu od práva na ochranu soukromí. Účelem práva na ochranu osobních údajů již není primárně ochrana soukromí fyzických osob, alespoň ne přímo.[188] Právo na ochranu osobních údajů nepřímo zajišťuje ochranu celé řady dalších práv a zájmů subjektů údajů, a to včetně práva na soukromí. Jde však o zprostředkovanou ochranu realizovanou ujištěním, že člověku nevznikne újma zneužitím jeho osobních údajů nebo jejich nekorektním zpracováním. Součástí tohoto účelu přitom není jen o ochrana subjektivních práv člověka (ve smyslu distributivní složky práva na ochranu osobních

183 LESSIG, Lawrence. *Free culture: how big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press, 2004, s. 305–306.

184 POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 76–81, Téma; POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 5.

185 Srovnej též POSNER, Richard A. *Law, pragmatism, and democracy*. Cambridge, Mass: Harvard University Press, 2003, s. 67–68.

186 Srovnej též LYNSKEY, Orla. *The foundations of EU data protection law*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2015, s. 46 a násl., Oxford studies in European law.

187 Viz čl. 1 odst. 2 Obecného nařízení.

188 Účel ochrany soukromí byl formulován v čl. 1 směrnice 95/46/ES.

údajů), ale rovněž ochranu veřejného dobra v podobě vytvoření bezpečného regulovaného prostředí, které člověka chrání, aniž by si to nutně sám aktivně uvědomoval (nedistributivní složka práva na ochranu osobních údajů).[189] V tomto prvním účelu můžeme spatřovat odraz Radbruchovy kategorie účelu spravedlnosti právní úpravy.

Druhým účelem je umožnění využití osobních údajů pro zpracování, která jsou v širokém slova smyslu přínosná pro společnost.[190] Odraz tohoto účelu můžeme spatřovat v textaci čl. 1 odst. 3 Obecného nařízení, který garantuje volný pohyb osobních údajů v Unii. Právní úprava ochrany osobních údajů je pragmatická a nesnaží se zamezit zpracování osobních údajů jako takovému. Naopak, jejím účelem je umožnit korektní zpracování osobních údajů, které bude přínosné správci údajů a v širším smyslu též společnosti.[191] Ve druhém účelu tak můžeme vidět odraz Radbruchovy kategorie účelu praktické užitečnosti (obecného blaha). Přítomné je rovněž napětí mezi prvním a druhým účelem úpravy.

Závěrem této části je možné konstatovat, že na právo na ochranu osobních údajů je možné takřka bez jakéhokoli problému vztáhnout i Lessigův poněkud abstraktní účel práva „činit dobře". Pokud by měl být systém ochrany osobních údajů shrnut do jednoho pravidla, jedné maximy, byl by to pokyn pro správce údajů ve znění *„buď dobrý – zpracovávej osobní údaje, ale dělej to tak, abys minimalizoval rizika újmy subjektu údajů"*.[192]

189 Srovnej POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 341–345, Téma.

190 Obdobně též Polčák, který označil za jeden z cílů právní úpravy osobních údajů (byť dle směrnice 95/46/ES) ekonomický pokrok (POLČÁK, Radim. Aims, methods and achievements in European data protection. *International Review of Law, Computers & Technology* [online]. 2009, roč. 23, č. 3, s. 180); Shodně též LYNSKEY, Orla. *The foundations of EU data protection law*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2015, s. 47 a násl. Oxford studies in European law.

191 Viz bod 4 odůvodnění Obecného nařízení, který stanoví, že *„Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy."*

192 Jde samozřejmě rovněž o obecnou prevenční povinnost, která je v kontextu českého práva formulována např. v § 2900 Občanského zákoníku (zákon č. 89/2012 Sb.) následovně: *„Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného."*

2.2 Ochrana osobních údajů jako rámec pro probíhající zpracování

Legislativní a politické dokumenty věnované ochraně osobních údajů potvrzují, že probíhající zpracování osobních údajů je v moderní společnosti fakticky nezbytné a tedy, že cílem právní úpravy ochrany osobních údajů je rovněž jeho umožnění. Jako nejstarší příklad je možné uvést pravidla Organizace pro hospodářskou spolupráci a rozvoj vydaná roku 1980, v jejichž preambuli stojí: *„On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers… Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.“*[193] Obdobné vyjádření je pak přítomné i v úmluvě 108, v jejíž preambuli je vyjádřena nezbytnost volného toku informací mezi lidmi.[194] V kontextu evropského práva je zmiňovaný aspekt patrný již z faktu, že směrnice 95/46/ES byla přijata jako nástroj, který krom zajištění ochrany subjektů údajů má pomoci harmonizovat společný vnitřní trh pro umožnění efektivnějšího zpracování a přenosu osobních údajů. Tento cíl byl pak zachován i v případě Obecného nařízení.[195] Vrátíme-li se ještě na okamžik ke srovnání práva na ochranu osobních údajů s právem na soukromí, tak druhé jmenované v sobě podobný procedurální cíl nenese. Závěry o rozdílném obsahu obou práv potvrzují rovněž Gloria González Fuster s Raphaelem Gellertem, když ve svém článku s odkazem na práci Isaiaha Berlina[196] označují právo na soukromí jako „pozitivní svobodu“ garantující člověku konkrétní práva (ve smyslu privilegia) a v kontrastu s ním identifikují právo na ochranu osobních údajů jako „negativní svobodu“, které chrání zájmy a svobody člověka

193 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online].

194 Viz Sdělení ministerstva zahraničních věcí č. 115/2001 Sb., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

195 Viz body č. 2–9 odůvodnění Obecného nařízení.

196 Autoři odkazují na původní vydání z roku 1969, předmětná esej však vyšla rovněž v dostupnějším vydání roku 2002. Viz BERLIN, Isaiah, Henry HARDY a Ian HARRIS. *Liberty: incorporating four essays on liberty*. Oxford: Oxford University Press, 2002, s. 178–179.

prostřednictvím regulace chování, které by je mohlo zasáhnout.[197] Pokud právo na soukromí ustupuje jiným právům, děje se tak na základě jeho zákonného omezení[198] a po provedení plného testu proporcionality hodnotícího přednost jednoho z kolidujících práv.[199]

Právní regulace ochrany osobních údajů je vrcholně pragmatická, protože vychází ze základního předpokladu, že zpracování osobních údajů při činnostech a naplňování potřeb moderní společnosti bude a musí probíhat,[200] a je jejím cílem, aby se tak dělo korektním způsobem, který bude co nejméně

197 GONZÁLEZ FUSTER, Gloria a Raphaël GELLERT. The fundamental right of data protection in the European union: In search of an uncharted right. *International Review of Law, Computers and Technology* [online]. 2012, roč. 26, č. 1, s. 80. Neznamená to ale, že by právní úprava ochrany osobních údajů stavěla subjekt údajů do zcela pasivní role. Dává mu řadu nástrojů, pomocí kterých může ověřovat, že správce údajů provádí své povinnosti správně, případně může směřovat případné nedostatky na úřady pro ochranu osobních údajů, které počínání správce mohou kontrolovat z pozice státní autority. Primárním předmětem regulace je však probíhající zpracování a ten, kdo ho provozuje, nikoli právo konkrétního člověka.

198 Omezením je myšlena např. Čl. 7 odst. 1 věta druhá LZPS, případně čl. 8 odst. 2 Evropské úmluvy o ochraně lidských práv a základních svobod. Srovnej například LANGÁŠEK, Tomáš. Čl. 7. In: WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012. Dostupné z: ASPI [Právní informační systém].

199 K zásadě proporcionality viz HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 219–239; Zásadní teoretické uchopení zásady proporcionality viz ALEXY, Robert a Julian RIVERS. *A Theory of Constitutional Rights*. Oxford, New York: Oxford University Press, 2009; Bohatou judikaturou týkající se zásady proporcionality oplývá český Ústavní soud (počínaje nálezem Ústavního soudu ze dne 12. 1. 1994, sp. zn. Pl.ÚS 4/94, č. N 46/2 SbNU 557, č. 214/1994 Sb., dále je možné uvést například nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl.ÚS 3/02, č. N 105/24 SbNU 177, č. 405/2002 Sb. a nález Ústavního soudu ze dne 28. 1. 2004, sp. zn. Pl.ÚS 41/02, č. N 10/32 SbNU 61, č. 98/2004 Sb.). Z hlediska práva na ochranu soukromí a osobnosti jsou zajímavé případy, ve kterých se ÚS věnuje proporcionalitě v kontextu pořizování fotografického a zvukového záznamu (např. nález Ústavního soudu ze dne 21. 3. 2002, sp. zn. III.ÚS 256/01, N 37/25 SbNU 287 a nález Ústavního soudu ze dne 9. 12. 2014, sp. zn. II.ÚS 1774/14, č. N 221/75 SbNU 485).

200 Srovnej například bod 4 odůvodnění Obecného nařízení, případně častá prohlášení, že data (a tedy i osobní údaje) jsou novým olejem světové ekonomiky. Srov. např. KUNEVA, Meglena. Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling. *Europa.eu* [online]; a VERSACI, Guiseppe. Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law,* 2018, roč. 14, č. 4, s. 377; K podobnému závěru je možné dojít i z textace směrnice 2019/770 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb, ve které je výslovně zanesen předpoklad možnosti poskytnout osobní údaje výměnou za poskytnutí online služby.

zasahovat do práv subjektů údajů.[201] Probíhající zpracování osobních údajů tudíž automaticky samo o sobě nutně nepředstavuje zásah do základních práva člověka.[202] Je pravdou, že aby mohl správce údajů provádět jejich zpracování, musí splnit zákonné povinnosti, které mu z právní úpravy plynou a bez jejich splnění je takové zpracování protiprávní a jako takové zakázané. Jde zejména o nezbytnost mít právní titul, který zpracování umožňuje. Jak však bude do detailu pojednáno dále, je právní úprava fakticky nastavena tak, že nabízí značnou šíři aplikace existujících právních titulů tak, aby bylo možné osobní údaje zpracovávat v celé řadě případů po právu. Trefně přirovnal koncept ochrany osobních údajů k politice udržitelného rozvoje Lee A. Bygrave, když ve svém článku z roku 2001 uvádí: *„… it can be argued that data protection laws have much the same aim and function that policies of ‚sustainable development' have in the field of environmental protection. Data protection laws seek to safeguard the privacy and related interests of data subjects at the same time as they seek to secure the legitimate interests of data controllers in processing personal data just as policies of 'sustainable development' seek to preserve the natural environment at the same time as they allow for economic growth. Both policy concepts promote a belief that the potential for conflict between these respective sets of interests can be significantly reduced through appropriate management strategies. Concomitantly, both policy concepts can be used to create an impression that the interests of data subjects and the natural environment are adequately secured, even when their respective counter-interests are also secured."*[203] Cílem právní úpravy ochrany osobních údajů je tedy zajistit, aby probíhající zpracování mělo co nejmenší negativní dopady na subjekty údajů a tím zprostředkovaně na společnost jako celek. V případě ochrany osobních údajů

201 Viz HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection*? Dordrecht: Springer, 2009, s. 3; Shodně též ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 245.

202 Samozřejmě i pro právo na ochranu osobních údajů platí, že pokud se dostane do střetu s jiným základním právem, je tento střet řešen zásadou proporcionality. Dobře to ukázala rozhodnutí ÚS ve věcech Data retention (nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625, 94/2011 Sb.; nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl.ÚS 24/11, č. N 217/63 SbNU 483, 43/2012 Sb.; a nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl.ÚS 45/17, č. 161/2019 Sb.).

203 BYGRAVE, Lee A. The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal*, 2001, roč. 24, č. 1, s. 282.

jsou „vhodnými strategiemi" ve smyslu citovaného Bygravova komentáře základní zásady řídící zpracování osobních údajů. Jde například o povinnost správce údajů zajistit technické a procesní zabezpečení zpracování osobních údajů, aby zabránil jejich úniku. Zejména jde však o zásadu limitace účelem zpracování, která představuje úhelný kámen celého systému právní ochrany osobních údajů.[204]

Klíčová role účelu zpracování vyplývá již z druhého odstavce čl. 8 Listiny základních práv EU, který zní: „[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.*"[205] Z citovaného ustanovení je zřetelná dynamika celé regulace, která je založena na třech bodech.[206] Prvním a ve skutečnosti zcela primárním je požadavek na účelové vymezení zpracování a jeho korektnost,[207] druhým bodem je nezbytnost právního titulu pro zpracování osobních údajů, které je však již vymezeno účelem, a proto i vhodný právní titul je třeba vybírat dle daného účelu, a konečně třetí bod spočívá v zajištění informovanosti a práva na informační sebeurčení subjektů údajů.[208]

---

204 Srovnej např. GUTWIRTH, Serge. *Short statement about the role of consent in the European data protection directive* [online]. Brusel: Bepress. 2012 [cit. 30. 6. 2020].

205 Čl. 8 odst. 2 Listiny základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

206 Jejich detailnější rozbor je přítomný dále v této publikaci.

207 Srovnej ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 247; Dále též k zásadnosti účelu zpracování osobních údajů např. NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; BYGRAVE, Lee A. *Data privacy law: an international perspective*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2014, s. 153–157; a HERBST, Tobias. Art. 5. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 218–231; VOIGT, Paul a Axel von dem BUSSCHE. *The EU general data protection regulation (GDPR)*. New York, NY: Springer Berlin Heidelberg, 2017, s. 88–90.

208 K nezbytnosti dostupných informací o probíhajícím zpracování se trefně vyjádřil Solove, když přirovnal skryté zpracování osobních údajů a následné rozhodování na něm založené ke Kafkově Procesu. SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review*, 2007, roč. 44, s. 756–757. Více je tématu práv subjektu údajů věnována třetí část této kapitoly.

Princip omezení účelem byl přítomný již v pravidlech pro zpracování osobních údajů, které vydala OECD,[209] a v Úmluvě 108.[210] Jde tedy o velice tradiční zásadu, která se vine právní úpravou ochrany osobních údajů od jejího počátku. Účel zpracování je zcela klíčový proto, že jsou na něj navázány téměř všechny další základní zásady zpracování osobních údajů zakotvené v čl. 5 Obecného nařízení.[211] Vzhledem k tomu je stanovení účelu nezbytně prvním krokem správce při zahájení zpracování údajů.[212] Dle vymezeného účelu zpracování je tak třeba posuzovat, jaké osobní údaje je možné zpracovávat,[213] jakými způsoby[214] a jak dlouho je možné údaje uchovávat.[215] Účel pro zpracování proto musí být konkrétní, specifický a legální, což znamená, že musí být v souladu nejen s právní úpravou ochrany osobních údajů, ale rovněž s právním řádem jako celkem.[216] Důležitou součástí zásady limitace účelem je, že obecně není možné změnit účel zpracování v jeho průběhu, protože právní úprava zapovídá zpracování osobních údajů způsobem, který je se stanoveným účelem neslučitelný.[217] Takto silná akcentace vazby na účel zpracování ukazuje, že právní úprava ochrany osobních údajů je procedurální v tom smyslu, že se soustředí konkrétně na jednotlivé procesy zpracování osobních údajů a reguluje je.[218] Nový účel zpracování

209 Viz odst. 9 a 10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online].

210 Viz čl. 5 in Sdělení ministerstva zahraničních věcí č. 115/2001 Sb., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

211 Tomu odpovídal čl. 6 směrnice 95/46/ES, pro který právě uvedená teze platila také. S výjimkou obecného požadavku na korektnost a zákonnost vyjádřeného v jeho písm. a) byl vztah k účelu zpracování přítomný ve všech dalších písmenech tohoto článku.

212 Shodně viz NOVÁKOVÁ, Ludmila. § 5, Odst. 1, písm. a]. In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář.* Praha: C. H. Beck, 2012, s. 102, Beckova edice komentované zákony.

213 Jen nezbytné a přesné vzhledem k danému účelu v souladu se zásadami minimalizace a přesnosti údajů dle čl. 5 odst. 1 písm. c) a d) Obecného nařízení.

214 Údaje není možné zpracovávat způsobem, který je neslučitelný s daným účelem (čl. 5 odst. 1 písm. b) Obecného nařízení).

215 Opět obecně jen po dobu nezbytnou pro daný účel, v souladu se zásadou omezení uložení dle čl. 5 odst. 1 písm. e) Obecného nařízení.

216 Srovnej PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 3/2013 o limitaci účelem. *Evropaská komise* [online]. 2. 4. 2013, s. 19–20 [cit. 30. 6. 2020].

217 Viz čl. 5 odst. 1 písm. b) Obecného nařízení, detailně je o problematice pojednáno ve výše citovaném stanovisku WP 29, č. 3/2013, s. 21 a násl.

218 K nezbytnosti chápání ochrany osobních údajů a její regulace jako procesu v čase více viz POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 8 [cit. 30. 6. 2020].

osobních údajů tak fakticky zakládá nový proces zpracování, tedy nové zpracování osobních údajů.

Otázka slučitelnosti následného zpracování je upravena v čl. 6 odst. 4 Obecného nařízení, které je tak nutné chápat jako výjimku z obecného zákazu změny účelu. Dle tohoto ustanovení je možné nové zpracování za novým účelem provádět buď na základě uložené právní povinnosti, souhlasu subjektu údajů, nebo pokud je nový účel slučitelný s účelem původním. Při hodnocení slučitelnosti je pak třeba brát v potaz zejména jakoukoli vazbu mezi oběma účely, okolnosti shromáždění údajů, povahu správce, existující vztah mezi správcem a subjektem údajů a možné důsledky zamýšleného dalšího zpracování pro subjekt údajů. Jinými slovy, nové zpracování je možné, pokud jej subjekt údajů mohl důvodně očekávat.[219] Tento přístup odpovídá konceptu kontextové ochrany informačního soukromí, jak o něm hovoří Nissenbaum, když uvádí znaky, pomocí kterých je možné určit, zda nový informační proces potenciálně zasahující do soukromí odpovídá procesu původnímu.[220] Při porovnání obou metod je zřejmé, že omezení účelem zpracování představuje užší přístup, než širší omezení kontextem (např. při výkonu činností v kontextu školy a zacházení s daty studentů může zahrnovat několik procesů zpracování, zatímco Nissenbaum toto uvádí jako příklad jednoho kontextu), obě metody však spočívají na stejném základě, kterým je dynamické nakládání s chráněnými informacemi.[221]

Zatímco účel zpracování tvoří rám, ve kterém má zpracování probíhat, právní titul je klíčem, bez kterého není možné začít. Čl. 8 Listiny základních práv EU stanoví, že na prvním místě mezi nimi spočívá souhlas se zpracováním osobních údajů. Tento přístup je pochopitelný, protože souhlas jako jedinečný projev vůle představuje aspekt projevu autonomie jedince. Na druhé straně, čl. 8 rovněž výslovně připouští možnost jiných právních titulů. Podíváme-li se pak do předpisů sekundárního evropského práva, je zřejmé, že souhlas je v praxi pouze jedním z právních titulů ke zpracování

219 Srovnej PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 3/2013 o limitaci účelem. *Evropaská komise* [online]. 2. 4. 2013, s. 24–25 [cit. 30. 6. 2020].

220 Viz NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010, s. 149–150.

221 Více se k tomuto tématu vracím v kapitole 6 této publikace.

osobních údajů a jeho role se nesmí přecenit.[222] Souhlas (podobně jako další právní tituly) je vzhledem ke zpracování podmínkou nutnou, nikoli však postačující. Pokud by správce osobních údajů porušoval základní zásady navazující na účel zpracování, případně by byl účel zpracování od základu protiprávní, souhlas se zpracováním nemůže takovou činnost legitimovat.[223] Na druhou stranu se to samozřejmě vztahuje i na opačný případ – bez právního titulu není možné provádět zpracování osobních údajů. To platí, i pokud je řádně stanovený jeho účel a jsou dodrženy požadavky s ním spojené.

Úprava právních titulů pro zpracování dobře ukazuje, že zákonodárce uznává nezbytnost zpracování osobních údajů a bylo jeho cílem jej umožnit. Zároveň s tím však bylo nezbytné poskytnout subjektu údajů dostatečné záruky ochrany jeho zájmů a základních práv. Obecné nařízení nabízí v prvním odstavci čl. 6 celkem šest právních titulů, kterými správce může podložit své zpracování. Vedle již zmíněného souhlasu se zpracováním, uvedeným pod písmenem (a), je možné zpracovávat osobní údaje, pokud je zpracování (b) nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů;[224]

222 Viz čl. 7 směrnice 95/46/ES, čl. 6 Obecného nařízení, čl. 5 nařízení EU č. 2018/1725. Více k této argumentaci viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 29–30; Detailně se problematice souhlasu se zpracováním věnovala WP 29 ve svém stanovisku č. 15/2011 (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 15/2011 k definici souhlasu. *Evropská komise* [online]. 13. 7. 2011, 38 s. [cit. 30. 6. 2020].) a v kontextu Obecného nařízení pak v Pokynech pro souhlas podle nařízení 2016/679 (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Pokyny pro souhlas podle nařízení 2016/679. *Evropská komise* [online]. 28. 11. 2017, v revidovaném znění ze dne 10. 4. 2018, č. WP259rev.01, 32 s. [cit. 30. 6. 2020]).

223 Je samozřejmě možné uvažovat o souhlasu jako o okolnosti vylučující protiprávnost, tehdy se však tato úvaha pohybuje mimo výsostné vody systému ochrany osobních údajů. Pokud bychom chtěli pracovat striktně se souhlasem se zpracováním osobních údajů ve smyslu čl. 6 odst. 1 písm. a) Obecného nařízení, není možné se požadavkům principu vymezení účelu vyhnout. Více obecně ke konceptu souhlasu v právu BEYLEVELD, Deryck. *Consent in the Law*. Oxford: Hart Publishing, 2007.

224 Aby mohly být osobní údaje zpracovávány na základě právního titulu plnění smlouvy, musí být jejich zpracování pro splnění daného smluvního závazku přísně nezbytné. Jde tedy například o zpracování údajů o adrese kupujícího v e-shopu, protože bez ní by nebylo možné zboží doručit.

(c) nezbytné pro splnění právní povinnosti správce údajů;[225] (d) nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;[226] (e) nezbytné pro splnění úkolu správce prováděného ve veřejném zájmu;[227] nebo (f) nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, ledaže by zpracování nepřiměřeně zasahovalo do zájmů a základních práv subjektu údajů. S výhradou národních zvláštností[228] jde o konečný výčet právních titulů umožňujících zpracování osobních údajů, na které dopadá aplikace Obecného nařízení.[229] V tom se právní úprava liší od stavu směrnice 95/46/ES a zákona č. 101/2000 Sb., které obsahovaly

225 Pro možnou aplikaci tohoto právního titulu musí zákon přesně specifikovat povinnost zpracovávat nějaké osobní údaje. Půjde tedy například o situace, kdy dochází na základě zákonného zmocnění k předávání údajů ze základních registrů, když jsou zveřejňovány údaje z registru osob nebo insolvenčního rejstříku, případně když je vedena zdravotnická dokumentace. Více viz NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; a KUČEROVÁ, Alena. § 5 odst. 2 písm. a). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 133–138, Beckova edice komentované zákony.

226 I v tomto případě se může jednat pouze o případy, kdy je zpracování vzhledem k situaci nezbytné. Bod 46 odůvodnění Obecného nařízení k tomu uvádí, že tento právní titul je možné použít jen v případě, že není zjevně možné použít žádný jiný. Oproti staré právní úpravě zákona 101/2000 Sb. doznal tento právní titul změny, protože již není přítomná podmínka vyžadující následné potvrzení zpracování souhlasem subjektu údajů. Vanda Foldová uvádí jako příklady životně důležitého zájmu subjektu údajů záchranu zdraví a života nebo ochranu majetku vysoké hodnoty. Viz FOLDOVÁ, Vanda. § 5 odst. 2 písm. c). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 141, Beckova edice komentované zákony.

227 Toto je nový právní titul, který do českého práva přineslo Obecné nařízení a v předchozí právní úpravě dle zákona 101/2000 Sb. nebyl obsažen, ačkoli ho směrnice 95/46/ES znala. Svým základem je velice blízký právnímu titulu dle písm. c), ovšem na rozdíl od něj pro jeho aplikaci není nezbytné, aby byla zákonem stanovena jasná povinnost. Stačí, když je orgán veřejné správy (nebo jiný relevantní subjekt) zmocněn k provádění nějaké činnosti a zpracování osobních údajů je její nezbytnou součástí, aniž by to ale zákon výslovně reflektoval. Subjekt údajů má možnost se proti takovému zpracování bránit vznesením námitky proti zpracování dle čl. 21 Obecného nařízení. Více viz např. NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Dostupné z: ASPI [Právní informační systém].

228 V české právní úpravě je jako zvláštní právní titul pro zpracování zanesen § 17 zákona č. 110/2019 Sb., který umožňuje zpracování osobních údajů *„slouží-li to přiměřeným způsobem pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu"*. Jde o aplikaci výjimky umožněné čl. 85 Obecného nařízení, který dává členským státům možnost upravit si dle svých národních zvyklostí rovnováhu mezi ochranou osobních údajů a právem na svobodu projevu. Zároveň můžeme toto české ustanovení chápat jako specifikaci právního titulu oprávněného zájmu.

229 Zpracování osobních údajů ležících mimo aplikační rozsah Obecného nařízení může být podmíněno jinak.

ještě zvláštní právní tituly pro zpracování tzv. citlivých osobních údajů.[230] V případě čl. 9 Obecného nařízení, který upravuje zpracování zvláštních kategorií osobních údajů (jak jsou nyní citlivé údaje nazývány[231]), však nejde o samostatné právní tituly, které by byly vůči čl. 6 v poměru speciality, ale o další úroveň podmínek, které musí být splněny současně s právními tituly dle čl. 6.[232]

Výčet právních titulů dle čl. 6 Obecného nařízení ukazuje, že subjekt údajů ve velkém množství případů nemůže aktivně ovlivnit, zda bude ke zpracování osobních údajů docházet nebo ne. Svoji vůli může projevit při volbě dodavatele zboží nebo služby, se kterým uzavírá smlouvu, pro jejíž splnění je dané zpracování nezbytné, případně může udělit souhlas se zpracováním, pokud není žádný jiný právní titul aplikovatelný. Ve všech ostatních případech však může správce osobních údajů údaje zpracovávat bez aktivního projevu vůle (nebo i proti vůli) subjektu údajů, zejména probíhá-li zpracování na základě plnění právní povinnosti uložené zákonem nebo za účelem plnění úkolu veřejného zájmu.[233]

---

230 § 4 písm. b) zákona č. 101/2000 Sb. definoval citlivé údaje jako *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů."*

231 Obsahově však došlo jen k minimálním změnám, když je čl. 9 vymezuje jako údaje, *„které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby."*

232 S počátkem účinnosti Obecného nařízení tak došlo k interpretačnímu posunu. Tento interpretační závěr je nezbytný, protože jinak by osobní údaje spadající do zvláštních kategorií byly v některých případech méně chráněné než údaje běžné. Jde konkrétně o situaci, kdy čl. 9 odst. 2 písm. e) umožňuje zpracování zvláštních osobních údajů, pokud je subjekt údajů sám zjevně zveřejnil. Na tuto situaci však není nijak pamatováno v čl. 6. Pokud bychom připustili interpretaci, že čl. 9 nabízí zvláštní právní tituly, tak by bylo možné zpracovávat zveřejněné údaje spadající mezi zvláštní kategorie bez dalšího právního titulu dle čl. 6. To by je stavělo do horší pozice než údaje běžné, což vzhledem k jejich privilegovanému postavení není možné. Shodně viz WEICHERT, Thilo. Art. 9. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 322–323; NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Dostupné z: ASPI [Právní informační systém].

233 Uvedené však neznamená, že by subjekt údajů neměl nad zpracováním žádnou možnost vlády nebo kontroly. Tu mu zajišťují pozitivně formulovaná práva, o kterých bude více řeč ve třetí části této kapitoly.

Velice specifickým právním titulem je umožnění zpracování osobních údajů, pakliže je to nezbytné pro účely oprávněných zájmů správce údajů nebo třetích strany podle čl. 6 odst. 1 písm. f) Obecného nařízení. Tento právní titul v sobě obsahuje internalizovaný test proporcionality, protože správce údajů se na něj může spolehnout pouze tehdy, pokud nemají přednost zájmy a základní práva a svobody subjektu údajů. Na rozdíl od střetu dvou základních práv na ústavní úrovni, probíhá při jeho aplikaci hodnocení vzájemného vztahu protichůdných hodnot uvnitř systému ochrany osobních údajů (proto jej nazývám internalizovaný). Tento právní titul byl znám již v kontextu směrnice 95/46/ES a jeho úprava v Obecném nařízení vychází ze stejných základů. Vzhledem k tomu je možné při jeho analýze (po patřičné mírné úpravě) vycházet z judikaturních a doktrinálních zdrojů, které souvisejí se starou úpravou. Základní popis tohoto institutu nabízí Pospíšil, když uvádí: *„Možnost zpracovávat osobní údaje na základě § 5 odst. 2 písm. e) [zákona č. 101/2000 Sb.] bez souhlasu subjektu údajů je založena na současném splnění dvou podmínek a výsledkem jejich následného posouzení. První podmínkou je, že takové zpracování je nezbytné pro ochranu práv správce, příjemce nebo jiné dotčené osoby… Druhou podmínkou je, že zpracování nezasahuje nepřiměřeným způsobem do soukromí subjektu údajů. Posouzení váhy chráněného práva na straně správce a míry zásahu do soukromí subjektu údajů poté vede k závěru správce, zda lze osobní údaje na základě tohoto ustanovení zpracovávat bez souhlasu subjektu údajů."*[234] Novák ve svém komentáři popsal ustanovení přesněji, když správně neomezoval poměřování zájmu subjektu údajů jen na jeho právo na soukromí, ale na všechny jeho zájmy a základní práva.[235] Oprávněný zájem správce nebo třetí osoby může být obecně jakýkoli cíl nebo činnost, která je v souladu s právem, a pro jeho dosažení je dané zpracování osobních údajů nezbytné. Může jít například

234 POSPÍŠIL, Daniel. § 5 odst. 2 písm. e]. In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 145, Beckova edice komentované zákony.

235 NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017].

o zajištění zabezpečení majetku a zdraví,[236] výkon svobody projevu a práva na informace,[237] zpracování osobních údajů za účelem zajištění kybernetické bezpečnosti,[238] opětovné užití informací veřejného sektoru[239] nebo zpracování osobních údajů za účelem marketingu.[240] WP 29 ve svém stanovisku k pojmu oprávněného zájmu navíc uvádí, že oprávněný zájem musí být jasně formulovaný a nesmí být spekulativní.[241] Právní titul oprávněného zájmu je tak velice flexibilní v tom, že umožňuje zpracovávat osobní údaje bez souhlasu subjektu údajů v celé řadě situací za předpokladu, že dané zpracování nezasahuje nepřiměřeně do práv a zájmů subjektu údajů. Vzhledem k tomu je možné vhodným nastavením procesů probíhajícího zpracování, jako jsou technické a organizační prostředky ochrany, pseudonymizace a podobně, přispět k tomu, aby se hodnocení v probíhajícím testu proporcionality

236 Viz například rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb.NSS, ve kterém soud dovodil, že zpracování osobních údajů prostřednictvím CCTV kamery umístěné na rodinném domě bylo v daném případě v oprávněném zájmu správce údajů. Zpracování ovšem musí úzce odpovídat stanovenému účelu. Dle usnesení Ústavního soudu ze dne 5. 9. 2017 sp. zn III.ÚS 3565/16, ve kterém soud potvrdil rozhodnutí Nejvyššího správního soudu ze dne 8. 6. 2016 č. j. 3 As 118/2015-34 tak není součástí účelu zpracování „zajištění ochrany majetku" umístění nahraného videa zobrazujícího krádež na internet, protože není možné nahrazovat činnost orgánů činných v trestním řízení.

237 Tímto důvodem podložil SDEU zpracování internetového vyhledávače v rozsudku ze dne 13. 5. 2014 ve věci *Google Spain,* C-131/12, připouští ho rovněž WP 29 ve svém stanovisku č. 6/2014, k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES, s. 25. Z uvedeného stanoviska mimo jiné vyplývá, že právní úprava zákona č. 110/2019 Sb., která nabízí nový právní titul pro zpracování údajů za účelem výkonu novinářské profese, je nadbytečná, protože by toto zpracování mohlo být dostatečně pokryto právě právním titulem oprávněného zájmu.

238 K tomu více viz HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, roč. 6, č. 12; SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security,* 2017, roč. 2017, č. 1.

239 Takovým příkladem je aplikace Hlídač státu, ve které jsou za účelem zajištění transparentnosti a veřejné kontroly kombinována data z registru smluv, obchodního rejstříku, transparentních účtů politických stran a hnutí a další datové zdroje. Viz MÍŠEK, Jakub. *Právní aspekty otevřených dat*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019, s. 125.

240 Tento účel je výrazněji přítomný až díky Obecnému nařízení, které zmínku o možnosti aplikace zpracování za oprávněným zájmem správce výslovně obsahuje v bodě 47 odůvodnění. Konkrétní instanci principu, na kterém tento právní titul spočívá, můžeme vidět například v umožnění zpracování kontaktních osobních údajů k zasílání obchodních sdělení, jestliže spotřebitel využil služby daného obchodníka a aktivně neuvedl, že si tato sdělení odebírat nepřeje. Viz čl. 13 směrnice 2002/58/ES a jeho provedené v podobě § 7 zákona č. 480/2004 Sb.

241 Stanovisko č. 6/2014, k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES, s. 25.

naklonilo spíše na stranu správce údajů.[242] Na druhou stranu je třeba zdůraznit, že na straně subjektu údajů nedochází k poměřování jen jeho základních práv, ale rovněž jeho zájmů. Míra ochrany je tak v tomto směru silnější.

Institut právního titulu ke zpracování za účelem oprávněného zájmu správce tak zcela odpovídá a přispívá k výše zmiňovanému charakteru celé právní úpravy ochrany osobních údajů, kterým je obecné umožnění zpracování za předpokladu, že probíhá korektně a nezasahuje nepřiměřeně do práv a zájmů subjektu údajů.[243] V tom je možné vidět zásadní rozdíl od režimu ochrany soukromí, který spočívá na vyloučení jakéhokoli zásahu do tohoto práva, s výhradou souhlasu nebo zákonné výjimky. Vlivem chybného rozhodnutí českého zákonodárce, který převzal textaci ustanovení upravujícího právní tituly ke zpracování v zákoně 101/2000 Sb. z občanského zákoníku č. 40/1964 Sb., došlo k nešťastné akcentaci souhlasu v právní úpravě ochrany osobních údajů. Důsledkem toho došlo ke značnému zmatení v odborné[244] i laické[245] debatě, která v konečném důsledku vyústila k devalvaci hodnoty souhlasu se zpracováním a až fetišizaci souhlasu.[246] Souhlas

242 Detailněji je problematice hodnocení testu proporcionality v případě oprávněného zájmu věnována část 5.4 této publikace.

243 Tomuto názoru odpovídají rovněž závěry rozsudku Soudního dvora Evropské unie ze dne 24. 11. 2011 ve věci *ASNEF*, C-468/10, ve kterém SDEU uvedl, že právní titul zpracování za oprávněnými zájmy správce nesmí být legislativně omezen, a že čl. 7 písm. f) směrnice 95/46/ES, který tento právní titul upravoval, měl přímý účinek do národního práva.

244 Uvedené je možné demonstrovat například dobovým komentářem (KINDL, Milan. K „novátorským" důsledkům zákona o ochraně osobních údajů. *Právní rozhledy*, 2001, roč. 9, č. 2) případně soudními rozhodnutími, které uvádějí souhlas jako základní právní titul se zpracováním a ostatní právní tituly jako výjimky z obecného pravidla (např. rozsudek Nejvyššího správního soudu ze dne 12. 2. 2009, č. j. 9 As 34/2008-68, č. 1844/2009 Sb.NSS, rozsudek Nejvyššího správního soudu ze dne 28. 6. 2013, č. j. 5 As 1/2011-156, nebo bod 22 rozsudku Nejvyššího správního soudu ze dne 13. 8. 2014, č. j. 1 As 78/2014-41, č. 3127/2014 Sb.NSS).

245 Jde o situace, kdy správce údajů požadoval použití souhlasu se zpracováním do dokumentu, i když od toho byl zrazován s tím, že to není třeba. Argument „pro jistotu to tam dáme" byl mnohdy silnější (osobní zkušenost autora).

246 Nejde však jen o české právní prostředí. Na problematickou aplikaci souhlasu se zpracováním upozorňuje například Borgesius (BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network, 2013, s. 38 a násl [cit. 30. 6. 2020]; Informed consent: We can do better to defend privacy. *IEEE Security and Privacy* [online]. 2015, roč. 13, č. 2, s. 104–105; Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law*. 2015, roč. 5, č. 3, s. 170–171). Systematicky více pojednáno v MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9.

se zpracováním osobních údajů je vhodné jako právní titul používat, až když není žádný jiný právní titul k dispozici, tedy pouze tehdy, když by jinak zpracování osobních údajů nebylo vzhledem k nepřiměřenosti legitimní, protože by neobstálo v interním testu proporcionality právního titulu oprávněného zájmu.[247] Jinými slovy, pokud je zpracování osobních údajů vzhledem ke stanovenému účelu oprávněné a přiměřené, tedy pokud jím není zasahováno do práv a zájmů subjektu údajů, souhlasu obvykle není třeba.[248]

Jako příklad dobře argumentovaného soudního rozhodnutí, ve kterém soud dospěl k závěru, že správce údajů může v určitých situacích provádět zpracování bez souhlasu subjektů údajů, je rozsudek NSS ve věci *Ryneš*.[249] V dané kauze šlo o zpracování osobních údajů prováděné za účelem ochrany zdraví a majetku správce, který byl již několikrát vystaven fyzickým útokům. Pan Ryneš umístil na svůj dům bezpečnostní kameru s uzavřenou smyčkou. Kamera částečně zabírala veřejný prostor za hranicí pozemku ve vlastnictví správce údajů, konkrétně veřejnou ulici a vchod do protějšího domu. Vzhledem k tomu docházelo ke zpracování osobních údajů lidí pohybujících se v tomto veřejném prostranství. Záznam, který odhalil útočníky, předal správce Policii ČR. ÚOOÚ udělil správci pokutu za protiprávní zpracování osobních údajů, protože k němu mělo docházet bez řádného právního titulu.[250] Dozorový orgán došel při hodnocení oprávněnosti zájmu správce k závěru, že sledování veřejného prostoru a vchodu do protějšího domu

247 Gutwirth se odkazuje na francouzskou a belgickou tradici, ve které před účinností směrnice 95/46/ES institut souhlasu nebyl vůbec přítomen, a jde v tomto směru úvah až k závěru, že zpracování osobních údajů, které probíhá na základě souhlasu, je v jádru nelegitimní, protože pokud by bylo legitimní, nebylo by třeba souhlasu (GUTWIRTH, Serge. *Short statement about the role of consent in the European data protection directive* [online]. Brusel: Bepress, 2012 [cit. 30. 6. 2020]). Tento přístup je myslím příliš extrémní. Pokud je souhlas udělen uvnitř systému ochrany osobních údajů v souladu s jeho požadavky na kvalitu souhlasu, jde o zcela legitimní zpracování a to zejména proto, že správce údajů musí plnit všechny své povinnosti. O nelegitimním zpracování by mohla být řeč až v teoretickém případě, kdy by byl souhlas udělen mimo režim ochrany osobních údajů, tedy například jako okolnost vylučující protiprávnost v kontextu § 30 zákona č. 40/2009 Sb., trestní zákoník.

248 Viz BROWNSWORD, Roger. Consent in Data Protection Law. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 91.

249 Rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb. NSS.

250 Ibid., bod 3 rozsudku. Byl to hlavní z důvodů udělení pokuty vedle zanedbání informační a registrační povinnosti.

není přiměřené, protože *„nelze připustit, aby si kdokoliv nepřetržitě pořizoval záznamy z veřejné ulice a současně zaznamenával pohyb sousedů“*.[251] Zároveň dodal, že by rovnováha zájmů byla nastolena a zásah by byl přiměřený, pokud by správce *„sklopil kameru tak, aby záběr z ní nezabíral podstatnou část veřejné ulice a především prostor u vchodu do cizích domů“*.[252] NSS tento výklad ÚOOÚ odmítl s tím, že v daném případě interní test proporcionality dopadl ve prospěch správce údajů, zejména vzhledem ke konkrétním událostem v podobě opakovaných útoků, předcházejícím zpracování údajů.[253] NSS tak v uvedeném případě potvrdil, že správce údaje zpracovávat může, pokud tak činí korektně a přiměřeně danému případu.

Závěrem této části je třeba zdůraznit, že fakt, že většina právních titulů umožňuje zpracování osobních údajů bez ohledu na vůli subjektu údajů, neznamená, že by subjekt údajů nebyl chráněn nebo se nemohl o své právo na ochranu osobních údajů zasadit. Z jedné strany je totiž chráněn poměrně přísnou zásadou účelovým omezením zpracování a na ni navazující nutností zvolit správný právní titul, na straně druhé je to pak série konkrétních subjektivních práv, které mu Obecné nařízení přiznává a pomocí kterých může zajistit své informační sebeurčení.[254]

2.3 Práva subjektu údajů jako pojistka před zneužitím osobních údajů

2.3.1 Role práv subjektů v systému ochrany osobních údajů

Systém ochrany osobních údajů spočívá na základech práva na informační sebeurčení, které je projevem autonomie jedince a zároveň nástrojem k jejímu zaručení. Může proto na první pohled vypadat zvláštně, že institut

251 Ibid., bod 13 rozsudku.

252 Ibid.

253 Ibid., bod 84 rozsudku. NSS doslova uvádí: *„Vysvětlení stěžovatele, proč kamera zabírala ulici i vchod do protějšího domu, je přitom naprosto logické: pokud by byla kamera ‚sklopena‘ a zabírala například jen obvodovou zeď stěžovatelova domu, funkce kamery by se míjela svým účinkem, neboť by potencionálního útočníka nikdy nezaznamenala. Pokud žalovaný ‚radí‘ stěžovateli opak, je to smutný důkaz toho, že je naprosto odtržen od reálií běžného života.“*

254 Právům subjektu údajů jako východiskům pro systém zpracování je věnována část 2.3 této publikace.

souhlasu, tedy základní nástroj, který se obvykle s autonomií pojí,[255] nehraje v konečném důsledku v systému ochrany osobních údajů příliš velkou roli. To je způsobeno výše pojednanou pragmatickou nezbytností zpracování osobních údajů, a tedy přítomností dalších právních titulů ke zpracování osobních údajů, které souhlas ve většině případů zastoupí. Je však důležité zdůraznit, že souhlasem, případně volbou smluvního partnera, možnosti projevu autonomie subjektu údajů končit nemohou. Krom pragmatického faktu, že v řadě případů souhlas není třeba (což by znamenalo vyloučení aspektu autonomie subjektu údajů z většiny zpracování), je nutné zahrnout aspekt plynoucího času. Autonomie subjektu údajů nemůže být omezena pouze na okamžik poskytnutí souhlasu. Naopak, je nezbytné zajistit možnost účasti subjektu údajů po celou dobu probíhajícího zpracování. Tento cíl naplňují pozitivně formulovaná subjektivní práva svědčící subjektům údajů. Představují totiž nástroj umožňující dohled a kontrolu nad probíhajícím zpracováním osobních údajů. V tomto směru je proto možné upozornit na další významný rozdíl, který spočívá mezi režimy ochrany soukromí a ochrany osobních údajů. Zatímco ochrana soukromí funguje jako „neprůhledná clona" a zajišťuje oblasti, v nichž je vyloučen zásah z venčí (komunikace, domov a další soukromé prostory, rodinný život a další),[256] systém ochrany osobních údajů naopak cílí na zaručení transparentnosti procesů

255 Viz v kontextu osobních údajů například KOSTA, Eleni. *Consent in European data protection law*. Leiden: Martinus Nijhoff Publishers, 2013, s. 130 a násl.; V češtině dále viz KRAUSOVÁ, Alžběta. Zásada autonomie v ochraně soukromí: možnosti a limity v rozhodování o vlastních biometrických údajích. *Právní rozhledy*, 2018, roč. 26, č. 6, s. 191.

256 Viz HERT, Paul de a Serge GUTWIRTH. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: CLAES, Erik, Antony DUFF a Serge GUTWIRTH (eds.). *Privacy and the criminal law*. Antwerp: Intersentia, 2006, s. 71–72; Zanfir uvádí, že právní úprava práva na ochranu soukromí pracuje s „nástroji neprůhlednosti" (ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 244). Právo na soukromí ve svém základu totiž akcent na transparentnost nemělo. Umožnění přístupu k informacím o soukromí nalezneme až v novější judikatuře ESLP, který v duchu otevřeného přístupu k výkladu pojmu soukromý život dovodil v případu *Gaskin vs. Spojené království*, že neposkytnutím záznamů z doby, kdy byl stěžovatel umístěn v ústavní výchově, bylo zasaženo do jeho práva na ochranu soukromého života garantovaného čl. 8 Úmluvy (viz rozsudek Evropského soudu pro lidská práva ze dne 7. 7. 1989 ve věci *Gaskin vs. Spojené království*, stížnost č. 10454/83); ...

zpracování údajů a tím pádem umožnění kontroly správce údajů ze strany subjektu.[257] Této transparentnosti je pak dosaženo zejména pozitivně formulovanými právy subjektu údajů. Obdobně situaci popisuje Bygrave, když uvádí, že možnost subjektu údajů zapojit se do procesu zpracování a mít na něj vliv je jednou z ústředních zásad ochrany osobních údajů.[258]

Zastavím se ještě u institutu souhlasu se zpracováním, protože z kontextu předchozí části této kapitoly by se mohlo zdát, že z nižšího akcentu na souhlas se zpracováním by mohli těžit výhradně správci osobních údajů. Subjekt údajů a jeho práva tímto posunem ve výkladu však rovněž nijak neutrpí. Naopak, akcent na práva (oproti akcentu na souhlas) postavení subjektu údajů a jeho ochranu fakticky posílí, a to i v případech, kdy je souhlas aplikován jako právní titul pro zpracování. To je důležité vzhledem k tomu, že ačkoli je aplikace souhlasu omezena na případy, kdy není možné využít jiných právních titulů, stále jde o množství zpracování, která navíc mohou být svým charakterem velmi intruzivní do práv a zájmů subjektů údajů, zejména jde-li například o zpracování za účelem cíleného marketingu nebo využívání služeb sociálních sítí.

...

Neposkytnutí informace o soukromí však neznamená zásah ve smyslu čl. 8 vždy, jak dokládá starší rozhodnutí ESLP ve věci *Leander* (rozsudek Evropského soudu pro lidská práva ze dne 26. 3. 1987 ve věci *Leander vs. Švédsko*, stížnost č. 9248/81). Více k judikatuře ESLP vztahující se k poskytování informací o soukromí viz BYGRAVE, Lee A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology,* 1998, roč. 6, č. 3, s. 277–283; SLOOT, Bart van der. Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of Big Data. *Utrecht Journal of International and European Law,* 2015, roč. 31, č. 80, s. 34; a NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017].

257 Viz HERT, Paul de a Serge GUTWIRTH. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: CLAES, Erik, Antony DUFF a Serge GUTWIRTH (eds.). *Privacy and the criminal law*. Antwerp: Intersentia, 2006, s. 77–78; Shodně dále též LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 595; a ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 245.

258 BYGRAVE, Lee A. *Data privacy law: an international perspective*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2014, s. 158.

Pokud bychom přistoupili k souhlasu se zpracováním jako k hlavnímu nástroji pro zajištění autonomie subjektu údajů,[259] narazíme na tři zásadní problémy. Prvním je zahlcení subjektů žádostmi o souhlas se zpracováním. Negativní efekt přebujelého množství žádostí o souhlas byl již dobře popsán. Když je uživatel vystaven velkému množství žádostí o souhlas, automaticky je začne přijímat. Je „vytrénován" k bezmyšlenkovitému udělování souhlasu.[260] Lidé klikají na tlačítko „souhlasím", aniž by si dostatečně zjistili, s čím vlastně souhlasí a v důsledku tak mohou bezmyšlenkovitě odsouhlasit i zpracování, které je pro ně nevýhodné nebo nebezpečné.[261]

S tím souvisí problém druhý, kterým je faktická nesplnitelnost požadavků kladených na platný souhlas. Dle čl. 4 odst. 11 Obecného nařízení musí být souhlas svobodný, konkrétní, informovaný a jednoznačný.[262] Z hlediska faktické proveditelnosti je problematický zejména požadavek na informovanost subjektu údajů. Správci údajů formálně naplňují svoji povinnost informovat před udělením souhlasu subjekt o chystaném zpracování, ke skutečné informovanosti subjektů údajů však jen zřídka kdy dojde vzhledem k několika překážkám, které Solove označuje jako kognitivní problémy.[263] Vzhledem k ohromnému množství požadovaných souhlasů lidé informace

259 Tím mám na mysli situaci, kdy by byl kladen větší důraz na souhlas se zpracováním oproti jiným právním titulům, tedy na situaci, která byla minimálně v českém donedávna poměrně běžná. Viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 67.

260 Viz BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network, 2013, s. 42 [cit. 30. 6. 2020].

261 To však není problém jen oblasti ochrany osobních údajů, na což upozorňují Beyleveld s Brownswordem, když uvádějí, že jde o běžný negativní jev, který se vyskytuje takřka ve všech oblastech, které spoléhají na institut souhlasu (viz BEYLEVELD, Deryck. *Consent in the Law*. Oxford: Hart Publishing, 2007, s. 63).

262 Další podmínky jsou specifikovány v čl. 7 Obecného nařízení. Souhlasu a jeho podmínkám je pak věnováno stanovisko a pokyny WP 29 (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 15/2011 k definici souhlasu. *Evropská komise* [online]. 13. 7. 2011, 38 s. [cit. 30. 6. 2020]; a PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Pokyny pro souhlas podle nařízení 2016/679. *Evropská komise* [online]. 28. 11. 2017, v revidovaném znění ze dne 10. 4. 2018, č. WP259rev.01, 32 s. [cit. 30. 6. 2020]); Více rovněž NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Správní právo*, 2011, roč. 44, č. 14.

263 SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2012, roč. 126, č. 7, s. 1888.

o zpracování nečtou.[264] Pokud je čtou, nerozumí jim, protože jsou psány složitým právnickým jazykem.[265] Pokud je čtou a rozumí jim, postrádají často dostatečné znalosti, aby si pod formulovanými pravidly představili konkrétní dopady na svoji situaci a dokázali se následně informovaně rozhodnout.[266] Poslední překážkou je, že i pokud je čtou, rozumí jim a dokáží se informovaně rozhodnout, často tak neučiní vzhledem k psychologickým a behaviorálním překážkám, které se při rozhodování projevují.[267] Celý problém je tak možné dle Soloveho přirovnat k situaci, ve které se nachází hrdina Kafkovy povídky *Před zákonem*. Ten touží projít dveřmi, které jsou však chráněny dveřníkem, a za nimi jsou jen další dveře s dalšími dveřníky, přičemž každý další je mocnější než ten předchozí.[268] Vzhledem k těmto překážkám stojícím v cestě udělení opravdu informovaného souhlasu je souhlas

264 Borgesius ve svém starším článku dovozoval, že průměrný Američan by musel strávit čtením 244 hodin ročně, aby zvládl zpracovat množství dokumentů informujících o podmínkách ochrany soukromí (viz BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network, 2013, s. 32 [cit. 30. 6. 2020]). Obdobně viz LESSIG, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006, s. 226.

265 Srozumitelnost informačních dokumentů je v reakci na tento fakt výslovně vyžadována čl. 12 Obecného nařízení. Bod 58 odůvodnění doslova uvádí: *„Zásada transparentnosti vyžaduje, aby všechny informace určené veřejnosti nebo subjektu údajů byly stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech navíc i vizualizace."* Shodně formuluje požadavky rovněž WP 29 (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Pokyny pro souhlas podle nařízení 2016/679. *Evropská komise* [online]. 28. 11. 2017, v revidovaném znění ze dne 10. 4. 2018, č. WP259rev.01, s. 14 [cit. 30. 6. 2020]).

266 Solove uvádí jako příklad průzkumy, ve kterých vysoké procento lidí nebylo schopno správně zodpovědět jednoduché otázky související s dopady, které mohou mít nabízené produkty a služby na jejich soukromí (viz SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2012, roč. 126, č. 7, s. 1886).

267 Borgesius je velmi dobře shrnuje ve své studii věnované souhlasu a jeho problémům. Lidé například obvykle trpí krátkozrakostí, takže upřednostňují okamžitý bonus před zamezením větší ztráty v delším časovém úseku. Další častou chybou je setrvávání na *statu quo*, pokud je tedy v základu služby nastaveno poskytování dat, je pravděpodobné, že to uživatel nezmění (z toho důvodu vyžaduje Obecné nařízení pro platnost souhlasu jeho jednoznačnost, tedy čistý opt-in režim). Více viz BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network, 2013, s. 38–43 [cit. 30. 6. 2020].

268 SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2012, roč. 126, č. 7, s. 1888.

často platně udělen jen formálně, nikoli však materiálně a tvoří tak fíkový list pochybnému zpracování.[269] Ačkoli některé uvedené překážky možnosti efektivního informování subjektu údajů již nejsou tak palčivé jako v době, kdy Solove a Borgesius psali své texty,[270] stále jsou přítomné a představují zásadní problémy fungování institutu souhlasu.

Konečně, třetí zásadní problém souhlasu vyvěrá z časové fixace zpracování osobních údajů k okamžiku udělení souhlasu a pomíjí následnou dynamiku celého procesu zpracování. Souhlas se zpracováním nesmí představovat „zelenou kartu", která by bez dalšího udělila správci pravomoc zpracovávat osobní údaje až do doby, než je případně souhlas odvolán. Význam osobních údajů se může v průběhu plynutí času měnit.[271] Údaje, které při počátku zpracování vypadaly neškodně, se vlivem dalších událostí mohou stát problematickými. Solove má pravdu, když říká, že v době udělení souhlasu není v lidských silách dohlédnout, jaké důsledky může zpracování konkrétních osobních údajů nést.[272]

Předchozí odstavce ukazují, že souhlas se zpracováním osobních údajů je ve svém jádru velice zatížen zásadními až nepřekonatelnými problémy. Vzhledem k tomu není možné o něm uvažovat jako o hlavním nástroji autonomie subjektu údajů. Jeho akcentace by naopak vedla ke zhoršení postavení subjektu údajů. Je proto možné souhlasit s Gutwirthem, když říká, že systém ochrany osobních údajů není (a nemůže být) vystaven na principu souhlasu.[273] Subjekt údajů musí mít možnost kontrolovat probíhající zpracování osobních údajů. Je nezbytné, aby měl k dispozici účinný nástroj, který mu umožní

269 Více viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 45–46; Můžeme zde vidět určitou paralelu s problémem promulgace právních předpisů jako předpokladu pro zásadu „neznalost práva neomlouvá", byť nikdo neočekává, že existuje člověk, který by reálně přečetl a znal všechny předpisy. Srovnej POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 208, Téma.

270 Zejména vzhledem k výše uvedené reakci evropského zákonodárce, který se novými pravidly v Obecném nařízení pokusil aspekt srozumitelnosti cíleně adresovat, a vzhledem k celospolečenské debatě, která se v souvislosti s přijetím Obecného nařízení vedla a rozšířila povědomí o ochraně osobních údajů.

271 Jako jeden ze základních problémů uvádí statičnost zpracování rovněž Polčák (POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 8 [cit. 30. 6. 2020].

272 Viz SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2012, roč. 126, č. 7, s. 1889–1893.

273 GUTWIRTH, Serge. *Short statement about the role of consent in the European data protection directive* [online]. Brusel: Bepress. 2012 [cit. 30. 6. 2020].

se do již probíhajícího zpracování aktivně zapojit. Právě tuto roli hrají pozitivně formulovaná subjektivní práva vztahující se ke zpracování, která subjektu údajů (pokud o to bude mít zájem) umožňují se o zpracování efektivně informovat a zasáhnout, pokud se bude domnívat, že probíhá protiprávně. Je zásadní, aby tak mohl činit i v době, kdy zpracování již probíhá, a to s ohledem na nové skutečnosti, které v době jeho počátku nebyly známé. Subjektivní práva tak mohou představovat účinný nástroj k výkonu práva na informační sebeurčení subjektu údajů a tím i jeho autonomie. Neznamená to však, že institut souhlasu nehraje vůbec žádnou roli. Je nezbytný pro případy, kdy není možné aplikovat jiné právní tituly a je opravdu jen na rozhodnutí subjektu údajů, zda dovolí zpracování. Zdrženlivé vyžadování souhlasu jen v nezbytných případech může velmi prospět právní jistotě subjektů údajů, protože přestane být věcí běžnou, ale stane se spíše výjimečnou. Tento fakt může zvýšit pozornost subjektu údajů a lépe si tak promyslet, zda opravdu chce souhlas udělit.[274] Subjektivní práva jsou pak nezbytnou navazující součástí zajištění autonomie subjektu údajů a rovnováhy mezi ním a správcem údajů, a to bez ohledu na to, který právní titul je nakonec opravdu použit.

V kontextu systému ochrany osobních údajů byla pozitivně formulovaná práva subjektu údajů přítomná již v nejstarších doporučeních a legislativních dokumentech, postupem času se však formulace konkrétních práv významně rozšiřovala. Odst. 13 doporučení OECD upravoval *„princip zapojení“*,[275] dle kterého má mít každý právo být informován o zpracování svých osobních údajů,[276] mít k nim přístup a mít možnost napadnout oprávněnost a správnost probíhajícího zpracování s tím, že pokud by taková stížnost byla úspěšná, musí být osobní údaje opraveny, nebo smazány. Tento odstavec rovněž zakládal povinnost správce údajů řádně odůvodnit případy, ve kterých by odmítl subjekt údajů informovat nebo mu data neposkytl. Úmluva 108

274 MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 49–50.

275 Participation principle, viz odst. 13 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online].

276 Ku příkladu jedna z větších sankcí, které byly doposud za účinnosti Obecného nařízení uloženy, byla pokuta ve výši 943 000 PLN (cca 220 000 €), udělená polským národním dozorovým úřadem za nesplnění informační povinnosti správce. Viz First fine imposed by the President of the Personal Data Protection Office. *Evropský inspektor ochrany osobních údajů* [online]. EDPB, 2019 [cit. 30. 6. 2020].

upravuje práva subjektů údajů v článku 8 zvaném *„Dodatečné záruky pro subjekt údajů"* v zásadě v totožném rozsahu.[277] Zároveň však obsahuje ustanovení umožňující výjimku z jejich aplikace v případech, kdy je to nezbytné vzhledem k ochraně subjektu údajů, práv a svobod jiných osob a ochrany bezpečnosti státu, veřejné bezpečnosti, měnových zájmů státu nebo potírání trestné činnosti.[278] Směrnice 95/46/ES vedle práva na informace o probíhajícím zpracování a správci údajů[279] a práva na přístup[280] a na námitku proti zpracování[281] zakotvila nově právo *„nestat se subjektem rozhodnutí, které vůči nim zakládá právní účinky nebo které se jich významně dotýká, přijatého výlučně na základě automatizovaného zpracování údajů"*.[282] Evropský zákonodárce tímto článkem adresoval fakt, že rozhodování o právech a povinnostech založené na automatizovaném zpracování osobních údajů, zejména je-li prováděno netransparentně,[283] může představovat zásadní zásah do práv a zájmů subjektů údajů, například vzhledem k vysokému riziku diskriminace.[284] Postupný nárůst počtu pozitivně formulovaných subjektivních práv subjektů údajů završilo Obecné nařízení, které k právům známým již z doby směrnice (byť přesněji vyjádřeným a věcně lehce rozšířeným)[285] přidalo několik práv nových v podobě samostatně stojícího práva na opravu,[286] práva na výmaz – známého spíše

277 Viz sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat, čl. 8. Doslova tento článek garantuje právo zjistit informace o probíhajícím zpracování a správci údajů, právo na přístup k těmto údajům, právo na jejich opravu nebo vymazání a právo na opravný prostředek pro případ nevyhovění žádosti při výkonu výše uvedených práv.

278 Ibid., čl. 9.

279 Čl. 10 a 11 směrnice 95/46/ES. Srovnej např. rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci *Bara*, C-201/14, a další.

280 Čl. 12 směrnice 95/46/ES.

281 Čl. 14 směrnice 95/46/ES.

282 Čl. 15 směrnice 95/46/ES.

283 Viz CITRON, Danielle Keats a Frank PASQUALE. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, 2014, roč. 89, č. 1, s. 10–11; ZARSKY, Tal. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Science Technology and Human Values* [online]. 2016, roč. 41, č. 1, s. 127–129.

284 Viz KAMIRAN, Faisal, Indré ŽLIOBAITE a Toon CALDERS. Quantifying explainable discrimination and removing illegal discrimination in automated decision making. *Knowledge and Information Systems* [online]. 2016, roč. 35, č. 3.

285 Právo na informace o zpracování nalezneme v čl. 13 a 14, právo na přístup k údajům v čl. 15, právo vznést námitku v čl. 21 a právo nebýt předmětem rozhodování založeného výhradně na automatizovaném zpracování v čl. 22.

286 Viz čl. 16 Obecného nařízení.

pod populárním označením „právo být zapomenut“,[287] jemu příbuzné právo na omezení zpracování[288] a zcela nové právo na přenositelnost údajů.[289] Cílem těchto nových práv pak bylo prohloubení možností subjektů údajů vykonávat kontrolu nad probíhajícím zpracováním a jeho osobními údaji a tím i možnost zajištění autonomie a výkonu práva na informační sebeurčení.[290]

Vazbu mezi subjektivními právy a autonomií subjektu údajů identifikoval Paul Bernal, který ve své monografii navrhuje zajištění efektivního výkonu ochrany informačního soukromí uživatelů internetu prostřednictvím tří subjektivních informačních práv, které jim mají svědčit. Je to „právo pohybovat se na internetu v soukromí“, které se vztahuje k fázi sběru osobních údajů, „právo dohlížet na dohlížející“ pro fázi samotného zpracování a využití údajů, a „právo na výmaz“ pro fázi uložení údajů.[291] Bernal je chápe jako

287 Viz čl. 17 Obecného nařízení. Tomuto právu je věnováno velké množství textů, příkladně je možné uvést AUSLOOS, Jef. The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review* [online]. 2012, roč. 28, č. 2; BARTOLINI, Cesare a Lawrence SIRY. The right to be forgotten in the light of the consent of the data subject. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2; KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law* [online]. Dordrecht: Springer Netherlands, 2015, Law, Governance and Technology Series, 20 [cit. 27. 10. 2016]; ZANFIR, Gabriela. Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law*. Dordrecht: Springer Netherlands, 2015; MIŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie*, Česká advokátní komora, 2015, roč. 2015, č. 1–2.

288 Čl. 18 Obecného nařízení.

289 Čl. 20 Obecného nařízení. Dle bodu 68 odůvodnění Obecného nařízení si toto právo klade za cíl zajištění subjektu údajů větší kontroly nad zpracováním osobních údajů tak, že mu usnadní možnost přechodu k jinému poskytovateli služeb a všechna svá data si bude moci vzít s sebou. Jak však uvádí například Van der Auwermeulen, tento koncept rozhodně není bezrozporný a přináší řadu výzev v podobě faktické efektivity tohoto práva, kybernetické bezpečnosti nebo práv duševního vlastnictví (viz AUWERMEULEN, Barbara Van der. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law & Security Review* [online]. 2017, roč. 33, č. 1, s. 60). Hlavním problémem však zůstává, že doposud není jasné, jak široká aplikace tohoto práva má být, viz HERT, Paul de et al. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 199–200.

290 Srovnej ZANFIR, Gabriela. The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law; Oxford* [online]. 2012, roč. 2, č. 3, s. 155.

291 Bernal je nazývá „a right to roam the internet with privacy“, „a right to monitor the monitors“ a „a right to delete“, viz BERNAL, Paul. *Internet privacy rights: rights to protect autonomy*. Cambridge: Cambridge, England; New York: Cambridge University Press, 2014, s. 207, Cambridge Intellectual Property and Information Law.

vzájemně provázané nástroje,[292] které společně mají za cíl zajistit informační autonomii jedince při pohybu v kyberprostoru a ochránit ho před zásahem do soukromí. Svůj koncept označuje jako *„autonomy by design"* a vysvětluje ho následovně: *„What suits the individual? Knowledge, understanding and control, which means that the individual has to be able to know what data is held, understand why it is held and how it is used, and then be able to control: controlling what is gathered (via the right to roam with privacy), controlling how it is used (via the right to monitor the monitors and collaborative consent)*[293] *and controlling what is held (via the right to delete)."*[294] Bernalův přístup k autonomii subjektu je vhodný. Neomezuje totiž projev autonomie vůle na jeden časový bod udělení souhlasu, ale respektuje dynamickou povahu probíhajícího procesu zpracování osobních údajů. Ačkoli to Bernal sám neučinil[295], je snadné provázat jeho tři práva informačního soukromí s pravidly obsaženými v Obecném nařízení. „Právo pohybovat se na internetu v soukromí" je vyjádřeno zásadou účelového omezení zpracování a na tento účel navazujícími právními tituly ke zpracování ve spojení se zásadami záměrné a standardní ochrany osobních údajů ve smyslu čl. 25 Obecného nařízení.[296] „Právo dohlížet na dohlížející" je vyjádřeno právem subjektu údajů na informace o zpracování, právem na přístup a právem

---

292 Označuje je jako „mechanistic rights", a v tomto směru je velice snadné najít paralelu s právy subjektu údajů. Viz Ibid., s. 212.

293 „Collaborative consent" je Bernalův koncept, kterým překonává zásadní slabinu souhlasu, kterou je časové zakotvení souhlasu k okamžiku jeho udělení. Výraz „collaborative" v jeho názvu označuje spolupráci mezi správcem a subjektem údajů, která probíhá po udělení souhlasu prostřednictvím možnosti kontrolovat, jak správce s údaji nakládá. Více viz BERNAL, Paul. Collaborative consent: Harnessing the strengths of the Internet for consent in the online environment. *International Review of Law, Computers & Technology* [online]. 2010, roč. 24, č. 3.

294 BERNAL, Paul. *Internet privacy rights: rights to protect autonomy*. Cambridge: Cambridge, England; New York: Cambridge University Press, 2014, s. 216, Cambridge Intellectual Property and Information Law.

295 Je tomu tak zřejmě zejména vzhledem k datu vydání jeho práce a vzhledem k tomu, že východiskem Bernalova textu není ochrana osobních údajů, ale soukromí v kyberprostoru (tedy informační soukromí).

296 Porovnání s Bernalovým právem pohybovat se na internetu v soukromí a čl. 25 je možné. Bernal při vysvětlení svého konceptu uvádí: *„the default position is that data is not gathered for storage and use unless an express choice has been made, for example by logging in to a premium, specified service"* (Ibid., s. 207). Čl. 25 Obecného nařízení je praktickým provedením zásady minimalizace a jeho cílem je zajistit, aby probíhající zpracování bylo od počátku nastaveno tak, aby docházelo ke zpracování jen zcela nezbytných údajů. Bernalův přístup je však o něco přísnější, protože zcela zakazuje jakýkoli sběr dat, zatímco systém ochrany osobních údajů ho umožňuje v přiměřené míře dané oprávněným zájmem správce.

na opravu;[297] koncept kolaborativního souhlasu pak nalezneme v kombinaci institutu souhlasu se zpracováním s navazujícími právy subjektu údajů. Konečně „právo na výmaz" najdeme v doslovné podobě v čl. 17 Obecného nařízení, úzce s ním však souvisí právo na omezení zpracování a právo vznést námitku. Jasnější a silnější vyjádření subjektivních pozitivních práv subjektů údajů v Obecném nařízení je prostředkem, který může vést k posílení subjektů vůči správcům a tím k možnosti vyrovnání pozice subjektu jako slabší strany (zejména vzhledem k informační a materiální nerovnosti[298]) a v konečném důsledku k již několikrát zmiňované autonomii.[299]

Je třeba zdůraznit, že práva subjektů údajů formulovaná předpisy ochrany osobních údajů mají v kontextu systému ochrany osobních údajů v zásadě instrumentální povahu a představují chráněné zájmy subjektů údajů. Jsou součástí širšího práva na ochranu osobních údajů, samostatně formulovaného a garantovaného na ústavní úrovni. Dílčí práva subjektů údajů však nejsou univerzální v tom smyslu, že by přesahovaly režim právní úpravy ochrany osobních údajů. Je tedy nezbytné je chápat a interpretovat vzhledem k účelu, jaký v systému ochrany osobních údajů plní. Tím je vyvažování informační a materiální asymetrie mezi subjekty a správci údajů. K tomu je nezbytná následná efektivní kontrola činnosti správce údajů, zajištění transparentnosti zpracování a umožnění aktivního zásahu ze strany subjektů práv. Vzhledem ke snaze zajistit co nejvyšší šance na účinné vymáhání těchto práv, zakotvil evropský zákonodárce v Obecném nařízení možnost jejich dodržování kontrolovat a vymáhat jak veřejnoprávní, tak soukromoprávní cestou. Minulá právní úprava v podobě směrnice 95/46/ES a zákona 101/2000 Sb. spoléhala zcela převážně na veřejnoprávní způsob kontroly a vymáhání povinností správců údajů prostřednictvím činnosti nezávislého

297 Důležitost práva na přístup zdůraznil rovněž SDEU v rozhodnutí ve věci *Rijkeboer* (viz rozsudek Evropského soudního dvora ze dne 7. 5. 2009 ve věci *Rijkeboer*, C-553/07).

298 Viz LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 592; GULIJK, Stephanie van a Joris HULSTJIN. Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach. *European Review of Private Law,* 2018, roč. 26, č. 5, s. 641–642.

299 Srovnej též WONG, Rebecca. Data protection: The future of privacy. *Computer Law & Security Review* [online]. 2011, roč. 27, č. 1, s. 56.

úřadu, kterým je v českém případě ÚOOÚ.[300] Domníval-li se subjekt údajů, že správce provádí zpracování protizákonně, nebo že je zasaženo do jeho práv, mohl se obrátit na ÚOOÚ prostřednictvím podnětu, jehož výsledkem byla kontrola a případně též správní trest. Mohl se ovšem obrátit rovněž na soud v rámci civilního řízení a požadovat například náhradu škody nebo újmy, která vznikla v důsledku porušení povinností správce. Tento způsob však nebyl primárně vyhledávaným.[301]

Institut práv subjektů údajů je v Obecném nařízení posílen oproti směrnici 95/46/ES díky jednoznačně formulovaným přímým nárokům subjektu údajů vůči správci nebo zpracovateli. Novým čl. 79 byla posílena soukromoprávní linie vedení obrany.[302] Subjekt údajů se může přímo obrátit na správce

300 Historicky, konkrétně do 25. 7. 2004, spadalo do kompetence ÚOOÚ rovněž rozhodování o individuálních nárocích subjektů údajů, jelikož § 21 zákona č. 101/2000 Sb. v prvním odstavci uváděl, že *„Pokud subjekt údajů zjistí, že došlo k porušení povinností správcem nebo zpracovatelem, má právo obrátit se na Úřad s žádostí o zajištění opatření k nápravě."* Krom nápravy protiprávního stavu mohl rovněž požadovat zaplacení peněžité náhrady. Toto ustanovení vyvolalo několik kompetenčních sporů mezi obecnými soudy a ÚOOÚ, jejichž výsledkem byla řada rozhodnutí určujících působnost rozhodovat spory mezi správcem a subjektem údajů právě do rukou ÚOOÚ (jde například o usnesení Nejvyššího správního soudu ze dne 6. 2. 2004, č. j. Konf 15/2003-24, č. 189/2004 Sb.NSS, nebo o usnesení Nejvyššího správního soudu ze dne 10. 3. 2004, č. j. Konf 11/2003-12, č. 426/2005 Sb.NSS). Tento stav změnila novela zákona 101/2000 Sb. provedená zákonem č. 439/2004 Sb., s účinnosti od 26. 7. 2004. Přechodové období nejistoty v interpretaci § 21 zákona 101/2000 Sb. a změnu v pravomoci ÚOOÚ dobře zmapoval Morávek (MORÁVEK, Jakub. Nad rozhodováním Nejvyššího správního soudu ohledně pravomocí Úřadu pro ochranu osobních údajů. *Právní rozhledy*, 2011, roč. 19, č. 9); Novější rozhodnutí Nejvyššího správního soudu potvrdila, že od novely zákonem 439/2004 Sb. již pravomoc rozhodovat soukromoprávní spory mezi subjektem a správcem údajů vyplývající z porušení povinností dle zákona 101/2000 Sb. nepřísluší ÚOOÚ, ale soudu (např. usnesení Nejvyššího správního soudu ze dne 24. 2. 2010, č. j. Konf 56/2009-7, č. 2274/2011 Sb.NSS, usnesení Nejvyššího správního soudu ze dne 17. 10. 2011, č. j. Konf 11/2011-6, č. 2500/2012 Sb.NSS a usnesení Nejvyššího správního soudu ze dne 4. 9. 2012, č. j. 1 As 93/2009-273, č. 2732/2013 Sb.NSS); Je proto s podivem, že i přes to, že jde o poměrně dlouho vyjasněné téma, stále se tento problém v rozhodování soudů objevuje (zejména v rozhodovací praxi obecných soudů), jak dokládá např. rozsudek Nejvyššího soudu ze dne 26. 2. 2019, sp. zn. 30 Cdo 2233/2017, v němž Nejvyšší soud s odkazem na rozhodovací praxi NSS opětovně potvrdil, že ÚOOÚ opravdu nemůže rozhodovat v soukromoprávních sporech.

301 Na tomto hodnocení se shodli panelisté workshopu INFORM den, konaném 6. 6. 2018 v Brně. Rád bych na tomto místě poděkoval za podnětnou diskuzi zejména Michalu Šalamounovi a Tomáši Rychlému.

302 Viz čl. 79 Obecného nařízení, jehož odst. 1 zní: *„Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením."*

nebo zpracovatele v případě, že se domnívá, že došlo k porušení práv garantovaných Obecným nařízením a pokud mu nevyhoví, může se domáhat splnění povinnosti nebo náhrady vzniklé škody nebo újmy. Vedle toho však může stále podat podnět na ÚOOÚ, který má možnost nedostatky ve zpracování údajů řešit po správněprávní linii. Práva subjektu údajů v kontextu zpracování osobních údajů tak požívají dvojí ochrany. Při řešení sporu soukromoprávní cestou bude hodnoceno konkrétní zpracování osobních údajů daného subjektu a pokud při něm došlo k pochybení, subjekt se může domáhat individuální náhrady. V případě správně právní cesty bude ÚOOÚ zkoumat (pravděpodobně na základě podnětu), zda má správce nastavené své zpracování tak, aby k porušování práv subjektů údajů nedocházelo a umožnil naopak jejich snadný výkon.

2.3.2 Problémy aplikace práv subjektu údajů

Z dosavadního výkladu vyplývá naprosto klíčová pozice práv subjektu údajů v systému ochrany osobních údajů. Proti nim je možné vznést dvě tradiční námitky, které je však nutné ovšem nakonec odmítnout. První spočívá v argumentaci, že osobní údaje jsou *de facto* komoditou, se kterou je možné obchodovat, a pokud svá data „prodám", nemohu k nim již dále mít žádná práva. Otázka, se kterou je třeba se v kontextu této námitky vypořádat, tedy je, zda je možné se vzdát práva na ochranu osobních údajů případně dílčích subjektivních práv, která z něj vyplývají. Druhá námitka pak vychází z tzv. paradoxu soukromí,[303] dle kterého lidé sice tvrdí, že pro ně má jejich soukromí hodnotu, ale fakticky se tak nechovají a svoje údaje nechávají volně šířit, z čehož je možné usuzovat, že i subjektivní práva přiznaná režimem ochrany osobních údajů jsou pro ně vlastně zbytečná.

Řada společností zejména v online prostředí nabízí své služby zdánlivě zdarma. Jejich zákazník však musí při jejich využívání poskytnout své osobní údaje a umožnit jejich zpracování. Díky tomu pak může získávat informační

303 Viz NORBERG, Patricia A., Daniel R. HORNE a David A. HORNE. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* [online]. 2007, roč. 41, č. 1; a dále například NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010, s. 104–108.

a reklamní obsah, který mu je ušit doslova na míru.[304] Když se proto hovoří o tom, že „platíme svými osobními údaji", jde o velmi užitečnou zkratku, díky které si má průměrný spotřebitel možnost uvědomit, že služby, které využívá, nejsou zcela zdarma.[305] Vzhledem k tomu, jak je praxe směny osobních údajů za spotřebitelské výhody častá, mohlo by se zdát, že přiznání osobním údajům statusu věci (a tím pádem i možnosti jejich prodeje *de iure*) by bylo pouze srovnání právního a faktického stavu.[306] Ve prospěch chápání osobních údajů v kontextu věcných práv hovoří řada autorů zejména z angloamerického právního prostředí.[307] Jako hlavní důvod uvádí zejména aspekt možnosti výkonu kontroly nad daty,[308] který však není příliš efektivní z hlediska ochrany práv subjektů údajů.[309] Purtova ve svém starším textu

304 Rizikům tohoto obchodního modelu se detailně věnuje Shoshana Zuboff v jedné z nejzásadnějších prací na poli ochrany soukromí posledních let. ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. 1. vyd. New York: PublicAffairs, 2019.

305 Pro potřeby této publikace se blíže nezabývám otázkou, zda je možné data považovat za věc v právním smyslu, protože dle mého názoru není pro potřeby této publikace zásadní. I za předpokladu, že data mohou být v určitých případech považována za věc v právním smyslu a můžeme tak uvažovat například o jejich prodeji, nic to nezmění na závěru, že právní regulace ochrany osobních údajů se na taková data (která jsou vzhledem ke svému kontextu osobními údaji) bude vztahovat. Obecně k otázce možnosti chápání dat jako věci v právním smyslu viz KOŠČÍK, Michal. Výzkumná data ve světle absolutních majetkových práv. In: KOŠČÍK, Michal et al. *Výzkumná data a výzkumné databáze. Právní rámec zpracování a sdílení vědeckých poznatků*. Praha: Wolters Kluwer ČR, 2018, s. 25–31; K otázkám vlastnického práva k informacím více viz HILDEBRANDT, Mireille a Bibi van den BERG (eds.). *Information, freedom and property: the philosophy of law meets the philosophy of technology*. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2016.

306 Viz PURTOVA, Nadezhda. Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Computers, privacy and data protection: an element of choice*. Dordrecht; New York: Springer, 2011, s. 39.

307 Nadezhda Purtova odvozuje počátky tohoto názorového proudu od Alana Westina (WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967. Citováno dle PURTOVA, Nadezhda. Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review* [online]. 2009, roč. 25, č. 6, s. 507); Dále například viz POSNER, Richard A. *Economic analysis of law*. 3. vyd. Boston: Little, Brown, 1986, s. 38–39; V evropském kontextu rozvíjí teorii vlastnictví osobních údajů Janeček (JANEČEK, Václav. Ownership of personal data in the Internet of Things. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 5).

308 Srovnej SOLOVE, Daniel J. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review* [online]. 2001, roč. 53, č. 6, s. 1446.

309 PURTOVA, Nadezhda. Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review* [online]. 2009, roč. 25, č. 6, s. 519–520.

publikovaném ještě před vznikem návrhu Obecného nařízení argumentuje, že v kontextu technologických výzev pro ochranu osobních údajů, spočívajících v nepřehledných tocích dat a fenoménu big data, by ustanovení věcných práv k osobním údajům usnadnilo výkon kontroly nad daty ze strany subjektů údajů, protože by taková data byla chráněná *erga omnes*.[310] Každý, kdo by osobní údaje zpracovával, by tak musel dodržovat povinnosti, které se s jejich zpracováním pojí. Hlavní argument proti úpravě osobních údajů prostřednictvím věcných práv však spočívá v riziku snížení úrovně ochrany subjektů údajů, protože „prodejem" vlastních osobních údajů by při plném chápání osobních údajů jako věci došlo ke vzdání se práv, která subjektu údajů k jeho osobním údajům svědčí. Purtova proto pro fungování postupu, který navrhuje, předpokládá, že „prodejem" osobních údajů by subjekt údajů neztratil všechna práva, která k nim má, a stále by mohl nad údaji vykonávat určitou úroveň kontroly.[311] Ještě zdrženlivěji se ke komodifikaci osobních údajů staví Gianclaudio Malgieri s Bartem Custersem, kteří k problému přistupují z lidskoprávního hlediska a tvrdí, že právo na ochranu osobních údajů je nezcizitelné jako jiná základní lidská práva.[312]

Purtova dospěla *de facto* ke stejnému závěru jako evropský zákonodárce. Ten ovšem nahradil věcně právní působení *erga omnes* komplexní regulací vycházející z osobnostních práv subjektů údajů,[313] dle které každý, kdo osobní údaje zpracovává, musí dodržovat povinnosti, které se k nim dle Obecného nařízení pojí. Stejně tak subjekt údajů může udělením souhlasu se zpracováním

310 PURTOVA, Nadezhda. Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Computers, privacy and data protection: an element of choice*. Dordrecht; New York: Springer, 2011, s. 56.

311 Ibid., s. 58. Kriticky se k chápání osobních údajů v kontextu majetkových práv vyjádřil Pearce, který ve své detailní analýze přesvědčivě shrnuje hlavní argumenty pro i proti jak majetkoprávního, tak osobnostně právního přístupu k osobním údajům a navrhuje quasi majetkový přístup (PEARCE, Henry. Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law. *European Data Protection Law Review*, 2018, č. 2).

312 Viz MALGIERI, Gianclaudio a Bart CUSTERS. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 300.

313 Zajímavou vazbu mezi osobnostními právy autora a právy k osobním údajů argumentuje Pearce (PEARCE, Henry. Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law? *Information & Communications Technology Law* [online]. 2018, roč. 27, č. 2).

(případně uzavřením smlouvy) umožnit využití jeho osobních údajů ke komerčním účelům (a tím je *de facto* „prodat" výměnou za poskytovanou službu). I v takovém případě se však s osobními údaji pojí práva a povinnosti vyplývající z Obecného nařízení.[314] Zároveň je nutné vyloučit možnost smluvního omezení nebo jednostranného vzdání se práv, která subjektu údajů Obecné nařízení garantuje,[315] a to ze dvou důvodů. První je ve své podstatě hmotněprávní a dobře jej formuluje Guiseppe Versaci, když vychází z účelu, který tato práva mají (tedy zajištění transparentnosti zpracování a kontroly subjektu údajů nad jeho daty) a uvádí: *„[W]here individuals disclose personal information against the access to goods or services, they are not waiving their right to data protection. This exploitation of personal data should be subject only to the condition of validity that individuals save the possibility to exercise the rights they have as data subjects. In the line with this view, the commercial exploitation of personal data can be conceived as an economic dimension of an individual's right to control their personal data, which starts by giving their consent for the processing of their data. Indeed, the same consent is not a waiver of protection, but it is an expression of self-determination."*[316] Pokud bychom měli připustit možnost vzdání se těchto práv, bylo by vzhledem k intenzitě zásahu do zájmů subjektu údajů nezbytné, aby takové právní jednání splňovalo minimálně nároky kladené na souhlas se zpracováním. Jak se ovšem

314 Ve stejné linii argumentace připravil evropský zákonodárce směrnici 2019/770/EU, o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb, ve které se předpokládá, že může docházet k „platbě" osobními údaji (bod 24 odůvodnění uvádí: *„Digitální obsah nebo digitální služby se často poskytují také v případech, kdy spotřebitel za ně neplatí, nýbrž poskytuje obchodníkovi osobní údaje."*). Uvedená směrnice však zároveň na několika místech uvádí, že všechna práva a povinnosti vyplývající z Obecného nařízení musí být zachovány (body odůvodnění 37, 38, 48 a 69 a články 3 odst. 8 a 16 odst. 2). Je zajímavostí, že proti návrhu této směrnice se silně vymezil Evropský inspektor ochrany osobních údajů, který ve svém stanovisku č. 4/2017 uvedl, že „prodej" osobních údajů porušuje čl. 8 Listiny základních práv Evropské unie (viz odst. 20 stanoviska Evropského inspektora ochrany osobních údajů ze dne 14. 3. 2017, č. 4/2017 [online]. [cit. 30. 6. 2020]).

315 Ve prospěch možnosti smluvního omezení práv subjektu údajů hovoří zejména proponenti quasi majetkového chápání osobních údajů. Srovnej PURTOVA, Nadezhda. Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Computers, privacy and data protection: an element of choice*. Dordrecht; New York: Springer, 2011, s. 57.

316 VERSACI, Guiseppe. Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, 2018, roč. 14, č. 4, s. 391. Shodně PURTOVA, Nadezhda. Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights. *Netherlands Quarterly of Human Rights*. 2010, roč. 28, č. 2, s. 197.

ukazuje, je takřka nemožné v okamžik udělení souhlasu (nebo vzdání se práv) dohlédnout reálných důsledků této činnosti v průběhu času, a proto nemůže být takové právní jednání dostatečně informované, jak vyžaduje zákonná úprava. Právě tento aspekt času je pak důležitým argumentem, proč není možné případné vzdání se práv interpretovat jako výkon práva na informační sebeurčení. Smluvním omezením nebo vzdáním se práv by se totiž subjekt údajů připravil o jakoukoli budoucí možnost s danými daty nakládat. Krom toho, práva subjektů údajů slouží jako prostředek ochrany slabší strany a jako v jiných oblastech, kde je tento postup používán (např. spotřebitelské právo), je nutné vzhledem k zachování tohoto účelu právní úpravy vyloučit možnost vzdání se těchto práv.[317]

Druhý důvod je ve své podstatě spíše procesní a spočívá v tom, že práva subjektů údajů jsou chráněna jak soukromoprávní cestou (kdy se jich může subjekt dovolat sám), tak cestou veřejnoprávní, kdy jejich dodržování kontroluje a vymáhá správní úřad. I pokud by se subjekt údajů vzdal svých práv, tedy by se fakticky zavázal k tomu, že je nebude vykonávat soukromoprávně, veřejnoprávní linie bude nadále aplikovatelná, protože tu subjekt údajů vyloučit nemůže. Vzhledem k uvedeným důvodům mám za to, že se subjekt údajů nemůže vzdát svých pozitivně formulovaných subjektivních práv, která mu Obecné nařízení garantuje.

Druhá systematická námitka proti silné roli práv subjektů údajů v kontextu systému ochrany osobních údajů zní, že tento způsob ochrany není v praxi efektivní, protože ačkoli subjekty údajů mají podle práva možnost vykonávat kontrolu nad svými údaji, velice často to nedělají, nebo dokonce naopak bezstarostně rozšiřují více a více svých osobních údajů na sociálních sítích.[318]

317 Srovnej MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12.

318 Tento aspekt je úzce propojen s přístupem tvrdícím, že soukromí je mrtvý koncept a že bychom si měli zvyknout na svět bez soukromí. Proponentem této myšlenky byl (nepřekvapivě) zakladatel společnosti Facebook Mark Zuckeberg (viz JOHNSON, Bobbie. Privacy no longer a social norm, says Facebook founder. *The Guardian* [online]. 2010; ani v jeho případě nešlo však o nový concept (viz například RAUHOFER, Judith. Privacy Is Dead, Get over It: Information Privacy and the Dream of a Risk-Free Society. *Information & Communications Technology Law,* 2008, č. 3); V kontextu dopadů sociálních sítí na zaměstnance hovoří o smrti soukromí SANDERS, Sherry D. Privacy Is Dead: The Birth of Social Media Background Checks. *Southern University Law Review*, 2011, č. 2.

Nissenbaum tuto tendenci nazývá *„mediálním exhibicionismem"*.[319] Průzkumy, které byly provedeny za účelem zjištění, jakou hodnotu lidé svému soukromí a jeho ochraně přikládají, opravdu vykazují podstatné rozdíly mezi tím, jak lidé o soukromí uvažují a tím, jak se chovají. Ačkoli slovně přikládají soukromí vysokou důležitost, jsou ochotní se svých osobních údajů a určité míry soukromí vzdát za relativně nízkou protihodnotu. Marek Kumpošt s Václavem Matyášem provedli výzkum, ve kterém se zabývali cenou, za jakou by byli ochotni respondenti poskytnout své údaje, přičemž objevili rozdíl ve vnímání hodnoty dle toho, zda se údaje poskytují za akademickým nebo komerčním účelem.[320] Alessandro Acquisti se svými kolegy při jiném experimentu dovodil, že není podstatná jen otázka účelu užití dat, ale i toho, jak se výzkumník zeptá. Dotázaní respondenti totiž vykázali výrazně tendence vzdát se svých údajů za úplatu než své soukromí za úplatu posílit.[321]

319 NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010, s. 106–107.

320 Viz KUMPOŠT, Marek a Václav MATYÁŠ. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU,* 2009, roč. 20, č. 1. Výsledek odpovídá závěrům Nissenbaum, dle které je pro koncové uživatele zásadní kontext, v jakém zpracování probíhá, a jeho udržení. K obdobným výsledkům došli Chellappa a Sin, když ověřili, že subjekt údajů spíše poskytne své údaje obchodníkovi za účelem personalizace služeb, pokud mu důvěřuje (CHELLAPPA, Ramnath K. a Raymond G. SIN. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management* [online]. 2005, roč. 6, č. 2–3).

321 GROSSKLAGS, Jens a Alessandro ACQUISTI. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In: *6th Annual Workshop on the Economics of Information Security, WEIS 2007, The Heinz School and CyLab at Carnegie Mellon University, Pittsburgh, PA, USA, June 7-8, 2007* [online]. 2007 [cit. 30. 6. 2020]; Další Acquistiho studie toto potvrdila, a navíc ukázala další zajímavý výsledek v podobě silného vlivu toho, která možnost je nabídnuta jako první – účastníkům výzkumu byly nabízeny dárkové karty různé hodnoty, přičemž ta s nižší hodnotou byla anonymní (v základní verzi experimentu 10 USD), a ta s vyšší hodnotou (v základní verzi experimentu 12 USD) byla vázána na jméno a umožnila sledovat, co účastník výzkumu koupí. Účastník si mohl zvolit, kterou si vezme. Pokud byla nejprve nabídnuta karta s nižší hodnotou nechalo si ji 60 % účastníků a 40 % si vyžádalo kartu s vyšší hodnotou. Pokud ale byla nabídnuta nejprve karta s vyšší hodnotou, zvolilo si méně zasahující kartu jen 33,3 % účastníků (ACQUISTI, Alessandro, Leslie JOHN a George LOEWENSTEIN. What Is Privacy Worth? *Journal of Legal Studies,* 2013, roč. 42, č. 2, s. 25). Uvedená data korespondují s Borgesiusovým popisem psychologických překážek člověka při rozhodování o svém soukromí (setrvávání na *statu quo* a rozhodovací krátkozrakost, viz BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network, 2013, s. 38–43 [cit. 30. 6. 2020]) a ukazují důležitost principů záměrné a standardní ochrany osobních údajů (*„data protection by design"* a *„data protection by default"*) zakotvených v čl. 25 Obecného nařízení.

Helia Marreiros a její kolegové pak nabídli jedno z možných vysvětlení paradoxu soukromí, když objevili souvislost mezi přítomností zmínky o ochraně soukromí v průběhu prováděného výzkumu a ochotou lidí poskytovat své údaje. Jinými slovy, pokud se zmínila problematika soukromí (a ne nutně v negativním kontextu např. ve smyslu porušení zabezpečení osobních údajů), lidé poskytovali méně dat.[322] Je to tedy jako bychom v záplavě jiných informací a nutností se rozhodovat na otázky soukromí zapomínali, ale když jsou nám připomenuty, zajímají nás. Právě proto je zcela zásadní zajištění efektivního informování o zpracování osobních údajů.

Zásadním problémem pro efektivní působení práv, která subjektu údajů garantuje právní regulace Obecného nařízení, je, že jejich výkon přímo subjektem údajů je nesmírně náročný. Příčin tohoto stavu je mnoho. Jde například o přílišné množství instancí zpracování, které by měl subjekt údajů vzhledem ke své osobě spravovat, ale fakticky to je nad jeho fyzické možnosti, nebo o neuvědomění si hodnoty vlastních údajů.[323] Další příčinou je složitost právních dokumentů, které by správně měly situaci usnadnit, ale často se to spíše neděje, protože jsou psány tak, aby minimalizovaly riziko sankce na straně správce údajů. Příčinou je pak rovněž kterýkoli z dalších dílčích důvodů identifikovaných ve výše citovaných výzkumech. Druhým zásadním problémem je, že ačkoli jsou práva subjektu údajů chráněna i veřejnoprávně činností dozorového úřadu, je činnost úřadu omezena limitovaným množstvím finančních a personálních zdrojů, které mohou být na kontrolu a vymáhání vynaloženy.

Přesto není možné pozitivně formulovaná práva subjektů údajů ze systému ochrany osobních údajů odstranit nebo na ně rezignovat. Hlavním účelem právní regulace ochrany osobních údajů je zajištění korektního zpracování osobních údajů a ochrana práv subjektu údajů. V tomto směru jsou

322 MARREIROS, Helia et al. "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization* [online]. 2017, roč. 140.

323 Hodnota osobních údajů se nezbytně liší, když se bude jednat o jeden záznam, nebo naopak velké množství záznamů zpracovávaných v režimu big data. Z toho důvodu například Malgieri navrhuje, že by v rámci informační povinnosti správce měla být sdělována i hodnota údajů daného subjektu. Viz MALGIERI, Gianclaudio a Bart CUSTERS. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 302.

probíraná práva nezbytná, protože zajišťují možnost výkonu autonomie subjektu údajů v průběhu času, tedy zatímco jsou data zpracovávána. Jsou nezbytným nástrojem transparentnosti zpracování. Zabrzďují správce údajů v mantinelech korektního zpracování a jsou tak předpokladem pro efektivní výkon práva na informační sebeurčení. Subjekt údajů proto musí mít možnost tato svá práva aplikovat, protože jinak by se normativní nastavení systému zpracování vychýlilo příliš na stranu správce.

Možnou praktickou cestou jak překonat fakticky slabou pozici subjektu údajů, když přijde na hájení jeho subjektivních práv, je inspirace v právní úpravě ochrany spotřebitele.[324] Evropský zákonodárce se pokusil tento praktický nedostatek reflektovat zanesením možnosti zastoupení subjektu údajů neziskovou organizací věnující se ochraně osobních údajů, a to včetně možnosti podávání hromadných žalob.[325] Čl. 80 Obecného nařízení výslovně uvádí možnost členských států zakotvit do svých právních řádů možnost, aby neziskové organizace zastupovaly subjekty údajů a vykonávaly jejich práva i bez pověření. Bohužel se však jedná jen o možnost nabídnutou evropským zákonodárcem. Řada členských států, včetně České republiky, ji však nevyužila a do svého právního řádu tuto možnost nezanesla.[326] Mám

324 Podobnostmi obou právních režimů v kontextu českého práva se ve svém starším textu zabýval Nonnemann (viz NONNEMANN, František. Ochrana spotřebitele a ochrana osobních údajů. *Právní rozhledy*, 2010, roč. 18, č. 22). Z novějších prací je možné zmínit Svantessonovu studii, ve které srovnává rámce právní úpravy ochrany osobních údajů a ochrany spotřebitele a dochází k závěru, že ochrana osobních údajů působí jako *lex specialis* vůči ochraně spotřebitele a může ji v určitých případech omezovat, protože na rozdíl od ní nechrání jen práva subjektu údajů (spotřebitele), ale také správce údajů a jeho zájem na zpracování a volném toku osobních údajů (což je druhý základní účel právní úpravy osobních údajů). Viz SVANTESSON, Dan Jerker B. Enter the quagmire – the complicated relationship between data protection law and consumer protection law. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 1, s. 34.

325 Tato myšlenka se jako varianta řešení zmiňovaného problému objevila již dříve, zejména v oblasti angloamerického práva viz např. VAN HAL, Timothy J. Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection Note. *Vanderbilt Journal of Entertainment and Technology Law,* 2013, roč. 15, č. 3; V evropském kontextu je třeba připomenout rozsudek Soudního dvora Evropské unie ze dne 25. 1. 2018, C-498/16, ve kterém SDEU odmítl takovou intepretaci nařízení Brusel I, která by umožnila podat hromadnou žalobu podle rakouského práva před rakouskými soudy, když má žalovaná strana (Facebook Ireland) sídlo v Irsku.

326 Dle Hodgese je nějaká forma hromadné žaloby upravena ve 20 členských státech EU (viz HODGES, Christopher. Delivering Data Protection: Trust and Ethical Culture Discussion. *European Data Protection Law Review*, 2018, roč. 4, č. 1, s. 78).

však za to, že do budoucna je toto jedna z možných cest, jak fakticky zlepšit výkon a ochranu práv subjektů údajů.

2.4 Ochrana osobních údajů jako nástroj prevence

V dosavadním výkladu této kapitoly bylo právo na ochranu osobních údajů identifikováno jako samostatné základní právo s jasně formulovanými účely. První účelem byla ochrana osobních údajů fyzických osob, díky které jsou zprostředkovaně chráněna další práva a zájmy subjektu údajů, které by mohly být zasaženy zpracováním osobních údajů. Druhý účel byl formulován jako možnost zajištění, že správce údajů bude moci provádět korektní zpracování osobních údajů. Těmto dvěma účelům odpovídají dvě základní premisy dále rozebrané v předchozích částech této kapitoly. Část 2.2 formulovala v souladu s druhým účelem úpravy tezi, že zpracování osobních údajů je pragmaticky nezbytné a právní úprava ochrany osobních údajů jejich zpracování obecně spíše umožňuje. Tato možnost však není bezbřehá. Ochranu subjektu údajů pomáhá z jedné strany zajistit silný princip omezení účelem zpracování společně s nezbytností mít před zahájením zpracování vhodný právní titul. Z druhé strany pak správce údajů limitují subjektivní pozitivní práva subjektů údajů. Právě těm byla věnována část 2.3 této kapitoly. Práva subjektů údajů formulovaná v Obecném nařízení úzce souvisí s právem na informační sebeurčení a zajišťují možnost projevu autonomie vůle subjektu údajů. Jsou prostředkem, kterým může subjekt kontrolovat správce v průběhu zpracování osobních údajů. Tuto roli pak plní (a vhledem k jejich postavení v rámci systému ochrany osobních údajů musí plnit) i přes zásadní problémy, které spočívají zejména v obtížném vymáhání těchto práv.

Posledním střípkem, který zbývá zasadit do mozaiky základních premis, na kterých právní úprava ochrany osobních údajů spočívá, je silně preventivní povaha práva na ochranu osobních údajů.[327] Ta vyplývá z jeho prvního výše formulovaného účelu, tedy zajištění ochrany fyzických osob při zpracování jejich osobních údajů. V rámci režimu ochrany osobních údajů aplikuje sankce nejen v případech vzniklé škody nebo újmy. Správce údajů může být sankcionován za špatné zpracování i tehdy, když subjektu žádná škoda

327 Srovnej shodně např. CAVOUKIAN, Ann. Privacy by Design: Leadership, Methods, and Results. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 192.

nebo újma nevznikla. Je tomu tak právě proto, že cílem ochrany osobních údajů je právě prevence zásahu do práv a zájmů subjektů údajů. Tomu odpovídá i řada veskrze preventivních povinností správce údajů, jako je zásada minimalizace zpracovávaných osobních údajů, povinnost zabezpečit zpracování před únikem dat nebo nový princip záměrné a standardní ochrany osobních údajů, který přineslo Obecné nařízení.[328] Interpretační závěr vyplývající z preventivní povahy ochrany osobních údajů a účelů její úpravy je následující: Ustanovení právních předpisů upravujících ochranu osobních údajů je nezbytné interpretovat tak, aby byla jejich aplikace co možná nejširší. Z toho vyplývají dva normativní závěry pro interpretaci: i) definiční ustanovení, která zakládají aplikaci daného předpisu, je třeba vykládat široce a ii) ustanovení, která v jakékoli podobě zavádějí výjimky z aplikace těchto předpisů, je třeba vykládat úzce. Tento závěr je potvrzen, když do argumentace zapojíme pozitivní subjektivní práva subjektů údajů. Aby se jich subjekt údajů mohl dovolat, a tím mohl vykonávat své právo na informační sebeurčení, je opět třeba, aby aplikace předpisů ochrany osobních údajů byla co nejširší. Uvedené koresponduje s maximou, kterou evropský zákonodárce stanovil jak pro směrnici 95/46/ES[329], tak i Obecné nařízení,[330] a která tvrdí, že musí být zajištěna *„vysoká úroveň ochrany osobních údajů"*.[331] Uvedená interpretační pravidla potvrzuje i rozhodovací praxe soudního dvora Evropské Unie. Účelem následujícího přehledu judikatury je předvést tendence v rozhodovací praxi SDEU, tedy postupně vyhodnotit, zda v konkrétním případě SDEU zvolil spíše extenzivní, nebo restriktivní interpretaci daného pojmu. Rozhodnutí jsou záměrně zanechána bez jejich detailnějšího popisu a jsou řazena v chronologickém pořadí.

328 Viz čl. 25 Obecného nařízení.

329 Bod 10 odůvodnění směrnice 95/46/ES.

330 Body 6 a 10 odůvodnění Obecného nařízení.

331 Tuto maximu ve svých rozhodnutích velice často cituje Soudní dvůr Evropské unie (viz např. body 72 a 73 rozsudku Soudního dvora Evropské unie ze dne 6. 10. 2015 ve věci *Schrems*, C-362/14). Mnohdy ji však používá jako argumentační zkratku, jako nezpochybnitelné dogma, kterým nahrazuje preciznější právní argumentaci (viz například bod 27 rozsudku Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13, případně bod 66 rozsudku Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12). Takový způsob argumentace pak hraničí s právním kýčem (více k pojmu viz MÍŠEK, Jakub. Právní kýč: Argumenty v zajetí koťátek a lidských práv. In: ŠKOP, Martin, Michal MALANÍK a Markéta KLUSOŇOVÁ. *Kreativita v právu 2014*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2014, s. 58–72).

V rozhodnutí ve věci Lindqvist SDEU určil, že umístění osobních údajů na soukromou webovou stránku představuje jejich zpracování.[332] V rozsudku ve věci Satamedia se SDEU dále zaměřil na vymezení pojmu zpracování osobních údajů. Potvrdil, že do jeho rozsahu spadá shromažďování osobních údajů (konkrétně údajů o příjmech z výdělečné činnosti, kapitálu a majetku fyzických osob) ve veřejných dokumentech finančního úřadu, jejich zveřejňování, komerční publikace údajů na CD-ROM a zasílání údajů formou SMS.[333]

Lisabonská smlouva přinesla z hlediska ochrany osobních údajů dvě základní novinky v podobě čl. 16 Smlouvy o fungování Evropské unie,[334] který nově slouží jako právní základ pro veškerou legislativu věnující se ochraně osobních údajů, a čl. 8 Listiny základních práv Evropské unie, který uvádí právo na ochranu osobních údajů jako samostatné základní právo. SDEU na tento vývoj zareagoval tak, že ztratil ostych silně využívat argument, že ochrana osobních údajů je základním právem, a proto musí být osobním údajům přiznána silná ochrana.[335] V době před Lisabonskou smlouvou se SDEU o koncept základního práva na ochranu osobních údajů nemohl plně opřít, protože Charta základních práv EU[336] nebyla právně závazná. Krom toho směrnice 95/46/ES byla přijata na základě čl. 100a smlouvy o Evropské unii (nynější čl. 114 smlouvy o fungování Evropské unie), který zmocňuje k vydání legislativy za cílem zajištění ekonomických aspektů fungování vnitřního trhu Unie. Vzhledem k tomu bylo hlavním legislativním cílem zajištění volného pohybu těchto dat v rámci Unie. Ve svých dřívějších rozhodnutích

332 Bod 27 rozsudku Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01.

333 Bod 37 rozsudku Evropského soudního dvora ze dne 16. 12. 2008 ve věci *Satakunnan Markkinapörssi a Satamedia*, C-73/07. Je zajímavostí, že rozhodnutí ve věci *Satamedia* je zároveň jedno z mála rozhodnutí, v nichž SDEU uvedl, že je třeba široce interpretovat jiné právo (právo na svobodu projevu), které bylo s ochranou osobních údajů v kolizi (viz bod 56 rozsudku). Více k rozhodnutí *Satamedia* viz TZANOU, Maria. Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection. *Croatian Yearbook of European Law & Policy*, 2010, roč. 6.

334 Viz čl. 8 Listiny základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

335 Srovnej též LYNSKEY, Orla. From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht, Springer Netherlands, 2013, s. 77–78.

336 Charta základních práv a svobod Evropské unie (dokument č. 2000/C 364/1).

proto lidskoprávní úroveň SDEU argumentoval ve smyslu čl. 8 Evropské úmluvy o ochraně lidských práv.[337] První rozhodnutí, ve kterém se nový přístup SDEU projevil, byl rozsudek ve věcech *Schecke* a *Eifert*.[338] V něm SDEU poprvé přímo argumentoval v kontextu ochrany osobních údajů Listinou základních práv EU a poprvé rovněž zneplatnil sekundární evropskou legislativu z důvodu jejího porušení základních práv chráněných Listinou základních práv EU. Byť toto rozhodnutí neobsahuje přímo žádný případ výkladu definičních ustanovení nebo šíře výjimek, uvádím jej zde vzhledem k zásadnosti změny, kterou představuje.

Tendence širokého výkladu naznačená v rozhodnutí ve věci *Lindqvist* byla po účinnosti Lisabonské smlouvy potvrzena. V rozhodnutí ve věci *Scarlet Extended* SDEU jako *obiter dictum* uvedl, že IP adresy spadají do definice osobních údajů, aniž by bohužel nabídl jakoukoli bližší argumentaci tohoto závěru.[339] Následně rozsudek ve věci *Worten* potvrdil, že údaje o denní pracovní době a době odpočinku pracovníka je třeba považovat za osobní údaje.[340] Poměrně bohatým z hlediska širokého výkladu definičních pojmů pak bylo rozhodnutí ve věci *Google Spain*, ve kterém SDEU určil, že činnost internetového vyhledávače v podobě indexování osobních údajů přítomných v dokumentech třetích stran a jejich následné nabízení jako výsledků vyhledávání představuje zpracování osobních údajů.[341] Zároveň ve stejném rozhodnutí SDEU nakročil k širokému chápání pojmu provozovna správce, když stanovil, že zpracování osobních údajů je *„prováděno v rámci činností provozovny správce na území členského státu…, pokud provozovatel internetového vyhledávače zřídí v členském státě pobočku nebo dceřinou společnost určenou k podpoře prodeje a k prodeji reklamního prostoru nabízeného tímto vyhledávačem, která zaměřuje svou*

337 Srovnej GONZÁLEZ-FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Cham; New York: Springer, 2014, s. 234.

338 Rozsudek Evropského soudního dvora ze dne 9. 11. 2010 ve věcech *Volker und Markus Schecke* a *Eifert*, C-92/09 a 93/09.

339 Bod 51 rozsudku Soudního dvora Evropské unie ze dne 24. 11. 2011 ve věci *Scarlet Extended*, C-70/10.

340 Bod 22 rozsudku Soudního dvora Evropské unie ze dne 30. 5. 2013 ve věci *Worten*, C-342/12; Shodnou interpretaci SDEU konstatoval rovněž v usnesení ze dne 19. 6. 2014 ve věci *Pharmacontinente - Saúde e Higiene*, C-683/13, a další.

341 Bod 28 rozsudku Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

činnost na obyvatele tohoto státu."[342] Na rozhodnutí *Google Spain* je zřetelně vidět snaha interpretovat ustanovení směrnice 95/46/ES tak široce, aby na daný případ dopadala i přes neřešitelné systematické problémy, které zvolená interpretace rovněž přinesla.[343]

V červenci 2014 SDEU poskytl vysvětlení rozdílu mezi nosičem informace a informací samotnou, když v rozsudku ve věci *YS* stanovil, že údaje, které se týkají fyzické osoby uvedené v protokolu nebo v právním rozboru jsou sice osobními údaji, protokol či případně právní rozbor samotný již však osobními údaji nejsou.[344] SDEU v tomto rozhodnutí vhodně limitoval rozsah pojmu osobní údaj tak, že se jedná o informace jako takové a nikoli o dokumenty, které tyto informace obsahují. Rozhodnutí ve věci *YS* je doposud jediným rozhodnutím, ve kterém SDEU při hodnocení otázky, zda hodnocený prvek spadá pod definici osobních údajů, rozhodl negativně.

V říjnu 2015 SDEU navázal na rozhodnutí *Google Spain* a nabídl další upřesnění a výrazné rozšíření pojmu provozovna správce v rozsudku ve věci *Weltimmo*, ve kterém dovodil, že správce údajů má v členském státě provozovnu i při splnění minimálních požadavků v podobě kombinace existující webové stránky v patřičném jazyce, stálého právního zastoupení a otevřeného bankovního účtu.[345] Druhou podmínku pro aplikaci právní úpravy ochrany osobních údajů v podobě požadavku, aby zpracování osobních údajů probíhalo „v rámci činnosti" této provozovny SDEU, rovněž vyložil široce. Připomněl, že není třeba, aby provozovna sama osobní údaje zpracovávala, ale stačí, aby prováděla činnosti se zpracováním související. V případě společnosti Weltimmo bylo takovou činností zveřejnění inzerátu s osobními údaji na její webové stránce a fakturace zveřejněné inzerce.[346]

Velice významným rozhodnutím z oblasti upřesnění definice pojmu osobní údaj byl rozsudek ve věci *Breyer* z října 2016. V něm SDEU navázal na své předchozí rozhodnutí ve věci *Scarlet Extended* a dovodil, že za osobní údaj

342 Ibid., bod 60.
343 Zmíněné problémy jsou detailně pojednány v části 3.2 této publikace.
344 Bod 48 rozsudku Soudního dvora Evropské unie ze dne 17. 7. 2014 ve věci *YS a další*, C-141/12.
345 Body 32-33 rozsudku Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci *Weltimmo*, C-230/14.
346 Ibid., body 34–36.

je nezbytné považovat rovněž dynamickou IP adresu.[347] Široký interpretační přístup k otázce definice osobních údajů SDEU pak udržel i v rozhodnutí ve věci *Nowak*, v němž určil, že za osobní údaje je třeba považovat rovněž písemně vyhotovené odpovědi uvedené zkoušeným při odborné zkoušce a s nimi rovněž i korekturní poznámky zkoušejícího pojící se k těmto odpovědím.[348]

V posledních letech SDEU nabídl sérii rozhodnutí, ve kterých se zabývá šíří interpretace pojmu správce údajů. Prvním z nich byl rozsudek ve věci *Wirtschaftsakademie Schleswig-Holstein*, v němž určil, že správce stránky na sociální síti Facebook je správcem (resp. společným správcem se společností Facebook) osobních údajů fanoušků spravované stránky.[349] Druhým takovým rozhodnutím, ve kterém SDEU rozšířil interpretaci pojmu správce údajů, byl rozsudek ve věci *Jehovan todistajat* (v češtině populárně označovaný jako rozhodnutí ve věci *Svědkové Jehovovi*), v němž SDEU dovodil, že náboženskou společnost je možné považovat za (společného) správce osobních údajů, které sbírají při misijní činnosti její členové, byť sama nemusí mít k takovým údajům přístup. Hlavním argumentem SDEU pro tento závěr bylo, že náboženská společnost *de facto* určuje účel zpracování těchto osobních údajů, protože své členy v rámci jejich podomní kazatelské činnosti podporuje a koordinuje.[350] Třetím rozhodnutím z této série, ve kterém SDEU potvrdil nezbytnost široké interpretace pojmu (společný) správce údajů, byl rozsudek ve věci *Fashion ID*. Dle něj je třeba za správce osobních údajů považovat provozovatele webové stránky, na které je umístěn *plugin* sociální sítě, který sbírá informace o návštěvnících dané stránky.[351] I v tomto případě je provozovatel stránky společným správcem se společností provozující danou sociální síť. Prozatím posledním rozhodnutím, které je možné

347 Bod 49 rozsudku Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer*, C-582/14. Hlubší analýza uvedeného rozhodnutí je přítomná v následujících částech této knihy.

348 Bod 62 rozsudku Soudního dvora Evropské unie ze dne 20. 12. 2017 ve věci *Nowak*, C-434/16.

349 Bod 44 rozsudku Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16.

350 Bod 75 rozsudku Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17.

351 Bod 85 rozsudku Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci *Fashion ID*, C-40/17.

v tomto kontextu zmínit, je rozsudek ve věci *Land Hessen*, v němž soudní dvůr stanovil, že pokud petiční výbor parlamentu člena federace, která je členským státem EU, určuje účel zpracování osobních údajů, je nutné jej chápat jako správce osobních údajů.[352] Tato série rozhodnutí tak dobře ukazuje, jak široký je v současné době výklad základního definičního pojmu správce údajů.

Nyní se opět v chronologickém pořadí zaměříme na případy, ve kterých se SDEU zabýval šíří výjimek ze zpracování osobních údajů. V rozsudku ve věci *Lindqvist* uvedl, že zveřejnění osobních údajů na (byť soukromé) webové stránce nemůže představovat zpracování osobních údajů výhradně pro osobní nebo domácí potřeby, a proto se na něj tato výjimka z režimu zpracování nemůže vztahovat.[353] Argumentem SDEU bylo zejména to, že jsou osobní údaje tímto způsobem zveřejněny a dostupné komukoli online a přesahují proto osobní sféru. Druhým případem, ve kterém se SDEU zabýval otázkou výjimek z aplikace směrnice 95/46/ES, byl rozsudek ve věci *IPI*, který se týkal výjimky z informační povinnosti v případech, kdy dochází ke zpracování osobních údajů za účelem předcházení trestným činům, jejich vyšetřování, odhalování a stíhání. SDEU tento případ rozhodl spíše extenzivně tak, že se tato výjimka může vztahovat rovněž na činnost soukromého detektiva.[354]

Restriktivní přístup naopak SDEU zvolil v případě věci *Ryneš*, ve kterém stanovil, že se výjimka zpracování osobních údajů výhradně pro osobní nebo domácí potřeby nevztahuje na činnost nahrávání záznamu bezpečnostní kamerou, která je umístěna tak, že snímá část veřejného prostranství.[355] V rozsudku ve věci *Jehovan todistajat* (*Svědkové Jehovovi*) pak SDEU určil, že na zpracování osobních údajů členy náboženské společnosti v rámci jejich podomní kazatelské činnosti se rovněž výjimka zpracování pro osobní

352 Bod 74 rozsudku Soudního dvora Evropské unie ze dne 9. 7. 2020 ve věci *Land Hessen*, C-272/19.

353 Bod 47 rozsudku Soudního dvora Evropské unie ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01.

354 Bod 52 rozsudku Soudního dvora Evropské unie ze dne 7. 11. 2013 ve věci *IPI*, C-473/12.

355 Bod 35 rozsudku Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13.

nebo domácí potřebu nevztahuje.[356] Zatím naposledy se pak SDEU k otázce výjimek z režimu právní úpravy směrnice 95/46/ES (nebo ochrany osobních údajů obecně) vyjadřoval v případu ve věci *Buivids*. V něm potvrdil svůj restriktivní přístup k výjimkám ze zpracování, když stanovil, že se žádná z výjimek nevztahuje na zpracování osobních údajů v podobě pořízení videozáznamu příslušníků policie při provádění procesních úkonů a jeho zveřejnění na internetu.[357]

V průběhu posledního roku je možné upozornit na rozhodnutí ve věci *Planet49*, ve kterém se SDEU věnoval výkladu toho, jak může koncový uživatel udělit souhlas s použitím technologie cookies.[358] SDEU se poměrně očekávatelně přiklonil k přísnější interpretaci konceptu souhlasu, když rozhodl, že předzaškrtnuté políčko ve formuláři nemůže být dostatečným platným projevem souhlasu subjektu údajů.[359]

Právě uvedený přehled rozhodovací praxe SDEU obsahuje všechna rozhodnutí, ve kterých se SDEU vyjadřoval k interpretační šíři pojmů, které určují, zda bude právní úprava osobních údajů v daném případě aplikována, či nikoli. Jde tedy o rozhodnutí, která se zabývala šíří definice klíčových pojmů osobní údaj, správce osobních údajů, zpracování osobních údajů, nebo které interpretovaly šíři výjimek z aplikace právní úpravy.[360] Výše popsaný přehled je možné shrnout následovně. Pojmem zpracování osobních údajů se SDEU zabýval ve třech případech a ve všech případech zaujal, případně potvrdil,

356 Bod 51 rozsudku Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17.

357 Bod 47 rozsudku Soudního dvora Evropské unie ze dne 14. 2. 2019 ve věci *Buivids*, C-345/17.

358 Ačkoli rozsudek ve věci *Planet49* vykládá ustanovení směrnice 2002/58/ES, je možné jej do tohoto přehledu zařadit, protože zmíněna směrnice přímo odkazuje na směrnici 95/46/ES s tím, že standard pro udělený souhlas se zpracováním osobních údajů je totožný. Toto rozhodnutí je zařazeno i přes to, že se v přísném slova smyslu nejedná o výjimku, nicméně otázka šíře interpretace souhlasu se zpracování tak fakticky působí, protože její výsledek ovlivňuje možnost existence takového zpracování.

359 Bod 65 rozsudku Soudního dvora Evropské unie ze dne 1. 10. 2019 ve věci *Planet49*, C-673/17.

360 Rozhodnutí byla vyhledána v systému Curia.Europa (curia.europa.eu) prostřednictvím funkce „citace dokumentu ve výroku", kdy jako související hledaný dokument byla zvolena směrnice č. 95/46/ES a nařízení č. 2016/679. Vzhledem k ustálené zvyklosti SDEU uvádět ve výrocích svých rozhodnutí označení dokumentu, kterého se týká zodpovídaná předběžná otázka, jde o spolehlivý způsob nalezení všech souvisejících rozhodnutí. Rozhodnutí, která se netýkala definičních pojmů nebo výjimek, nebyla do přehledu zahrnuta.

nutnost jeho širší interpretace. SDEU se dále sedmkrát zabýval významem pojmu osobní údaj a v šesti případech přistoupil k interpretaci extenzivně.[361] SDEU přikročil k extenzivní interpretaci rovněž ve dvou případech, ve kterých se věnoval definičnímu vymezení pojmu provozovna správce,[362] a ve čtyřech případech, ve kterých se zabýval pojmem správce údajů. V případě výjimek naopak zaujal SDEU v pěti případech ze šesti restriktivní intepretaci, a tedy zachování daného případu v režimu zpracování osobních údajů. Krom toho je třeba zmínit, že SDEU nezbytnost restriktivního přístupu k interpretaci rozsahu výjimek výslovně uvádí a potvrzuje.[363]

Tento přehled rozhodovací praxe potvrzuje existenci prevenčního principu systému ochrany osobních údajů, který nutně vede k závěru, že definiční ustanovení je třeba vykládat široce a výjimky úzce, tak aby aplikace právní úpravy ochrany osobních údajů dopadla na maximální množství případů. Závěrem této části je nutné zmínit starší rozhodovací praxi českých soudů, které zejména k pojmu osobní údaj přistupovaly restriktivně. Například Ústavní soud ve svém nálezu z března roku 2004, sp. zn. Pl. ÚS 38/02, dovozuje, že fyzické osoby, které jsou podnikateli, nepožívají v kontextu výkonu jejich podnikatelské činnosti ochrany osobních údajů, protože je na ně třeba pohlížet stejně, jako na osoby právnické, které takto chráněny nejsou.[364] Jako druhý příklad je možné uvést rozsudek NSS ze srpna 2009, ve kterém soud dospěl k závěru, že jméno a příjmení fyzické osoby v kombinaci s číslem jejího občanského průkazu není osobním údajem, protože *„na základě těchto údajů totiž není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla průkazu.“*[365] Tato rozhodnutí a další jim podobná je třeba

361 Výjimkou byl rozsudek ve věci *YS*, v němž došlo k rozdělení osobních údajů a jejich nosiče.

362 Více k otázce provozovny správce viz SVANTESSON, Dan Jerker B. Article 4(1)(a) 'establishment of the controller in EU data privacy law—time to rein in this expanding concept? *International Data Privacy Law*, 2016, roč. 6, č. 3.

363 Viz bod 38 rozsudku Soudního dvora Evropské unie ze dne 27. 9. 2017 ve věci *Puškár*, C-73/16; bod 37 rozsudku Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17; a bod 41 rozsudku Soudního dvora Evropské unie ze dne 14. 2. 2019 ve věci Buivids, C-345/17.

364 Viz nález Ústavního soudu ze dne 9. 3. 2004, sp. zn. Pl.ÚS 38/02, č. N 36/32 SbNU 345, č. 299/2004 Sb.

365 Rozsudek Nejvyššího správního soudu ze dne 29. 7. 2009, č. j. 1 As 98/2008-148, č. 1944/2009 Sb.NSS., s. 11; Tento přístup je typickým příkladem tzv. subjektivního přístupu k osobním údajům. Více viz kapitola 4 této publikace.

označit jako jednoznačné překonaná. Jejich závěry již v dnešní době nemohou obstát, a to zejména vzhledem k výše pojednané rozhodovací praxi SDEU, která má v těchto otázkách vzhledem k prioritě evropského práva a nutnosti euro-konformního výkladu interpretační přednost.[366]

2.5 Shrnutí kapitoly

Cílem této kapitoly bylo představit východiska, na kterých spočívá právní úprava ochrany osobních údajů a která poslouží jako základ pro další výklad této publikace. V její první části byl rozebrán historický vývoj práva na soukromí (včetně informačního soukromí), práva na ochranu osobních údajů a jejich vztah k právu na informační sebeurčení. Právo na ochranu osobních údajů, které z práva na informační sebeurčení vychází, bylo identifikováno jako samostatné, od práva na soukromí již zcela oddělené základní právo, které má vlastní metody a účely. Tento dílčí závěr tvoří první východisko této knihy.

Účely právní úpravy ochrany osobních údajů byly identifikovány dva a tvoří druhé a třetí východisko této publikace. Prvním účelem práva na ochranu osobních údajů je ochrana fyzických osob před zneužitím a nekorektním zpracováním jejich osobních údajů, čímž dochází k nepřímé ochraně dalších práv a zájmů těchto fyzických osob. Zpracování osobních údajů totiž může představovat virtualizovanou informační úroveň aplikace dalších práv subjektů údajů. Je rovněž třeba zdůraznit, že zpracování osobních údajů není statické, ale probíhá v čase, a jeho okolnosti se mohou měnit. Účelem právní úpravy ochrany osobních údajů je proto zajištění ochrany práv a zájmů subjektu údajů po celou dobu probíhajícího zpracování.

366 Vzhledem k uvedenému je pak zcela nepochopitelnou chybou, když soudy tato stará rozhodnutí přejímají a citují jako danost, jako se to stalo v případě rozsudku Nejvyššího soudu ze dne 17. 12. 2015, sp. zn. 21 Cdo 367/2015, č. 45/2017 Sb.NS, v jehož bodě 24 stojí: *„Informace o pacientech uvedené v přehledech návštěv se však netýkají určených nebo určitelných subjektů, neboť pacienty na základě nich nelze přímo ani nepřímo identifikovat. Dospěla-li judikatura soudů ve věcech správního soudnictví… k závěru, že jméno a příjmení fyzické osoby v kombinaci s číslem občanského průkazu není osobním údajem ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, neboť na základě těchto údajů není možné určit konkrétní osobu, tím spíše je opodstatněný závěr, že osobním údajem ve smyslu tohoto ustanovení není jméno a příjmení fyzické osoby ve spojení s rokem jejího narození."*

Druhým účelem práva na ochranu osobních údajů je umožnění využití osobních údajů pro zpracování, která jsou v širokém slova smyslu přínosná pro společnost. Právní úprava ochrany osobních údajů je postavena tak, aby poskytovala široké možnosti pro provádění zpracování osobních údajů, což vychází z pragmatického přiznání velkého socio-ekonomického potenciálu, který ve zpracování osobních údajů leží. Tento druhý účel byl pak detailněji rozebrán v druhé části této kapitoly, která interpretovala právní úpravu ochrany osobních údajů jako rámec, který vymezuje možnosti nakládání s osobními údaji, ale který zároveň přiznává důležitost probíhajícího zpracování. Vzhledem k tomu je nezbytné, aby byly povinnosti správce údajů odpovídající povaze probíhajícího zpracování. Jak ukázala třetí část této kapitoly, která se soustředila blíže na první účel právní úpravy, tedy ochranu práv a zájmů subjektů údajů, subjektivní pozitivní práva subjektů údajů plní v systému ochrany osobních údajů zásadní funkci pojistky, když pomáhají narovnat informační deficit na straně subjektu údajů a umožňují mu vykonávat kontrolu správce během probíhajícího zpracování. Působí tak jako nástroj projevu autonomie vůle subjektu údajů umožňující výkon práva na informační sebeurčení a zároveň jako pojistka před protiprávním a nekorektním zpracováním osobních údajů ze strany správce.

Konečně poslední část této kapitoly za pomoci analýzy rozhodovací praxe SDEU identifikovala prevenci jako interpretační princip, který se projevuje při výkladu ustanovení předpisů upravujících ochranu osobních údajů. V důsledku principu prevence a v souladu se závěry rozhodovací praxe SDEU je třeba vykládat extenzivně ta ustanovení, která zakládají působnost ochrany osobních údajů (typicky se jedná o definiční ustanovení), a naopak je třeba vykládat restriktivně ustanovení, která zakládají výjimky z aplikace této právní úpravy. Tento dílčí závěr tvoří čtvrté základní východisko ochrany osobních údajů a této publikace.

3 MINULOST OCHRANY OSOBNÍCH ÚDAJŮ: SMĚRNICE 95/46/ES A JEJÍ PROBLÉMY

Směrnice 95/46/ES byla v souladu s jejím čl. 33 během doby své účinnosti podrobena přezkumům ze strany Evropské komise, která hodnotila, zda stále odpovídá potřebám a cílům, pro které byla přijata. První hodnocení bylo zveřejněno v roce 2003.[367] Komise identifikovala několik nedostatků spočívajících zejména v rozdílech v národních implementacích, které sice nedosahovaly takové intenzity, aby se jednalo o porušení komunitárního práva, ale přesto způsobovaly značné problémy v kontextu jednotného trhu a volného pohybu údajů na něm.[368] Problémy byly shledány i v oblastech plnění povinností správců údajů, kteří jen neradi měnili své fungování tak, aby odpovídalo požadavkům ochrany osobních údajů. Podobně pak bylo konstatováno nedostatečné vymáhání povinností ze strany dozorových úřadů a nízké povědomí subjektů údajů o jejich právech.[369] I přes uvedené nedostatky však Komise hodnocení uzavřela s tím, že vzhledem k novosti celého systému a nízkým praktickým zkušenostem s jeho fungováním je předčasné dělat jakékoli závěry o jeho komplexním fungování a doporučila neprovádět žádnou legislativní změnu.[370] Druhé hodnocení zveřejnila Komise v březnu 2007.[371] V něm sice konstatovala, že nadále přetrvalo několik pochybení, ovšem v celku byla směrnice nadále odpovídající, zejména díky svému technologicky neutrálnímu přístupu k regulované materii.[372] Žádná změna proto zatím nebyla potřeba. Na druhé hodnocení reagoval Evropský inspektor ochrany osobních údajů, který ve svém stanovisku souhlasil se závěrem, že v danou chvíli je právní stav dostatečný,

367 First report on the implementation of the Data Protection Directive (95/46/EC). *Evropská komise* [online]. 2003, 27 s. [cit. 30. 6. 2020].

368 Ibid., s. 12.

369 Ibid.

370 Viz HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/ EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 147.

371 Sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů, č. KOM(2007) 87. *Evropská komise* [online]. 2007, 10 s. [cit. 30. 6. 2020].

372 Ibid., s. 7.

ovšem změny budou nezbytné zejména vzhledem k technologickému vývoji, a proto je vhodné se na ně začít připravovat.[373]

Třetí hodnocení bylo zveřejněno v listopadu 2010.[374] Předcházely mu veřejné konzultace, ve kterých se k otázce vhodnosti dosavadní právní úpravy vyjádřilo velké množství stran, včetně WP 29.[375] Dle Petera Hustinxe[376] hodnocení jako přední nedostatek fungování dosavadního systému právní úpravy shledalo zaostávání za technologickým vývojem. Viviane Reding, bývalá komisařka pro spravedlnost, která měla probíhající reformu v gesci, rovněž řadila technologický pokrok na první místo důvodů, proč bylo třeba reformu provést. Konkrétně uvedla: *„The new ways of creating, using, and transferring data bring benefits to individuals, businesses, and public authorities. However, the data revolution we are witnessing must go hand in hand with the necessary respect for the personal data of our citizens, in order to gain their trust and contribute to boosting our economies. In addition to trust, the security of personal information needs to be ensured – in particular when data are stored 'in the cloud'."* [377] Hustinx jako další nezbytný důvod pro aktualizaci právní úpravy uvedl nedostatečnou úroveň harmonizace mezi členskými státy. Rozdíly se nadále prohlubovaly výkladovými odlišnostmi národních dozorových orgánů a soudů. Bylo tak nezbytné sladit právní úpravu na úrovni sekundárního evropského práva s právem

373 Opinion of the European Data Protection Supervisor on the Communication from the Commissionto the European Parliament and the Council on the follow-up of the Work Programme for betterimplementation of the Data Protection Directive (2007/C 255/01), odst. 23 a násl.

374 EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Komplexní přístup k ochraně osobních údajů v Evropské unii, č. KOM(2010) 609. *Evropská komise* [online]. 19 s. [cit. 30. 6. 2020].

375 Srovnej HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 147; Do debaty se zapojila i WP 29, která přispěla inspirativním dokumentem Budoucnost soukromí (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, 28 s. [cit. 30. 6. 2020]).

376 Ibid., s. 148–149.

377 Tento důvod také specificky zmiňuje Viviane Reding, bývalá eurokomisařka pro spravedlnost, která měla probíhající reformu v gesci. Viz REDING, Viviane. The upcoming data protection reform for the European Union. *International Data Privacy Law; Oxford* [online]. 2011, roč. 1, č. 1.

primárním v kontextu změn, které přinesla Lisabonská smlouva.[378] Uvedené problémy byly ve zprávě identifikovány jako natolik zásadní, že bylo nezbytné začít pracovat na komplexní změně právní úpravy osobních údajů.

Citované zdroje se shodují, že hlavním důvodem pro nezbytnou aktualizaci právní úpravy ochrany osobních údajů byl právě technologický vývoj, který nastal od doby přijetí směrnice 95/46/ES v roce 1995, kdy si nikdo nemohl představit dopady a změny, které rychlé a snadné šíření informací přes internet přinese. Prohlubující se mezeru mezi technickou realitou a psanou normou dokázal po určitou dobu překlenout SDEU díky tomu, že ve své rozhodovací praxi využil možností technologicky neutrálního přístupu, na kterém evropský zákonodárce směrnici 95/46/ES postavil. Ukázala to zejména rozhodnutí ve věcech *Bodil Lindqvist*, C-101/01, ve kterém SDEU potvrdil, že zveřejnění osobních údajů online je zpracováním osobních údajů;[379] *Google Spain*, C-131/12, ve kterém bylo rozhodnuto, že provozovatel internetového vyhledávače je správcem osobních údajů indexovaných z dokumentů třetích stran;[380] *Breyer*, C-582/14, ve kterém bylo určeno, že dynamické IP adresy je třeba pokládat za osobní údaje,[381] nebo *Wirtschaftsakademie Schleswig-Holstein*, C-201/16, ve kterém soud uzavřel, že správce fanouškovské stránky na síti Facebook je správce osobních údajů uživatelů, kteří ji využívají.[382] I tato rozhodnutí však ukázala limity směrnice 95/46/ES v podobě její nedostatečné vnitřní škálovatelnosti a granularity povinností správce.

Zastaralost právní úpravy oproti technologickému vývoji a její nevhodnost zejména v kontextu rozvoje zpracování informací (včetně osobních údajů)

---

378 Změna byla nezbytná zejména v kontextu nového čl. 16 Smlouvy o fungování Evropské unie, který mohl nově posloužit jako samostatný právní důvod pro přijetí pravidel sekundárního práva ve všech oblastech unijního práva, a to včetně oblasti bývalého třetího pilíře. Druhou zásadní změnou, kterou Lisabonská smlouva přinesla, bylo ustanovení Listiny základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02) na roveň primárního práva, včetně jejího čl. 8 garantujícího ochranu osobních údajů.

379 Rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01.

380 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

381 Rozsudek Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer*, C-582/14.

382 Rozsudek Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16.

v kyberprostoru kritizovali i další autoři, jako například Christopher Kuner,[383] Paul de Hert,[384] nebo Radim Polčák, který označil za hlavní problém systému ochrany osobních údajů jeho akcent na statický quasi-majetkový přístup k osobním údajům, protože nerespektuje fungování informačních procesů probíhajících zejména v kyberprostoru.[385] Polčák proto přirovnal systém ochrany osobních údajů k Potěmkinově vesnici, která na oko sice vypadá dobře (v textu pěkně napsané normy), ovšem v praxi nefunguje pro své fundamentální nedostatky spočívající v popření informačních principů.[386] Vhodnějším způsobem regulace by dle něj bylo založení absolutních práv k *„souvislostem výskytu osobních údajů, tj. typicky k lidskému soukromí, ke společenské reputaci člověka nebo k veřejnému zájmu"*.[387] Nedomnívám se však, že hlavní problém spočívá v tom, že by docházelo ke konstruování majetkových práv k osobním údajům, protože se tak podle mého názoru minimálně v evropském prostředí neděje.[388] Systém ochrany osobních údajů pracuje s pojmem osobní údaj zejména proto, aby došlo k vymezení věcné působnosti daných právních nástrojů, tedy Obecného nařízení, směrnice 2016/680, zákona 110/2019 Sb. a dalších. Není a nikdy nebylo účelem právní úpravy zpracování osobních údajů vyloučit, ale zajistit jeho korektnost a rovnováhu mezi zájmy na tok údajů na straně správců a ochranou práv a zájmů na straně subjektů údajů. Je proto třeba s Polčákem souhlasit, že při interpretaci norem

383 KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*. 2012, s. 14.

384 De Hert doslova uvádí: *„Practically all basic data protection regulating documents in effect until today have either already been replaced or are in the process of being thoroughly amended. This is probably a development that was long overdue, given that all of them have an age of several decades while none of them has been released taking the internet into account… Directive set the EU and international, through its „adequacy" criterion, data protection standard. However, it remained hopelessly outdated, because it was released before the advent of the Internet."* Viz HERT, Paul de. The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents Editorial. *Utrecht Journal of International and European Law,* 2015, roč. 31, č. 80, s. 1.

385 Viz POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 8 [cit. 30. 6. 2020].

386 POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13, s. 84; POLČÁK, Radim a Dan Jerker B. SVANTESSON. *Information sovereignty: data privacy, sovereign powers and the rule of law*. Cheltenham, UK: Edward Elgar Publishing, 2017, s. 26.

387 POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13, s. 84.

388 K tomu viz výklad v kapitole 2.3 této publikace.

z oblasti ochrany osobních údajů je nezbytné soustředit se proces zpracování jako takový, tedy zpracování osobních údajů probíhající v čase za konkrétním účelem.[389] Omezení zájmu regulace na počátek zpracování (tedy určení účelu, vybrání vhodného právního titulu a sběr dat) by nebyl dostatečný ani z hlediska subjektu údajů, který by jen obtížně mohl realizovat svá práva (a tedy své informační sebeurčení), ale ani z hlediska správce údajů, který musí být schopen dynamicky reagovat na změny, které se mohou v průběhu zpracování objevit.[390]

Hlavním problémem staré právní úpravy zpracování osobních údajů byla nicméně podle mého názoru její nedostatečná flexibilita ve smyslu nedostatečné škálovatelnosti a granularity povinností správce osobních údajů, která se projevovala i v nedostatcích zmíněných v předchozích odstavcích.[391] Škálovatelnost povinností znamená možnost přizpůsobit způsob a míru splnění povinností tak, aby odpovídaly reálným potřebám konkrétního zpracování, tedy skutečné situaci, ve které se správce údajů nachází. Granularita pak značí stav, kdy se určité povinnosti správce začínají nebo přestávají aplikovat v návaznosti na potřeby konkrétní situace. Dohromady vytváří možnost existence různých vrstev, případně variant povinností, které by si opět správce údajů mohl zvolit tak, aby odpovídaly požadavkům reálné situace, ve které správce osobní údaje zpracovává.[392] Taková detailnější rozvrstvenost povinností v bývalé právní úpravě téměř chyběla, s čestnou výjimkou citlivých osobních údajů, jejichž zpracování některé povinnosti přidávalo, a tedy vytvářelo vyšší vrstvu přísnějších požadavků a ochrany. Vzhledem k tomu

389 Viz POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 8 [cit. 30. 6. 2020].

390 Například změna výsledku testu proporcionality prováděného v průběhu identifikace právního titulu zpracování za účelem oprávněného zájmu správce způsobená např. plynutím času. K tomu více viz KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law* [online]. Dordrecht: Springer Netherlands, 2015, [cit. 27. 10. 2016], Law, Governance and Technology Series, 20.

391 Shodně viz např. ERDOS, David. From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection. *Common Market Law Review*, 2015, roč. 52, č. 1, s. 124–125.

392 Pojem „vrstvy povinností" je převzat z SVANTESSON, Dan Jerker B. A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4.

se zejména v kontextu zpracování osobních údajů v prostředí kyberprostoru správci osobních údajů dostávali do situací, ve kterých by splnění povinností, které jim dle zákona náležely, bylo absurdní, technicky nemožné nebo by to po nich vzhledem k povaze daného případu nebylo možné spravedlivě požadovat. V důsledku toho docházelo k situacím, ve kterých správci osobních údajů klidně i po velmi dlouhou dobu zpracovávali osobní údaje *de iure* protiprávně a dozorové orgány v tomto směru nezasahovaly. Pokud bychom na tento stav pohlédli v kontextu Fullerovy Morálky práva, dochází k porušení minimálně dvou z osmi Fullerových požadavků.[393] Vzhledem k tomu byla právní úprava ochrany osobních údajů v době účinnosti směrnice 95/46/ES nefunkční již na své čistě normativní úrovni. Nemohla proto již stačit ani v každodenní aplikaci.

Tato kapitola představuje čtyři příklady zpracování osobních údajů, které ukazují zásadní nedostatky způsobené nedostatečnou granularitou a škálovatelností povinností v systému ochrany osobních údajů v době účinnosti směrnice 95/46/ES. Tyto příklady byly vybrány, protože představují (nebo ve své době představovaly) hraniční případy zpracování osobních údajů, kde přestávala právní úprava prakticky dostačovat, které ale zároveň v kontextu zpracování dat online běžně probíhají. Dobře tak demonstrují výše uvedené nedostatky. Při hodnocení staré pozitivně právní úpravy analyzuji ustanovení směrnice 95/46/ES a zákona č. 101/2000 Sb.

3.1 IP adresy v kybernetické bezpečnosti[394]

Dohledová pracoviště kybernetické bezpečnosti (CSIRT, CERT nebo CIRC, nadále jen „CERT“)[395] jsou důležitým prvkem zajištění kybernetické

393 Právní norma nesmí uložit povinnost přesahující reálné možnosti povinného subjektu a právní normy musí být vymáhány. FULLER, Lon L. *The morality of law*. Rev. vyd. New Haven: Yale University Press, 1978, s. 39; Analýzu systému ochrany osobních údajů v kontextu Fullerova díla dále detailně nabídl Kuner (viz KUNER, Christopher. The 'Internal Morality' of European Data Protection Law. *SSRN Scholarly Paper* [online]. ID 1443797. Rochester, NY: Social Science Research Network. 2008 [cit. 28. 6. 2019]).

394 Tato podkapitola vychází z článků HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, roč. 6, č. 12; a SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security,* 2017, roč. 2017, č. 1.

395 Jedná se o zkratky z anglických termínů *Computer Security Incident Response Team*, *Computer Emergency Response Team* a *Computer Incident Response Capability*.

bezpečnosti ať už veřejnoprávního[396] nebo soukromoprávního subjektu.[397] Obecně se jedná o jakékoli kapacity vyhrazené pro řešení bezpečnostních incidentů a jejich úkolem je chránit definovaný okruh působnosti před hrozbami.[398] Při tom mohou provádět výzkumnou činnost, během které identifikují nové hrozby a vytvářejí vhodná protiopatření. Zároveň se mohou formálně i neformálně sdružovat za účelem spolupráce a předávání poznatků.[399] Jednou z nejpopulárnějších metod, jak získat informace o probíhajících útocích, je využití tzv. honeypotů nebo honeynetů.[400] Název honeypot je odvozen z techniky chytání hmyzu do otevřené nádoby s medem a jeho technologická obdoba funguje analogicky. Honeypot (nebo honeynet v případě, že jde o celou síť honeypotů) je struktura, která je cíleně ponechána k tomu, aby byla kompromitována kybernetickými útoky. Tyto útoky následně může CERT analyzovat a zjistit tak, jaké postupy a nástroje útočník použil. Honeypoty je možné klasifikovat buď dle úrovně interakce,[401] nebo jejich účelu.[402] Činnost honeypotu představuje čtyři základní prvky, kterými jsou kontrola dat (monitorování a logování činnosti útočníka v honeypotu), zachycení dat (kontrola a zachycení aktivity útočníka), sběr dat (uložení všech

396 Například vládní CERT ve smyslu § 20 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. V současné době jde o Národní úřad pro kybernetickou a informační bezpečnost (GovCERT.cz).

397 Například národní CSIRT ve smyslu § 17 zákona č. 181/2014 Sb. V současné době jej provozuje sdružení CZ.NIC (CSIRT.CZ). Může ale jít rovněž o interní týmy zajišťující informační bezpečnost libovolných soukromých společností, vysokých škol a podobně.

398 Více viz HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie*, 2013, roč. 4, č. 8.

399 Příkladem takového sdružení je Shadowserver Foundation.

400 Více k pojmu viz SPITZNER, Lance. *Honeypots: tracking hackers*. Boston: Addison-Wesley, 2003; The Honeynet Project: trapping the hackers. *IEEE Security & Privacy* [online]. 2003, č. 2.

401 Rozlišujeme honeypoty s nízkou mírou interakce, které emulují jen některé vlastnosti operačního systému a sítě, a honeypoty s vysokou mírou interakce, které nabízejí útočníkovi k dispozici kompletní operační systém včetně všech jeho služeb. Viz SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security,* 2017, roč. 2017, č. 1, s. 2; Více informací například WINN, Michael et al. Constructing cost-effective and targetable industrial control system honeypots for production networks. *International Journal of Critical Infrastructure Protection* [online]. 2015, roč. 10.

402 Rozlišujeme výzkumné honeypoty, jejichž účelem je získání maximálního množství informací o útočnících, a produkční honeypoty, které jsou využívány v prostředí chráněného subjektu a pomáhají snížit riziko škody z útoků. Viz SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, 2017, roč. 2017, č. 1, s. 2.

zachycených dat na jednom místě) a analýza dat.[403] Sesbíraná data o kyberbezpečnostních událostech obsahují údaje popisující daný útok, zejména pak IP adresu zařízení, ze kterého byl útok veden.

Při síťovém provozu se zařízení připojují za užití IP adres a při procesu komunikace jsou zaznamenávány adresy jak odesílatele, tak recipienta. Vzhledem k tomu, že již v současné době je k internetu připojeno více zařízení, než nyní primárně používaný systém IPv4 umožňuje, je tento nedostatek vyřešen protokolem NAT („Network Address Translation"). Příkladem zařízení, kde je tento protokol užíván, jsou domácí routery, k nimž je připojeno několik samostatných zařízení. Router má jednu IP adresu, kterou užívá na komunikaci s vnějším světem, a zároveň přiděluje vlastní IP adresy zařízením k němu připojeným. Za jednu veřejnou IP adresou tak může být „ukryto" více zařízení.

IP adresa je série číslic, sloužící k jedinečné identifikaci zařízení připojeného k síti internet. Skládá se ze dvou částí – identifikace sítě, která určuje geografickou lokalizaci sítě, a „Host ID" přesně určující konkrétní zařízení nebo část sítě. Na základě toho, zda je jedna IP adresa trvale přiřazena konkrétnímu zařízení, nebo zda se IP adresa zařízení mění v průběhu času, rozlišujeme ještě statické a dynamické IP adresy. V současné době vzhledem k výše uvedenému nedostatku IP adres při využívání protokolu IPv4 převažují dynamické adresy, které jsou konkrétním zařízením přiděleny ve chvíli, kdy se připojí k internetu. Nová technologie IPv6, která je postupně zaváděna, nabízí řádově větší počet možných současně připojených zařízení, díky čemuž umožní, aby více zařízení mělo statickou IP adresu. Tento stav může mít za následek, že jedno konkrétní zařízení bude dle IP adresy vždy dohledatelné nehledě na to, odkud se připojuje, a bude tak snadnější sledovat pohyb konkrétních zařízení po světě.[404]

IP adresu je třeba považovat za osobní údaj, protože může vést k identifikaci fyzické osoby, a to i přes to, že je IP adresa opravdu vázána k zařízení

403 SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, 2017, roč. 2017, č. 1, s. 2.

404 Viz LAH, Frederick. Online and Locational Privacy: Are IP Addresses "Personally Identifiable Information"? *I/S: A Journal of Law and Policy for the Information Society*, 2008, roč. 4, č. 3, s. 686.

a nikoli k člověku.[405] Aby byla naplněna zákonná definice, musí informace odkazovat na fyzickou osobu, nikoli na technické zařízení. IP adresa je však vzhledem k soukromí velmi specifickou informací, vzhledem k úzkému provázání zařízení, jako je osobní počítač nebo mobilní zařízení, se svým vlastníkem.[406] Je obvyklé, že osobní počítač nebo mobilní zařízení používá právě jedna osoba. Je samozřejmě možné, aby člověk své zařízení půjčil někomu jinému, v praxi však taková situace nastává jen zřídka. Vzhledem k tomu je možné se na uvedenou domněnku spolehnout a pracovat s ní. Pokud jsou ukládány klíčové údaje identifikující zařízení, jako právě jeho IP adresa, IP adresy, na které se dané zařízení připojuje, lokalitu, kde zařízení operuje, a čas, kdy se tak děje, je díky tomu možné poměrně snadno identifikovat, co daná osoba se zařízením dělala, jaké informace hledala a kde se pohybovala. Vezmeme-li výše uvedený příklad se statickou IPv6 IP adresou, můžeme snadno sledovat pohyb osob po celé planetě. Ovšem i v případě dynamických IP adres je možné snadno dojít ke konkrétnímu zařízení a tím i fyzické osobě. Litvinov k tomu říká: *„Internet service providers can determine which subscriber received a particular address and the time at which the address was assigned. Such information has been used to identify individuals for the purposes of imposing criminal liability.“*[407] IP adresa je tak klíčovou nepřímo identifikující informací, esenciální složkou množiny dat, která vede k identifikaci konkrétního člověka. Proto je třeba považovat ji za osobní údaj.[408] Stejný závěr potvrzuje rovněž rozhodovací praxe SDEU, který se otázce povahy IP adresy v kontextu osobních údajů věnoval zejména v rozhodnutí *Breyer*, C-582/14.[409]

405 Viz MCINTYRE, Joshua J. Balancing Expectations of Online Privacy: Why Internet Protocol (ip) Addresses Should Be Protected as Personally Identifiable Information. *DePaul Law Review*, 2011, roč. 60, č. 3, s. 900.

406 Toto konstatuje například WP 29 (PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení. *Evropská komise* [online]. S. 7 [cit. 30. 6. 2020].

407 LITVINOV, Aleksandr V. The Data Protection Directive as Applied to Internet Protocol (IP) Addresses: Uniting the Perspective of the European Commission with the Jurisprudence of Member States. *The George Washington international law review*, 2013, roč. 45, č. 3, s. 584.

408 Ke shodnému závěru dospěl dále např. NONNEMANN, František. IP adresa jako osobní údaj. *Právní rozhledy*, 2017, roč. 25, č. 3.

409 Viz bod 49 rozsudku Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer*, C-582/14. Dále též viz bod 51 rozsudku Soudního dvora Evropské unie ze dne 24. 11. 2011 ve věci *Scarlet Extended*, C-70/10.

Přirozeně existují situace, kdy IP adresa za žádných okolností nemůže být osobním údajem. Jedním příkladem je situace, kdy, jak uvádí Josef Prokeš *„dostupnými nástroji nelze identifikaci provést, zejména pokud jsou údaje uchovávány krátce."*[410] Další možností je fenomén Internet of Things. Jeho principem je připojení velkého množství zařízení, které však nejsou provázány s konkrétním člověkem. Jedná se například o různá čidla monitorující své okolí, elektronické spotřebiče, systémy řídící klimatizaci, a podobně. V takovém případě není možné vytvořit podobnou vazbu mezi zařízením a člověkem jako například v případě mobilních telefonů, nebo osobních počítačů a nemůže se proto jednat o osobní údaje. Protože však není technicky možné na úrovni osoby logující internetový provoz dodatečně odfiltrovat IP adresy zařízení Internet of Things od IP adres mobilních zařízení a osobních počítačů, je třeba ke všem IP adresám přistupovat tak, jako by osobními údaji byly.

Z výše uvedeného vyplývá, že CERT při své práci (například provozování honeypotu) zpracovává osobní údajů a je v pozici správce osobních údajů. IP adresy je třeba považovat za osobní údaje, CERT určuje účel jejich zpracování (například může jít o zajištění bezpečnosti chráněné sítě nebo o analýzu síťového provozu z hlediska kyberbezpečnostních rizik) a činnosti, které se sesbíranými daty provádí, odpovídají vymezení „zpracování osobních údajů".[411] IP adresy jsou sbírány, ukládány, analyzovány a mnohdy předávány třetím stranám (i mimo oblast EU) v rámci dobrovolných sdružení CERT týmů. Není přitom možné spolehnout se na některou z výjimek, které zákon nabízí. Určitě se nejedná pouze o nahodilé shromažďování osobních údajů[412] a v absolutní většině případů ani o zpracování prováděné

410 PROKEŠ, Josef. IP adresa v ochraně osobních údajů. *Data Security Management,* 2014, roč. 2014, č. 4, s. 31.

411 Směrnice 95/46/ES definovala zpracování osobních údajů jako *„jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace"* (Čl. 2 písm. b) směrnice 95/46/ES), definice přítomná v zákoně 101/2000 Sb. pak této definici odpovídala.

412 Dle § 3 odst. 4 zákona č. 101/2000 Sb. se nejednalo o zpracování osobních údajů tehdy, když by se jednalo jen o nahodilé shromažďování osobních údajů za předpokladu, že údaje nebyly dále využívány. Toto ustanovení se však na tento případ vzhledem k dalšímu uchovávání a analýze IP adres nevztahuje.

výlučně pro osobní potřebu správce údajů.[413] Právním titulem pro zpracování osobních údajů je v tomto případě ochrana práv a právem chráněných zájmů správce,[414] protože zásah do práv subjektu údajů je v případě takového zpracování IP adres obecně minimální a žádný jiný právní titul není možné použít.[415]

Fakt, že je CERT správcem osobních údajů, znamená, že musí plnit povinnosti, které vyplývají z relevantních právních předpisů. V tomto případě byla problematická zejména informační povinnost formulovaná v § 11 zákona č. 101/2000 Sb. Dle něj totiž byl správce povinen při shromáždění osobních údajů informovat subjekt údajů o tom, *„v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21"*.[416] Na daný případ při tom nebylo možné aplikovat žádnou z výjimek, které stanovil odst. 3 téhož ustanovení. Naopak, odst. 5 situaci ještě zpřísnil, když stanovil, že *„Při zpracování osobních údajů podle § 5 odst. 2 písm. e)… je správce povinen bez zbytečného odkladu subjekt údajů informovat o zpracování jeho osobních údajů."* Pokud by tedy správce údajů provozující honeypot měl splnit svoji zákonnou povinnost, musel by neprodleně po začátku zpracování (tedy zalogování IP adresy) informovat o probíhajícím zpracování subjekty údajů, což je jednak vzhledem k účelu zpracování jen málo efektivní, ale hlavně zcela technicky nerealizovatelné. Jde o prázdnou povinnost, která je nesplnitelná.

413 Viz čl. 3 odst. 2 směrnice 95/46/ES a § 3 odst. 3 zákona č. 101/2000 Sb. Tím výjimečným případem by byla situace, kdy si člověk sám spustí takový systém pro ochranu své vlastní domácí sítě. Více k úzké interpretaci výjimky pro zpracování pro výlučně osobní potřebu správce viz odst. 46–48 rozsudku Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01; odst. 35 rozsudku Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13; a odst. 51 rozsudku Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17.

414 Viz čl. 7 písm. f) směrnice 95/46/ES a § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

415 Souhlas je samozřejmě zcela neaplikovatelný. Je možné uvažovat možná o plnění zákonné povinnosti v případě vládního CERTu, ale i v tomto případě by dle mého názoru aplikace právního titulu plnění zákonné povinnosti [§ 5 odst. 2 písm. a) zákona č. 101/2000 Sb., čl. 6 odst. 1 písm. c)] nebyla možná, protože zde neexistovala jednoznačně formulovaná povinnost tyto údaje za daným účelem takovým způsobem zpracovávat. Pro upřesnění zbývá dodat, že přesně pro takové případy slouží po změně právní úpravy právní titul zakotvený v čl. 6 písm. e) Obecného nařízení.

416 Viz § 11 odst. 1 zákona č. 101/2000 Sb.

Obdobně byla jen velmi obtížně splnitelná povinnost odpovídající právu subjektu na přístup k údajům o jeho osobě, které bylo založené § 12 zákona č. 101/2000 Sb. Technicky nebylo možné tuto povinnost splnit, pokud by subjekt údajů sám neuvedl, na jakou IP se ptá (včetně časové známky), a zůstává otázkou konkrétního databázového uspořádání, zda by bylo možné osobní údaje poskytnout i pokud by správce údajů věděl, po jaké IP adrese se má dívat. Na správce údajů pak dopadal i taxativní výčet povinností souvisejících se zajištěním zabezpečení osobních údajů podle § 13 zákona č. 101/2000 Sb.[417]

3.2 Rozhodnutí *Google Spain* a jeho následky[418]

Rozhodnutí SDEU ve věci *Google Spain*, C-131/12, je známé zejména díky tomu, že v něm SDEU formuloval tzv. právo být zapomenut,[419] případně tím, že upřesnilo požadavky na místní působnost směrnice 95/46/ES skrze specifikaci pojmu provozovna správce.[420] Aby však k těmto závěrům mohl SDEU dospět, bylo třeba nejprve ustanovit, že společnost provozující internetový vyhledávač je správcem osobních údajů, které indexuje na webových stránkách a dalších dokumentech třetích stran.

Španělskému občanovi Mario Costejovi Gonzálezovi byly na konci devadesátých let z důvodu dluhů na sociálním zabezpečení zabaveny nemovitosti a následně byly dány do veřejné dražby, z jejíhož výtěžku měl být dluh

417 Například požadavek uvedený v § 13 odst. 4 písm. c) spočívající v pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány je v kontextu analýzy kybernetického bezpečnostního incidentu nadbytečný.

418 Tato podkapitola vychází z článku MÍŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie*, Česká advokátní komora, 2015, roč. 2015, č. 1–2.

419 K právu být zapomenut viz např. AUSLOOS, Jef. The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review* [online]. 2012, roč. 28, č. 2; JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016; KRITIKOS, Katie Chamberlain. The Right to Forget, Obliterate, Erase: Defending Personal Data Privacy in the Digital Age. *Journal of Information Ethics,* 2018, roč. 27, č. 2; ZANFIR, Gabriela. Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law*. Dordrecht: Springer Netherlands, 2015.

420 Srovnej například ALSENOY, Brendan Van et al. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?* [online]. Rochester, NY: Social Science Research Network, 2013, s. 20–22 [cit. 30. 6. 2020].

uhrazen.[421] Aby se informace o dražbě dostala k co nejširšímu množství zájemců, regionální deník La Vanguardia splnil povinnost vyvěrající z nařízení ministerstva práce a sociálních věcí a otiskl v lednu a březnu 1998 dva články, v nichž bylo krom oznámení dražby uvedeno i Gonzálezovo jméno.[422] Tyto články byly umístěny do internetového archivu novin a při zadání Gonzálezova jména do internetového vyhledávače Google byly zobrazeny mezi prvními nalezenými výsledky. González tento stav pociťoval jako újmu na svém právu na soukromí a ochranu osobnosti a tvrdil, že vzhledem k tomu, že se jedná o již dávno uhrazené dluhy, není důvod, aby tato informace byla stále snadno veřejně dostupná. Roku 2010 proto podal stížnost ke španělskému Státnímu úřadu pro ochranu údajů proti společnostem La Vanguardia, vydavateli regionálních novin stejného jména, Google Inc. a její lokální dceřiné společnosti Google Spain. Dožadoval se odstranění článků z archívu novin, případně odstranění indexace těchto článků Googlem a tedy znemožnění jejich zobrazení jako výsledku vyhledávání.[423] Státní úřad pro ochranu údajů stížnost zamítl co do publikace článku novinami, jelikož se jednalo o zákonné zveřejnění, ovšem v případě Google stížnosti vyhověl. Google rozhodnutí úřadu napadl žalobou k soudu, který SDEU předložil předběžné otázky týkající se interpretace směrnice o ochraně osobních údajů 95/46/ES. Byť byl Costeja González nakonec úspěšný a Google musel i vlivem rozhodnutí *Google Spain* odkaz na novinový archiv odstranit, stal se obětí tzv. Streisand efektu.[424]

Při řešení otázky, zda je provozovatel internetového vyhledávače správcem osobních údajů, SDEU vycházel převážně z textového výkladu směrnice 95/46/ES, jejíž čl. 2 písm. b) definovalo zpracování osobních údajů jako

421 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain,* C-131/12, bod 14.

422 Ibid., bod 16.

423 Ibid., bod 15.

424 Informační efekt spojený s online prostředím pojmenovaný po americké herečce Barbře Streisand, která se sice soudně domohla smazání fotografie znázorňující její dům, ale díky pohotové reakci uživatelů internetu se předmětná fotografie rozutekla do všech koutů kyberprostoru. Stránka na Wikipedii věnující se Streisand efektu danou fotografii obsahuje (viz WIKIPEDIA. Streisand effect. *Wikipedia.org* [online]; Jiný příklad Streisand efektu uvádí Polčák na příběhu bývalého presidenta Mezinárodní automobilové federace FIA Maxe Mosleyho (POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012, s. 334–335*,* Téma); Více k fenoménu jako takovému viz HAGENBACH, Jeanne a Frédéric KOESSLER. The Streisand effect: Signaling and partial sophistication. *Journal of Economic Behavior and Organization* [online]. 2017, roč. 143.

„jakýkoli úkon nebo soubor úkonů s osobními údaji" a uváděl demonstrativní seznam činností, které je třeba považovat za zpracování osobních údajů.[425] Je to například shromažďování, zaznamenávání, uspořádávání, uchovávání, vyhledávání, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování a další. Tyto činnosti jsou typické pro funkčnost internetového vyhledávače. Obsahem indexování a vyhledávání pak jsou bez pochyby i osobní údaje umístěné na webových stránkách a v dokumentech třetích stran. Jak je uvedeno v rozsudku: *„Vzhledem k tomu, že uvedené úkony jsou výslovně a bezpodmínečně uvedeny v čl. 2 písm. b) směrnice 95/46, musí být kvalifikovány jako ‚zpracování' ve smyslu uvedeného ustanovení"*.[426] Provozovatel internetového vyhledávače určuje účel tohoto zpracování (indexování pro funkčnost systému vyhledávání a následné řazení výsledků) a byl proto nezbytně vyhodnocen správcem těchto údajů ve smyslu směrnice 95/46/ES a tedy i zákona 101/2000 Sb.[427] Byť bylo rozhodnutí SDEU v tomto směru oprávněně průlomové, nebylo to poprvé, co tento názor zazněl. WP 29 označila provozovatele internetového vyhledávače za správce osobních údajů ve svém stanovisku již v roce 2008.[428] Stanovisko se však o zpracování osobních údajů získaných indexací dokumentů třetích stran zmiňuje jen okrajově, když na s. 14 uvádí: *„Formální, právní a praktická kontrola vyhledávače nad dotčenými osobními údaji je obvykle omezena na možnost odstranění údajů ze svých serverů. Pokud jde o odstranění osobních údajů z jejich výsledků indexování a vyhledávání, vyhledávače mají dostatečnou kontrolu tak, aby mohly být v takových případech považovány za správce."*[429] Je pochopitelné, že SDEU musel dospět k tomuto závěru, protože bez něj by zbytek případu nemohl být rozhodnut tak, jak byl, následkem čehož by byla snížena úroveň ochrany práv subjektů údajů (což je v rozporu se zásadami a cíli právní úpravy osobních údajů). Na druhou stranu v konečném důsledku určení provozovatele internetového

425 Věcně se stará právní úprava nikterak neliší od úpravy v Obecném nařízení.

426 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12, bod 28.

427 Ibid., bod 41. Tento argument SDEU posílil poznámkou, že internetové vyhledávače ovlivňují, jak informace vnímáme, a umožňují snadno sestavit na základě jména profil člověka (body 37–38 rozhodnutí).

428 PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 1/2008 k otázkám ochrany údajů v souvislosti s vyhledávači. *Evropská komise* [online]. 4. 4. 2008, 29 s. [cit. 30. 6. 2020].

429 Ibid., s. 14.

vyhledávače za správce indexovaných údajů způsobilo několik zásadních systematických problémů, které nebyly nikterak adresovány. Pokud je provozovatel internetového vyhledávače správcem osobních údajů, znamená to opět, že by měl plnit povinnosti, které mu právní úprava ukládá.

Aby mohl správce údajů se zpracováním začít, potřebuje mít vhodný právní titul. Vzhledem k tomu, že vyhledávač pracuje s nepředstavitelným množstvím osobních údajů předem neznámých subjektů, je třeba vyloučit zpracování na základě souhlasu nebo z důvodu plnění smlouvy. Sám SDEU v rozhodnutí *Google Spain* označil za aplikovatelný právní titul oprávněný zájem správce nebo třetích osob dle čl. 7 písm. f) směrnice 95/46/ES.[430] Tím oprávněným zájmem, o který se zpracování opírá, je pak krom ekonomického zájmu provozovatele internetového vyhledávače rovněž zájem na fungování internetu jako komunikačního prostředku a právo na informace a ochrana svobody projevu jeho uživatelů,[431] protože bez funkčního vyhledávače by byla práce s internetem fakticky znemožněna. V kontextu staré právní úpravy bylo možné ještě uvažovat o právním titulu zpracování oprávněně zveřejněných osobních údajů,[432] mezi které spadaly například údaje zveřejněné v rámci žurnalistické činnosti, případně subjektem údajů samotným.[433] Při plošném zpracovávání informací celého internetu však není možné zajistit, aby takto nebyly zpracovány i nezákonně zveřejněné osobní údaje.

---

430 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12, bod 73.

431 Společenský zájem na fungujícím internetu je možné demonstrovat například rozhodovací činností ESLP, kdy soud přiznává důležitost připojení k internetu jako zásadního prostředku pro šíření informací a zajištění svobody slova a přístupu k informacím (např. viz rozsudek Evropského soudu pro lidská práva ze dne 28. 9. 1999 ve věci *Öztürk vs. Turecko*, stížnost č. 22479/93; a rozsudek Evropského soudu pro lidská práva ze dne 18. 12. 2012 ve věci *Ahmet Yildirim vs. Turecko*, stížnost č. 3111/10). Rovněž Ústavní soud judikoval o zásadní roli, kterou hraje možnost připojení k internetu v kontextu práva na informace, svobody projevu a širšího práva na informační sebeurčení jako takového (viz nález Ústavního soudu ze dne 7. 4. 2010, sp. zn. I.ÚS 22/10, č. N 77/57 SbNU 43). Více k problematice připojení k internetu jako rašícího základního práva viz např. FIALOVÁ, Eva. Právo na přístup k internetu. *Právník*, 2018, roč. 157, č. 7.

432 Tento právní titul byl českým specifikem, který neměl ve směrnici 95/46/ES oporu a český zákonodárce pomocí něj vyřešil otázku zpracování osobních údajů v kontextu zpravodajství a medií (viz POSPÍŠIL, Daniel. § 5 odst. 2 písm. d) a e). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 143, Beckova edice komentované zákony).

433 Ibid., s. 143.

Hlavní problém však nastal v případě zpracování citlivých osobních údajů. Na webových stránkách a dalších dokumentech třetích osob se bez pochyby nacházejí rovněž citlivé osobních údaje,[434] které provozovatelé internetových vyhledávačů zpracovávají jejich indexací a nabídkou ve svých aplikacích. Zákon č. 101/2000 Sb. však ve svém § 9 nenabízel žádnou možnost, která by jejich zpracování umožnila a kterou by bylo možné aplikovat na situaci internetových vyhledávačů. Veškeré zpracování citlivých osobních údajů umístěných na webových stránkách třetích stran tak bylo nezákonné a vyhledávač by je měl ukončit. Vzhledem k tomu, že nebylo v tomto případě technicky možné oddělit zpracování citlivých a necitlivých údajů, měly zpracováním osobních údajů (a tedy nabízením vyhledávací služby) skončit úplně. Absence právního titulu pro zpracování citlivých osobních údajů ve smyslu § 9 zákona č. 101/2000 Sb. tak učinila činnost všech internetových vyhledávačů spadajících do jurisdikce států EU nelegální.

Proti uvedenému závěru se nabízí argument, že provozovatel internetového vyhledávače se nachází v pozici odpovídající poskytovateli služeb informační spolčenosti typu hosting, protože nakládá s obsahem třetích osob.[435] Tuto interpretaci je však třeba vyloučit, protože směrnice 2000/31/ES ze své působnosti čl. 1 odst. 5 písm. b) explicitně vylučuje otázky týkající se ochrany osobních údajů.[436] Krom toho, striktně vzato, argumentace SDEU je věcně správná. Internetový vyhledávač není jen pasivním přenašečem dat. Jeho provozovatel aktivně určuje způsob, jak bude indexování fungovat,

434 Čl. 8 směrnice 95/46/ES je vymezoval jako *„údaje, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního života"*, § 4 písm. b) zákona 101/2000 Sb. pak následovně *„citlivým údajem* [se rozumí] *osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů"*. Koncept v zásadě odpovídá zvláštním kategoriím osobních údajů ve smyslu čl. 9 Obecného nařízení.

435 Viz čl. 14 směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) a § 5 zákona č. 480/2004 Sb., o některých službách informační společnosti.

436 Více srovnej ALSENOY, Brendan Van et al. *Search Engines after "Google Spain": Internet@ Liberty or Privacy@Peril?* [online]. Rochester, NY: Social Science Research Network, 2013, s. 60–61 [cit. 30. 6. 2020]. Shodně též LYNSKEY, Orla. Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *Modern Law Review* [online]. 2015, roč. 78, č. 3, s. 533.

jak dlouho bude indexovaná data uchovávat, jak často je bude aktualizovat a v neposlední řadě, v jakém pořadí je po aplikaci personalizačního algoritmu bude nabízet svým uživatelům. Problém nespočíval v označení provozovatele vyhledávače za správce údajů, ale v tom, že na tuto eventualitu již právní úprava směrnice 95/46/ES nestačila.

Podobně jako v případě týmů CERT a jejich zpracování IP adres bylo v době účinnosti zákona 101/2000 Sb. a směrnice 95/46/ES i v případě provozovatelů internetových vyhledávačů vysoce problematické a technicky fakticky neřešitelné splnění informační povinnosti správce údajů. Je jen velmi obtížně představitelné, jak by takové informování mělo vzhledem k nespecifikovanému (a neurčitelnému) počtu neznámých subjektů údajů vypadat. Možným řešením by snad mohlo být oznámení na webových stránkách vyhledávače, které by však svojí nezbytnou obecností[437] působilo spíše komicky než jakkoli užitečně. Stejně tak problematické je splnění povinnosti odpovídající právu subjektu na přístup k osobním údajům dle § 12 zákona 101/2000 Sb. Správce má povinnost na žádost sdělit, jaké údaje zpracovává a jakými způsoby. I zde je praktická implementace problematická. Pravděpodobně jediný možný způsob, jak zjistit, jaké údaje vyhledávač indexováním zpracovává, je zadání jména a zobrazení výsledků. Aby však byla zákonná povinnost řádně splněna, měl by subjekt údajů mít přístup ke svým osobním údajům v podobě, která není zatížena jeho preferencemi ve vyhledávání a personalizací ze strany vyhledávače. Krom toho by měl být vyhledávač schopný odfiltrovat záznamy další – týkající se osob stejného jména. Obojí je však technicky jen velmi obtížně proveditelné.

3.3 Hypertextové odkazy jako zpracování osobních údajů[438]

Třetí příklad uvedený v rámci této kapitoly je hraničním příkladem aplikace právního rámce ochrany osobních údajů. Tato podkapitola se zabývá povahou hypertextového odkazu (označovaného rovněž jako hyperlink nebo jen

437 Mohlo by vypadat např. následovně: „Informujeme Vás o tom, že pokud se Vaše osobní údaje nacházejí na námi indexovaných stránkách, zpracováváme je za účelem poskytování služeb vyhledávače."

438 Text této podkapitoly vychází z kapitoly MÍŠEK, Jakub. Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing). In: SVANTESSON, Dan Jerker B. a Dariusz KLOZA (eds.). *Trans-Atlantic data privacy relations as a challenge for democracy*. Cambridge, Antwerp, Portland: Intersentia, 2017, s. 331–346.

link) ve světle ochrany osobních údajů. Otázka, kterou řeší, je, zda linkování je (nebo může být) zpracováním osobních údajů nacházejících se v cílovém dokumentu, případně zda hypertextový odkaz sám nespadá pod definici osobního údaje. Hypertextový odkaz je metoda odkazování užívaná v informačních technologiích, v kontextu tohoto textu mám na mysli zejména v prostředí internetu. Hypertextový odkaz je tvořen kotvou, kterou představuje určité místo ve zdrojovém dokumentu, ze kterého je možné odkaz následovat,[439] a adresou, která určuje cílový dokument nebo jeho konkrétní část. Kotva hypertextového odkazu může být uživateli skrytá, ale většinou je nějakým způsobem typograficky zvýrazněná. Cílová adresa je oproti tomu obvykle ukrytá ve zdrojovém kódu webové stránky.

Cílovým dokumentem se rozumí konkrétní dokument, ke kterému hypertextový odkaz vede. Jedná se zejména o případy takzvaných „hlubokých odkazů" („deep hyperlink"), které cílí na konkrétní dokumenty, než o odkazy cílící na domovskou stránku webu. Důležitý je přitom obsah cílového dokumentu, nikoli dokument samotný, protože dokument nelze považovat za osobní údaj.[440] Mějme jako příkladný cílový dokument webovou stránku paní Lindqvist, která na ní zveřejnila informace o svých osmnácti kolezích včetně úplných jmen, zaměstnání a koníčků. Hypertextový odkaz na tuto webovou stránku by mohl být osobním údajem, nebo by alespoň představoval zpracování osobních údajů na stránce uvedených. Pokud by stránka obsahovala rovněž údaje o zdraví, případně o náboženském vyznání,[441] představovalo by linkování na ni zpracování citlivých osobních údajů.

Je třeba předeslat, že analyzovaná záležitost není čistě akademickým problémem, ale má praktické dopady například v oblasti právní úpravy informací veřejného sektoru a otevřených dat. Nejvyšším kvalitativním stupněm otevřených dat jsou tzv. „propojená data" („linked data"),[442] která fungují na principu přímého propojování více databází odkazy mezi nimi a jejich

439 Může se jednat o řetězec znaků, obrázek, nebo klidně celý dokument jako v případě webové stránky, která automaticky přesměruje uživatele na jinou webovou stránku.

440 Viz bod 48 rozsudku Soudního dvora Evropské unie ze dne 17. 7. 2014 ve věci *YS a další,* C-141/12; Obdobně též rozsudek Nejvyššího soudu ze dne 16. 9. 2015, sp. zn. 30 Cdo 3629/2014, č. 55/2016 Sb.NS.

441 V původním případě tomu tak opravdu bylo, viz bod 13 rozsudku Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01.

442 BERNERS-LEE, Tim. *5*Open Data* [online].

jednotlivými prvky.[443] I na nižších stupních však dochází k propojování různých databází obsahujících osobní údaje. Pokud například tvůrce aplikace postavené na otevřených datech data z volně dostupného rejstříku neukládá, ale pouze je ve své aplikaci zobrazuje v aktuální podobě z daného rejstříku, děje se tak prostřednictvím odkazu. Určení, zda je odkaz na zdroj obsahující osobní údaje jejich zpracováním, je tak v kontextu otevřených dat zcela zásadní.

Jak ukázala kapitola 2.4 této publikace, při interpretaci pojmů obsažených ve směrnici 95/46/ES (nebo v Obecném nařízení) je třeba vycházet z prevenčního principu a postupovat tak, aby byla zachována vysoká úroveň ochrany práv a zájmů subjektu údajů. Z toho vyplývá, že definiční pojmy, které zajišťují aplikaci právní úpravy, je třeba vykládat maximálně široce a naopak, veškeré výjimky maximálně úzce.[444] Při analýze charakteru hypertextového odkazu z hlediska ochrany osobních údajů *de lege lata* vycházím proto z uvedených principů a respektuji praxi SDEU, která je pro správnou interpretaci zásadní.

Prvně se zaměříme na variantu, že by hypertextový odkaz mohl být sám osobním údajem, protože odkazuje na dokument jiné osobní údaje obsahující. Rozhodovací praxe SDEU v tomto případě pomůže jen omezeně. Ukázala sice, zejména rozhodnutím ve věci *Breyer*, že pojem osobní údaj je třeba vykládat velice široce, konkrétně otázkou hypertextového odkazu v kontextu osobních údajů se však Lucemburský soud zatím nezabýval.[445] Jako interpretační pomoc může být použito stanovisko WP 29 k pojmu

443 K propojeným datům více viz např. SCHAIBLE, Johann et al. Linking Study Descriptions to the Linked Open Data Cloud. *IASSIST Quarterly,* 2014, roč. 38/39, č. 4/1.

444 Viz část. 2.4 této publikace.

445 SDEU nabízí poměrně bohatou rozhodovací praxi k hypertextovým odkazům a jejich působení z hlediska autorského práva. Hlavní otázkou postupně řešenou již v několika rozhodnutích je, zda odkázání na dílo představuje užití tohoto díla sdělováním veřejnosti (viz rozsudek Soudního dvora Evropské unie ze dne 13. 2. 2014 ve věci *Svensson,* C-466/12, a další; rozsudek Soudního dvora Evropské unie ze dne 21. 10. 2014 ve věci *BestWater International*, C-348/13; a rozsudek Soudního dvora Evropské unie ze dne 8. 9. 2016 ve věci *GS Media*, C-160/15). Mám za to, že i přes určitou faktickou blízkost užití díla hypertextovým odkazem a zpracování osobních údajů skrze stejnou technologii není možné z rozhodovací praxe SDEU v této oblasti příliš vycházet za použití pouhé analogie. Hlavním důvodem je přílišná rozdílnost pozitivní právní úpravy spočívající zejména v tom, že v případě osobních údajů není třeba jakkoli uvažovat o požadavku „nové veřejnosti", tak jako v případě sdělování díla veřejnosti. Zveřejnění osobního údaje nikterak nezakládá výjimku nebo úlevu v případě jeho dalšího (jiného) zpracování.

osobní údaj (č. 4/2007), které byť je již staršího data, je stále s drobnými výhradami použitelné vzhledem k tomu, že se základní koncept osobních údajů nezměnil, ačkoli došlo v průběhu času k jeho judikaturnímu rozšíření. WP 29 detailně popsala definici osobních údajů pomocí čtyř prvků: i) „veškeré informace", ii) „o" (vztah mezi informacemi a osobou), iii) „identifikovaná nebo identifikovatelná" a iv) „fyzická osoba",[446] které jsou v uvedeném stanovisku dále detailně rozebrány. Pojem informace je dle WP 29 chápan velice široce, jako libovolný typ informací, bez ohledu na jejich formu a povahu.[447] Druhý prvek, tedy vztah mezi informací a osobou, WP 29 rozkládá na tři alternativní faktory, a sice prvek „obsahu",[448] prvek „účelu"[449] nebo prvek „výsledku".[450] Třetí prvek pokrývá otázku identifikovatelnosti konkrétní fyzické osoby, protože aby se jednalo o osobní údaje, musí být pomocí nich osoba přímo nebo nepřímo identifikovatelná. Právě tento aspekt se dotýká problému anonymizace a byl jako hraniční řešen v kontextu IP adres SDEU v rozhodnutí ve věci *Breyer*, které potvrdilo požadavek na širokou interpretaci pojmu.[451] Čtvrtý prvek, který uvádí, že se musí jednat o fyzickou osobu, pak není třeba více rozebírat.

Hypertextový odkaz naplňuje všechny čtyři znaky osobních údajů uváděné ve stanovisku WP 29.[452] Mám však za to, že závěr, že hypertextový odkaz mířící na dokument obsahující osobní údaje je sám osobním údajem, je nepřesvědčivý i přes nezbytnost širokého výkladu zkoumaného pojmu.

446 PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 4/2007 k pojmu osobní údaj. *Evropská komise* [online]. 20. 6. 2007, s. 6 [cit. 30. 6. 2020].

447 Ibid., s. 6–7.

448 Ibid., s. 9. „Prvkem obsahu" WP 29 míní případy, kdy *„se informace podávají o konkrétní osobě, a to bez ohledu na jakýkoli účel, který sleduje správce údajů nebo třetí osoba, nebo na dopad těchto informací na subjekt údajů."* Jde tedy o situace, jak chápeme „informace o někom" v běžné mluvě.

449 Ibid. Pod „prvkem účelu" WP 29 rozumí údaje, jejichž účelem, za *„kterým se používají nebo pravděpodobně budou používat, je hodnotit jednotlivce, zacházet s ním určitým způsobem nebo ovlivnit jeho postavení či chování."*

450 Ibid., s. 11. Prvek výsledku je zbytkovou kategorií pro případy, kdy chybí prvek obsahu a účelu, ale přesto bude mít použití dané informace dopad na subjekt údajů, byť by byl minimální.

451 Jde o problém tzv. subjektivního a objektivního přístupu k osobním údajům. Více je mu věnována následující kapitola této publikace.

452 Jde o informace, která se *de facto* vztahuje k fyzické osobě, o níž je pojednáváno v cílovém dokumentu, a daná osoba je identifikovatelná právě využitím této informace (kliknutím na odkaz a přejitím na cílovou adresu).

Těžko si totiž lze představit situaci, že by se jeden osobní údaj vztahoval k více fyzickým osobám, což by se mohlo stát, pokud by na cílové stránce byly osobní údaje více osob. Bez pochyby existují případy, kdy hyperlink osobním údajem bude, jako například v situaci, kdy odkaz nebude mířit na jiný dokument, ale obsahuje emailovou adresu. V tomto případě je možné připomenout starší českou rozhodovací praxi, dle které je informace osobním údajem i tehdy, když je pomocí ní možné fyzickou osobu kontaktovat.[453] Nejde však o příklad odpovídající původnímu zadání (tedy odkaz je osobním údajem proto, že míří na dokument s osobními údaji), ale pouze o technicky obohacenou variantu emailové adresy. Z uvedeného vyplývá, že závěr o povaze odkazu jako osobního údaje neobstojí.

Jiná situace však nastane, pokud budeme odkaz hodnotit jako zpracování osobních údajů na cílové stránce. Směrnice 95/46/ES definovala zpracování osobních údajů jako *„jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace“*.[454] Česká implementace v podobě zákona č. 101/2000 Sb. evropskému předobrazu věcně odpovídala s výjimkou toho, že obsahovala požadavek, aby zpracování bylo systematické, tedy nikoli nahodilé.[455] Podobně jako v případě definice osobního údaje je nezbytné vykládat pojem zpracování široce. Obecně se jedná o jakoukoli činnost, kterou správce údajů s osobními údaji provádí. V kontextu analyzovaného problému je třeba upozornit na to, že v rámci

453 Srovnej zejména rozsudek Nejvyššího správního soudu ze dne 12. 2. 2009, č. j. 9 As 34/2008-68, č. 1844/2009 Sb.NSS, s. 5; dále pak např. rozsudek Nejvyššího správního soudu ze dne 29. 7. 2009, č. j. 1 As 98/2008-148, č. 1944/2009 Sb.NSS; a rozsudek Nejvyššího správního soudu ze dne 14. 8. 2014, č. j. 1 As 78/2014-41, č. 3127/2014 Sb.NSS, odst. 18.

454 Viz čl. 2 písm. b) směrnice 95/46/ES.

455 Viz § 4 písm. e) zákona č. 101/2000 Sb.; Rozdíl mezi evropskou a českou úpravou precizně komentuje NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; Výslovně formulovaný požadavek na systematičnost již nenalezneme v definici obsažené v Obecném nařízení, které odpovídá směrnici 95/46/ES (viz čl. 4 odst. 2 Obecného nařízení).

demonstrativního výčtu možností zpracování údajů, je výslovně uvedeno jejich šíření nebo jakékoli jiné zpřístupnění.

Správcem osobních údajů mám v uvažovaném příkladě na mysli toho, kdo hypertextový odkaz vytvoří a určí tak účel zpracování osobních údajů, kterým je jejich zobrazení v cílovém zařízení po aktivaci odkazu.[456] SDEU k povaze zpracování osobních údajů v bodě 28 rozhodnutí ve věci *Google Spain,* C-131/12, uvádí: *„automatickým, neustálým a systematickým prohlížením internetu za účelem vyhledávání tam zveřejněných informací provozovatel vyhledávače ‚shromažďuje' takové údaje, které ‚vyhledává', ‚zaznamenává' a následně v rámci svých programů indexování ‚uspořádává', ‚uchovává' na svých serverech a případně ‚sděluje' a ‚zpřístupňuje' svým uživatelům ve formě seznamů výsledků jejich vyhledávání. Vzhledem k tomu, že uvedené úkony jsou výslovně a bezpodmínečně uvedeny v čl. 2 písm. b) směrnice 95/46, musí být kvalifikovány jako ‚zpracování' ve smyslu uvedeného ustanovení, aniž je důležité, zda vyhledávač používá tytéž úkony rovněž na další druhy informací a nerozlišuje mezi nimi a osobními údaji."*[457] SDEU v citovaném odstavci výslovně zmiňuje, že osobní údaje přítomné na jiných stránkách internetu jsou sdělovány a zpřístupňovány uživatelům vyhledávače ve formě seznamu výsledků vyhledávání. Seznam výsledků není nic jiného než seznam hypertextových odkazů, které míří na cílové dokumenty obsahující osobní údaje. Citovaná argumentace Soudního dvora nabízí interpretaci, že SDEU v tichosti přiznal užití hypertextového odkazu status zpracování osobních údajů přítomných v odkazovaných dokumentech. Je proto důležité prozkoumat, jaká je vazba jednotlivých kroků, o kterých SDEU hovoří, a zda jsou na sobě závislé, nebo nikoli.

Propojíme-li životní cyklus dat zpracovávaných vyhledávačem s pojmy, které obsahuje směrnice č. 2 písm. b) 95/46/ES a které SDEU použil ve výše citovaném odstavci, můžeme je pak porovnat s prostým linkováním. Když internetový vyhledávač indexuje dokument obsahující osobní údaje *A*, tak je nejprve prostřednictvím web crawlerů „vyhledává" a „shromažďuje"

456 Uživatel internetové stránky, který na odkaz klikne, nemůže být správcem o nic víc než uživatel internetu, který si zobrazuje stránky s osobními údaji. I kdybychom v rámci široké interpretaci přiznali, že dočasné ukládání obsahu stránek do paměti počítače, aby mohly být zobrazeny na monitoru, je zpracováním osobních údajů, bude se na takové případy aplikovat výjimka zpracování pro osobní potřebu.

457 Bod 28 rozsudku Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

a následně „zaznamenává" tak, že ukládá jejich kopii na své servery. Tuto kopii označím jako *A'*. Všechny takto získané kopie jsou rozděleny do slov, která jsou „uspořádána" do rejstříku a „uchována" takovým způsobem, aby vyhledávač mohl určit zdroj jejich původu. Když uživatel zadá do vyhledávače svůj dotaz, dojde k prohledání databáze, ve které se nachází kopie *A'*. Na základě tohoto kroku vyhledávač určí původní zdroj a nabídne uživateli seznam hypertextových odkazů, čímž mu osobní údaje „sděluje" a „zpřístupňuje". Je třeba upozornit na to, že takto zpřístupňované jsou původní osobní údaje *A*, a nikoli *A'*. Uživatel nikdy nevidí, jak vypadá vnitřní pracovní kopie dat, která zajišťuje chod vyhledávacího algoritmu. Výsledkem je tedy hypertextový odkaz, který má za cíl dokument s osobními údaji *A*. V tomto směru se „sdělování" a „zpřístupňování" nikterak technicky neliší od prostého hypertextového odkazu. Z rozhodnutí SDEU ve věci *Google Spain*, C-131/12, tak (byť nepřímo) vyplývá, že prostý hypertextový odkaz může v případech, kdy se v cílovém dokumentu nachází osobní údaje, představovat zpracování těchto údajů.

Na první pohled by se mohlo zdát zvláštním, že by za správce byla označena osoba, i když nemá faktický přístup k osobním údajům, které zpracovává. Rozhodovací praxe SDEU však takový stav připouští minimálně v kontextu společných správců,[458] zejména pak v rozhodnutí ve věci *Jehovan todistajat / Svědkové Jehovovi,* C-25/17.[459] SDEU v tomto rozhodnutí připomněl, že široká interpretace pojmu správce osobních údajů je nezbytná, protože jejím cílem je *„zajistit účinnou a úplnou ochranu subjektů údajů"*.[460] Zároveň však dodává, že všichni zúčastnění společní správci nemohou nést stejnou míru odpovědnosti za probíhající zpracování, protože ji nesou jen v míře

458 Směrnice 95/46/ES výslovně společné správcovství neupravovala, nicméně možnost existence takového uspořádání vyplývala z definice správce údajů obsažené v čl. 2 písm. d), dle kterého je správcem údajů osoba, která sama nebo společně s jinými určí účel zpracování. Směrnice nevyžadovala, na rozdíl od Obecného nařízení, žádnou formální úpravu vztahu společných správců. Více viz PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel". *Evropská komise* [online]. 16. 2. 2010, s. 17–23 [cit. 30. 6. 2020].

459 Viz rozsudek Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17; Dále rovněž viz rozsudek Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16; a rozsudek Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci *Fashion ID*, C-40/17.

460 Bod 66 rozsudku Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17.

odpovídající jejich zapojení.[461] Závěr, že tvůrce hypertextového odkazu je společným správcem osobních údajů přítomných v cílovém dokumentu spolu s provozovatelem cílové webové stránky, se jeví být v souladu se současnou interpretací směrnice 95/46/ES Soudním dvorem. Tvůrce hypertextového odkazu totiž určuje nový účel a způsob zpracování již zpracovávaných osobních údajů, a právě za tuto činnost může nést odpovědnost. Uvedená konstrukce by však byla problematická z hlediska staré české úpravy, protože zákon č. 101/2000 Sb. koncept společných správců ze směrnice 95/46/ES nepřevzal.[462] Stejně tak v kontextu Obecného nařízení již tato interpretace není udržitelná, protože zde nedochází k žádné domluvě mezi tvůrcem původního obsahu a tvůrcem odkazu, což však Obecné nařízení v čl. 26 vyžaduje.

Na druhou stranu, pro interpretaci, že vytvoření hypertextového odkazu je zpracováním osobních údajů, pak hovoří rovněž argument účelem právní úpravy ochrany osobních údajů. Tou je ochrana práv subjektů údajů a je možné se plně odkázat na rozhodovací praxi SDEU, jak v kontextu právě citovaných rozhodnutí zabývajících se povahou správce údajů, tak opět na rozhodnutí ve věci *Google Spain*. V něm soud zdůraznil, že rozšiřování prostřednictvím vyhledávače je samostatným zpracováním nezávislým na účelech a zákonnosti zveřejnění na původní stránce. Pokud dochází druhým zpracováním do zásahu práv subjektu údajů, pak musí mít možnost se proti takovému zásahu bránit. Je jisté, že v kontextu prostého linkování je dopad zpracování na subjekt údajů nesrovnatelně nižší než v případě internetového vyhledávače. Avšak i tehdy může dojít k zásahu do práv a zájmů subjektu údajů (nebo jejich ohrožení) a není možné takové případy přejít. Jiná a výrazně závažnější situace pak může nastat při použití technologie hypertextového odkazu pro propojování databází obsahujících osobní údaje v kontextu propojených dat. Z pragmatického hlediska jsou pak nástroje ochrany osobních údajů nezbytné, protože je jejich výkon efektivnější než v případě

461 Viz body 43–44 rozsudku ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16; bod 66 rozsudku ve věci *Jehovan todistajat*, C-25/17; a bod 70 rozsudku ve věci *Fashion ID*, C-40/17.

462 Srovnej NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: ASPI [Právní informační systém, text aktuální k 1. 7. 2017]; Komentář od Kučerové et al. zmínku o společných správcích neobsahuje pak vůbec (KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, Beckova edice komentované zákony).

např. ochrany soukromí vzhledem k tomu, že není nutné prokazovat vznik-lou újmu, ale stačí fakt, že např. správce údajů nemá právní titul pro jejich zpracování.[463] Vzhledem k tomu mám za to, že hypertextový odkaz je možné považovat za zpracování osobních údajů i přes výše uvedené výhrady.

Určité možné východisko se nabízelo v případě, že bychom tvrdili, že osobní údaje na odkazované stránce jsou zpracovávané nahodile.[464] V takovém případě se však situace komplikovala, protože by bývalo nutné v případě hodnocení zpracování odkazovaných osobních údajů hodnotit úmysl tvůrce odkazu, tedy zda vytvořil odkaz jako takový za účelem zpracování těchto údajů (a v takovém případě by byl správcem údaje), a nebo je to vedlejší efekt.

Pokud bychom přijali použití hypertextového odkazu jako hraniční případ zpracování osobních údajů,[465] rázem získáme řadu problémů z hlediska možnosti plnění povinností, které správci údajů přísluší. Řadu povinností souvisejících s právy subjektu na přístup k údajům nebo jejich opravu nebude možné aplikovat, protože s osobními údaji na stránce třetí strany nemůže tvůrce odkazu nijak nakládat (pokud budeme uvažovat o variantě společného správcovství, pak tvůrce odkazu za tyto prvky procesu zpracování nemůže odpovídat). Právním titulem pro zpracování by byl stejně jako v případě rozhodnutí *Google Spain* oprávněný zájem správce, kterým by byl například výkon práva na svobodu projevu. Technicky nemožné, případně nesmírně obtížné (v závislosti na charakteru osobních údajů na cílové stránce) by bylo plnění informační povinnosti a je nejasné, jak by splnil povinnost zabezpečení údajů a zpracování vyplývající z § 13 zákona č. 101/2000 Sb. Již zcela absurdní je představa, že by se takový správce údajů měl registrovat u ÚOOÚ, jak vyžadovala bývalá právní úprava. Uvedené následky zní natolik nepředstavitelně, že by se mohlo zdát logickým závěrem interpretaci hyperlinku jako zpracování osobních údajů vyloučit. Ve světle účelu právní úpravy ochrany osobních údajů a vývoji rozhodovací praxe SDEU mám však za to, že to není možné.

463 K tomu srovnej nedávné rozhodnutí Royal Courts of Justice, Strand, London zde dne 8. 10. 2018, sp. zn. [2018] EWHC 2599 (QB).

464 Viz § 4 písm. e) zákona č. 101/2000 Sb.

465 V kontextu českého práva v době účinnosti směrnice 95/46/ES a zákona 101/2000 Sb. by ještě myslím bylo možné vyloučit většinu takových případů s odkazem na to, že se jedná o nahodilé zpracování osobních údajů.

3.4 Anonymizace a otevřená data

Otevřená data představují nejefektivnější způsob, jak mohou orgány veřejné správy poskytovat informace veřejného sektoru.[466] Na rozdíl od práva na informace realizovaného prostřednictvím žádostí, které má charakter politického práva a jeho cílem je zajištění transparentnosti výkonu veřejné správy,[467] jsou otevřená data způsobem poskytování informací zveřejněním tak, aby bylo maximálně umožněno jejich další využití a nesou proto silný ekonomický aspekt a cíle.[468] Otevřenými daty se rozumí poskytování informací online ve strojově čitelném[469] a otevřeném formátu[470] s minimální mírou omezení jejich dalšího užití.[471] Principem otevřených dat je umožnit veřejnosti co nejjednodušší přístup k datům veřejného sektoru, aby nad nimi mohly vznikat nové aplikace a objevila se pro ně nová využití.

Jako otevřené mohou být poskytovány rovněž datové sady obsahující osobní údaje, což samozřejmě kvůli snadné možnosti zneužití dat znamená potenciálně nejrizikovější způsob zveřejňování informací o fyzických osobách.[472] V kontextu českého práva je pro poskytování osobních údajů

466 Kvalitní přehledová meta-analýza studií věnovaných otevřeným datům viz SAFAROV, Igbal, Albert MEIJER a Stephan GRIMMELIKHUIJSEN. Utilization of open government data: A systematic literature review of types, conditions, effects and users. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2017, roč. 22, č. 1.

467 Tradičně je spojováno s právem na svobodu projevu. Viz podrobně MOLEK, Pavel. *Politická práva*. 1. vyd. Praha: Wolters Kluwer, 2014, s. 29–107.

468 Shodně viz POLČÁK, Radim. Structure and Proportionality of Fundamental Rights in PSI Re-use. *Masaryk University Journal of Law and Technology,* 2013, roč. 6, č. 3, s. 383.

469 Zákon č. 106/1999 Sb. definuje v § 3 odst. 7 strojově čitelný formát jako *„formát datového souboru s takovou strukturou, která umožňuje programovému vybavení snadno nalézt, rozpoznat a získat z tohoto datového souboru konkrétní informace včetně jednotlivých údajů a jejich vnitřní struktury."* Jde tedy například o tabulkový soubor typu .XCL nebo .CSV, nikoli však o .PDF obsahující obrázky nascanovaných tabulek.

470 Zákona č. 106/1999 Sb. definuje v § 3 odst. 8 otevřený formát jako *„formát datového souboru, který není závislý na konkrétním technickém a programovém vybavení a je zpřístupněn veřejnosti bez jakéhokoli omezení, které by znemožňovalo využití informací obsažených v datovém souboru"*. Příkladem je soubor typu .TXT .CSC a .XLSX, nikoli však již staré .XCL.

471 Této definici odpovídá i zákonná definice v § 3 odst. 11 zákona č. 106/1999 Sb., která však navíc obsahuje ještě povinnost registrace v Národním katalogu otevřených dat. Více viz MÍŠEK, Jakub. Data veřejného sektoru. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 372–377.

472 Proti této praxi se proto silně vyjádřil zvláštní zpravodaj OSN pro právo na soukromí ve své zprávě z roku 2017 (Report of the Special Rapporteur on the right to Privacy, ze dne 19. 10. 2017, s. 16–17 [cit. 30. 6. 2020]).

jako otevřených dat zapotřebí jasně formulovaná zákonná povinnost tento proces provádět, protože bez ní by poskytovatel dat neměl vhodný právní titul, který by pro takové zpracování mohl použít.[473] Tuto roli plní § 4b odst. 2 zákona č. 106/1999 Sb. prováděný nařízením vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data. Toto nařízení ve své příloze obsahuje výčet informací, které mají dotčené úřady povinnost zveřejňovat jako otevřená data a nalezneme mezi nimi rovněž řadu databází obsahujících osobní údaje. Jde tak například o datové sady ze systému ARES (Administrativní registr ekonomických subjektů) vedený Ministerstvem financí, který obsahuje informace z veřejných rejstříků,[474] případně o metadata k registru smluv.[475]

Pokud taková data chce používat tvůrce aplikace pro svůj projekt, který pak bude nabízet koncovým uživatelům, stává se nutně správcem osobních údajů, protože určuje účel jejich zpracování. Tento účel nesmí být spekulativní a obecný, není tedy možné zpracovávat údaje za účelem „jejich užití v aplikaci", ale je třeba specifikovat, proč údaje budou v aplikaci využité.[476] Právním titulem pro zpracování osobních údajů tvůrcem aplikace může být oprávněný zájem správce nebo třetí osoby podle čl. 6 odst. 1 písm. f) Obecného nařízení, pokud dané zpracování projde interním testem proporcionality,[477] ve výjimečných specifických případech pak zvláštní právní titul pro zpracování v kontextu novinářské výjimky dle § 17 zákona č. 110/2019 Sb.[478] V době před účinností Obecného nařízení se správce údajů mohl spolehnout ještě na právní titul zpracování oprávněně zveřejněných

473 K problematice poskytování a opětovného užití otevřených dat s osobními údaji detailně viz MÍŠEK, Jakub. *Právní aspekty otevřených dat*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019, s. 96–131.

474 Bod 19 přílohy k nařízení č. 425/2016 Sb.

475 Ibid., bod 22.

476 Více k tomu srovnej stanovisko WP 29 zabývající se principem limitace účelem. Viz PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 3/2013 o limitaci účelem. *Evropská komise* [online]. 2. 10. 2013, 70 s. [cit. 30. 6. 2020].

477 Shodně viz NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. *Právní rozhledy*, 2018, roč. 26, č. 5.

478 Takovým případem by mohla být například aplikace Hlídač státu kombinující data z registru smluv, obchodního rejstříku, transparentních účtů politických stran a hnutí a další za účelem zvýšení transparentnosti a kontroly výkonu veřejné správy. Více viz MÍŠEK, Jakub. *Právní aspekty otevřených dat*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019, s. 126–129.

osobních údajů dle § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., Obecné nařízení však tento právní titul neobsahuje. Tvůrce aplikace samozřejmě musí plnit všechny povinnosti, které mu vyplývají z právní úpravy ochrany osobních údajů. Stejně jako v jiných příkladech uvedených v této kapitole bylo dle staré právní úpravy problematické zejména splnění informační povinnosti v případě subjektů údajů, k jejichž kontaktním údajům tvůrce aplikace často ani neměl přístup.

Situace při poskytování otevřených dat se může nečekaně výrazně zkomplikovat v případě, že jsou publikovány datové sady obsahující anonymizované osobní údaje, zejména pokud jde například o statistické údaje z oblasti zdravotnictví. Anonymizace je proces zpracování osobních údajů, jehož účelem je nevratně zamezit možnosti identifikace subjektu údajů.[479] Anonymizovaná data tak přestávají být osobními údaji.[480] Povinný subjekt je proto dle zákona č. 106/1999 Sb. může volně zveřejnit na základě vlastního rozhodnutí,[481] a příjemce otevřených dat s nimi může volně pracovat, aniž by se musel ohlížet na pravidla ochrany osobních údajů. Příkladem aplikace, která zajímavě pracuje s anonymizovanými daty veřejného sektoru (byť se nejednalo o otevřená data ale o data získaná na základě žádosti), je Mapa exekucí, která na základě anonymizovaných dat Exekuční komory umožňuje zobrazit počty lidí v exekucích v různých věkových kategoriích a počty exekucí na hlavu až na úroveň jednotlivých obcí.[482]

Směrnice 95/46/ES přistupovala k anonymizaci duálně. Data jsou anonymizovaná a potom nejde o osobní údaje, nebo data nejsou anonymní a pak se právní režim ochrany osobních údajů musí aplikovat. Tento přístup však příliš neodpovídá skutečnému provádění anonymizace, která je spíše

479 PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 5/2014 k technikám anonymizace. *Evropská komise* [online]. 10. 4. 2014, s. 6 [cit. 30. 6. 2020].

480 Viz bod 26 odůvodnění směrnice 95/46/ES, případně bod 26 odůvodnění Obecného nařízení.

481 Viz § 5 odst. 7 zákona č. 106/1999 Sb., který dává v souladu se zásadou publicity veřejné správy povinným subjektům diskreci poskytovat jakékoli informace, pokud to zákon neomezuje (k zásadě publicity veřejné správy srovnej KORBEL, František. *Svobodný přístup k informacím podle zákona č. 106/1999 Sb. – vybrané problémy*. Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, 2005, s. 14. Možnost zvolit jako způsob publikace otevřená data pak vyplývá z § 4b odst. 1 zákona č. 106/1999 Sb.

482 Viz M*apa exekucí* [online]. [cit. 30. 6. 2019].

procedurální aplikací různých anonymizačních technik.[483] To souvisí se základním nedostatkem procesu anonymizace spočívající v nepřímé úměře mezi informativní hodnotou, tedy mírou užitečnosti dat a anonymitou subjektů údajů. Paul Ohm ve své studii precizně ukázal, že neexistuje dokonalá anonymizace, která by vyloučila možnost opětovné identifikace a zároveň zachovala informační hodnotu předmětných dat.[484] Na tomto stavu se podepsal zejména rozvoj informačních technologií a možnost efektivně propojovat různé datové zdroje. V kontextu otevřených dat pak toto riziko platí ještě silněji, protože jejich vlastností a cílem je propojování s jinými datovými podklady.

Právě uvedené ukazuje hlavní problém, který zpracování anonymizovaných otevřených dat přináší tvůrcům aplikací. V průběhu zpracování těchto dat, tedy v době, kdy aplikace je nějakým způsobem naprogramovaná a funguje bez toho, aby její autor bral ohledy na ochranu osobních údajů (protože nemusel), může dojít k deanonymizaci datové sady, se kterou aplikace pracuje. Tvůrce aplikace se tak dostává do pozice správce údajů a musí plnit všechny povinnosti, které mu z ní vyplývají. V důsledku by to nejspíše znamenalo nutnost zásadní přestavby předmětné aplikace nebo až konce nabízené služby. A to i přestože by míra zásahu do práv subjektu údajů nebo riziko jeho vzniku bylo minimální. Směrnice 95/46/ES a zákon 101/2000 Sb. neobsahovaly žádné úlevy a výjimky pro takové případy a stavěly správce do často neřešitelných situací.

3.5 Shrnutí kapitoly

Technologický vývoj dospěl dál, než si zákonodárce při tvorbě směrnice 95/46/ES dokázal představit. Do jisté míry tento nedostatek dokázal překonat SDEU, když přistoupil k intepretaci definičních ustanovení směrnice rozšiřujícím způsobem. Zajistil tak, že se právní úprava osobních údajů dále

483 Přehledně se jim věnuje výše citované stanovisko WP 29 č. 5/2014, k technikám anonymizace. Příkladem jedné z často využívaných technik je k-anonymita (viz např. SAMARATI, Pierangela a Latanya SWEENEY. *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression*. 1998; SWEENEY, L. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems* [online]. 2002, roč. 10, č. 5).

484 OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 2009, roč. 57, č. 6.

vztahovala i na případy, kdy to bylo vzhledem k okolnostem oprávněné, ale na které nebyla původně nachystána. Výsledkem bylo, že se správce údajů zejména v kontextu zpracování osobních údajů v kyberprostoru mohl snadno dostat do situace, ve které nebylo možné splnit povinnosti, které mu právní úprava ukládala, nebo ve které by bylo plnění těchto povinností vzhledem k povaze případu zjevně neproporcionální zátěží. Důvodem tohoto stavu byla nedostatečná vnitřní granularita a škálovatelnost povinností vyplývajících ze směrnice a zákona č. 101/2000 Sb.

V případě prvního příkladu zpracování IP adres v kontextu kybernetické bezpečnosti právní úprava po správci údajů požadovala, aby informoval subjekty údajů, byť to nebylo technicky možné. Dále měl správce povinnost splnit za účelem zabezpečení osobních údajů konkrétní v zákoně vyjmenované povinnosti, které však v daném kontextu byly zcela nadbytečné. V případě druhého příkladu, kdy se jednalo o zpracování osobních údajů provozovatelem internetového vyhledávače, byl jako hlavní problém identifikován fakt, že právní úprava neobsahovala možnost, jak takové zpracování legálně provádět, protože správce údajů nemohl aplikovat žádnou z výjimek umožňujících zpracování citlivých osobních údajů. Třetí příklad spočíval ve zpracování osobních údajů prostřednictvím hypertextového odkazu. Takové zpracování může v konkrétních případech představovat zásah do práv subjektů údajů, a proto je vhodné, aby měl například možnost aplikovat na něj svá práva. Na druhou stranu takřka jakékoli jiné povinnosti správce jsou vzhledem k povaze takového zpracování nesplnitelné anebo nepřiměřené. Konečně, čtvrtý případ se věnoval anonymizovaným údajům a poukázal na nedostatky plynoucí z časové fixace zpracování do bodu jeho počátku. V průběhu zpracování může například dojít k částečné opětovné identifikaci, čímž se z daných dat opět stanou osobní údaje. V takové situaci by měl podle bývalé právní úpravy správce údajů začít zcela naplňovat všechny povinnost, které mu právní úprava předepsala, a to i přes to, že vzhledem k povaze takového zpracování zásah do práv subjektů údajů prakticky nehrozil.

4 ZÚŽENÍ INTERPRETACE DEFINIČNÍCH POJMŮ A NEVYMÁHÁNÍ POVINNOSTÍ

Třetí kapitola této publikace představila zásadní systematické problémy, kterým čelila bývalá právní úprava ochrany osobních údajů v podobě směrnice 95/46/ES a na ní navazujícího zákona 101/2000 Sb. V hraničních případech, které přinesl technologický pokrok, vyžadovala právní úprava po správcích údajů povinnosti, které byly vzhledem k danému případu zpracování osobních údajů zjevně nepřiměřené, nebo rovnou zcela nesplnitelné. Bylo tomu tak z důvodu nedostatečné flexibility směrnice 95/46/ES a jejích národních implementací, které neumožnily zavedení odpovídající škálovatelnosti a granularity povinností správce. Následkem toho bylo možné vysledovat dva praktické způsoby řešení, které se objevily ve snaze vyrovnat se s tímto nedostatkem. Prvním z nich je zúžení definic klíčových pojmů ochrany osobních údajů (zejména osobní údaj) tak, aby na problematické případy právní úprava ochrany osobních údajů nedopadla. Druhý způsob spočívá v rozhodnutí orgánu dozoru nevymáhat na správcích osobních údajů povinnosti, které z takto problematických zpracování vyplývají. Tato kapitola se postupně zabývá oběma zmíněnými způsoby a hodnotí jejich aplikovatelnost a správnost z hlediska premis představených v první kapitole (v prvním případě) a obecné právní úpravy a právních zásad (v druhém případě).

4.1 Objektivní a subjektivní přístup k osobním údajům[485]

Jak už bylo naznačeno v kapitole 3 této publikace, Obecné nařízení nabízí v zásadě totožnou definici pojmu osobní údaj jako směrnice 95/46/ES. Osobní údaje jsou tedy *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě“*.[486] Ustanovení pak dále uvádí, že identifikovanou nebo identifikovatelnou osobou je taková fyzická osoba, kterou lze přímo či nepřímo identifikovat.[487] Přímou identifikací je myšlen takový proces, kdy k identifikaci subjektu údajů stačí právě daná informace sama o sobě (například rodné číslo

485 Text této podkapitoly vychází z publikovaného článku HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, roč. 6, č. 12.

486 Viz čl. 4 odst. 1 Obecného nařízení.

487 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 4/2007 k pojmu osobní údaj. *Evropská komise* [online]. 20. 6. 2007, 26 s. [cit. 30. 6. 2020].

osoby). O nepřímou identifikaci se jedná tehdy, kdy je pro určení subjektu údajů třeba spojit dohromady více informací, které samy o sobě danou osobu přímo neidentifikují. Jinými slovy, pokud je možné za pomoci dané informace vytvořit takový kontext, ve kterém bude možné identifikovat fyzickou osobu, jedná o osobní údaj. Definice osobního údaje je díky tomuto vymezení nesmírně široká. Tento mohutný rozsah potvrzuje i bod 26 odůvodnění Obecného nařízení, který stanoví: *„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.“*[488] Výhodou takto širokého vymezení je jeho technologická neutralita. Ať se identifikující informace nachází v jakékoli formě, dopadá na ni režim zákonné úpravy ochrany osobních údajů.

Šíře rozsahu aplikace tohoto ustanovení je dána zejména díky možnosti nepřímé identifikace. Kupříkladu Obecné nařízení oproti směrnici 95/46/ES výslovně zavedlo pojem pseudonymní údaje, kterými se myslí takové osobní údaje, které nemohou být přiřazeny konkrétnímu subjektu údajů bez dodatečných informací.[489] Pseudonymizace je však pouze způsob zvýšení úrovně technického zabezpečení zpracování, protože i pseudonymní data jsou stále osobní údaje. Je tomu tak právě díky možnosti nepřímé identifikace, tedy přiřazení dodatečných informací. V případě, že již je opětovné ztotožnění subjektu údajů nemožné, Obecné nařízení hovoří o anonymních údajích.[490] Na anonymizované údaje, které již dále nejsou osobní údaje, protože je není možné použít k identifikaci fyzické osoby ani nepřímo, právní úprava ochrany osobních údajů na ně nedopadá. Anonymizace je tak vhodný postup, jak zajistit, že správce osobních údajů přestane být správcem a bude s daty moci dále nakládat bez jakéhokoli zákonného omezení.[491] Problém

488 Bod 26 odůvodnění Obecného nařízení.

489 Srovnej čl. 4 odst. 5 Obecného nařízení. Více též MOURBY, Miranda et al. Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2.

490 Bod 26 odůvodnění Obecného nařízení.

491 Více k anonymizaci viz BALBONI, Paolo a Milda MACENAITE. Privacy by design and anonymisation techniques in action: Case study of Ma3tch technology. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 4; COLLINGWOOD, Lisa. Privacy, anonymity and liability: Will anonymous communicators have the last laugh? *Computer Law & Security Review* [online]. 2012, roč. 28, č. 3; DARIES, Jon P. et al. Privacy, Anonymity, and Big Data in the Social Sciences. *Communications of the ACM* [online]. 2014, roč. 57, č. 9; SWEENEY, L. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems* [online]. 2002, roč. 10, č. 5.

nastává tehdy, kdy anonymizace není provedena dostatečně precizně nebo se vlivem vývoje možností výpočetní techniky časem objeví nové možnosti ztotožnění údajů. V takovém případě se totiž opět jedná pouze o pseudonymní údaje. Jako příklad můžeme uvést notoricky známý případ Netflix. Společnost Netflix poskytovala službu online půjčování filmů a následně zveřejnila statistiky toho, jak její uživatelé hodnotili sledované filmy. Byly uveřejněny následující informace: jméno filmu, hodnocení v rozsahu jedné až pěti hvězdiček a datum hodnocení. Tato data byla stále svázána na jednoho člověka, byť byly přímé identifikační údaje z datové sady odstraněny. Nedlouho poté, co ke zveřejnění došlo, bylo prokázáno, že postačuje, aby člověk znal přesné hodnocení šesti netradičních filmů, aby dokázal jedinečně identifikovat 84 % uživatelů. K přesné identifikaci 99 % uživatelů pak stačilo vědět přibližné datum (v rozmezí dvou týdnů) ohodnocení šesti filmů, nehledě na to, zda byly netradiční, nebo obecně známé.[492]

Uvedený příklad ukazuje, že je vhodné o anonymizaci osobních údajů uvažovat nikoli jako o dvou stupních „anonymní" a „neanonymní", ale jako o škále, která vyjadřuje zároveň obtížnost opětovné identifikace, kdy na jedné straně stojí přímo identifikující údaje a na straně druhé zcela anonymní statistická data. Tento fakt reflektovali Paul Schwartz s Danielem Solove, když ve svém textu navrhovali vymezení více definičních kategorií (identifikující, nepřímo identifikující a anonymní údaje), kterým měly být přiřazeny odpovídající povinnosti jako podmínka pro jejich zpracování.[493] Škála identifikovatelnosti je vhodným vyjádřením problému anonymizace i z hlediska vyjádření informační hodnoty daného datasetu. Čím jsou totiž údaje anonymnější, tím méně informace nesou.

Obecné nařízení s identifikovatelností rovněž pracuje jako se škálou, byť není tak návodné jako Schwartzův a Soloveho text. K určení hranice – místa na škále anonymizace – kde se nachází kvalitativní zlom mezi osobními údaji a anonymními daty, napomáhá opět odůvodnění Obecného nařízení, když uvádí, že *„Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci*

492 Srovnej OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 2009, roč. 57, č. 6, s. 1721.

493 Viz SCHWARTZ, Paul M. a Daniel J. SOLOVE. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 2011, roč. 86, č. 6, s. 1877 a násl.

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."[494] Uvedené se samozřejmě netýká jen osobních údajů, které prošly procesem anonymizace. Vyjádření bodu 26 odůvodnění Obecného nařízení se vztahuje na otázku identifikovatelnosti obecně.

Možnost vyloučení určitých informací ze zpracování osobních údajů je podmíněna tím, že v daném případě není možné rozumně předpokládat, že by mohly být použity k opětovné identifikaci. Interpretační zúžení definičního rozsahu pojmu údaj (tedy argumentace, že v daném případě není subjekt údajů identifikovaný nebo identifikovatelný) je přímý způsob, jak pro daný případ dosáhnout vyloučení aplikace právních předpisů upravujících ochranu osobních údajů. Příklady takové argumentace přináší texty Patricka Lundevall-Ungera[495] a Eneken Tikk[496] věnované povaze IP adres z hlediska ochrany osobních údajů. K výslovně zužující interpretaci pojmu osobní údaj pak přistoupil například NSS v rozsudku č. j. 1 As 98/2008-148. Jednalo se v něm o zpracování osobních údajů zanesených v knize návštěv na policejní stanici v rozsahu datum a čas příchodu a odchodu, jméno a číslo občanského průkazu návštěvy.[497] NSS dospěl k závěru, že se nejedná o osobní údaje, protože *„za osobní údaj však zdejší soud nepovažuje ani jméno a příjmení osoby (návštěvníka) ve spojení s číslem jeho občanského průkazu. Ani na základě těchto údajů totiž není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla průkazu. Navíc v případě čísla občanského průkazu se jedná o označení, které je v průběhu času proměnlivé. Fyzická osoba totiž neobdrží jedno číslo občanského průkazu na celý život, nýbrž při každé výměně tohoto průkazu získává průkaz s číslem novým.*"[498]

494 Bod 26 odůvodnění Obecného nařízení. Citovaný výňatek je rozpracováním textu, který byl přítomný již ve směrnici 95/46/ES, jejíž bod 26 odůvodnění uváděl jen požadavek, že *„pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby"*.

495 LUNDEVALL-UNGER, Patrick a Tommy TRANVIK. IP Addresses – Just a Number? *International Journal of Law and Information Technology* [online]. 2011, roč. 19, č. 1.

496 TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken a Anna-Maria TALIHÄRM (eds.). *International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.

497 Viz s. 11 rozsudku Nejvyššího správního soudu ze dne 29. 7. 2009, č. j. 1 As 98/2008-148, č. 1944/2009 Sb.NSS.

498 Ibid.

Ke stejnému závěru s totožnou argumentací pak došel NS v rozsudku ve věci sp. zn. 21 Cdo 367/2015.[499]

Uvedené případy spojuje, že k definici osobních údajů přistupují zužujícím subjektivním přístupem, při kterém se možnost ztotožnění subjektu údajů hodnotí pouze z pozice daného konkrétního správce osobních údajů. Subjektivní přístup k osobním údajům je možné vymezit následovně. Pokud má předmětná informace takovou povahu, že neidentifikuje subjekt údajů přímo, a zároveň se nedá rozumně předpokládat, že by daná osoba měla možnost získat další informaci, která by způsobila, že by mohlo dojít k nepřímé identifikaci (byť by objektivně existovala), není zkoumaná informace považována za osobní údaj a nedopadá na ni proto Obecné nařízení.[500] V protikladu vůči subjektivnímu pojetí osobních údajů leží pojetí objektivní. V tomto přístupu nezáleží na konkrétních možnostech a schopnostech osoby, která zrovna informacemi disponuje. Pokud někde objektivně existuje jiná informace, která může posloužit k vytvoření nezbytného kontextu pro opětovnou identifikaci subjektu údajů, je první zkoumaná informace osobním údajem a dle toho je nezbytné k ní přistupovat.

Subjektivní přístup k osobním údajům představuje v kontextu systému ochrany osobních údajů nežádoucí zúžení interpretace klíčového pojmu osobních údajů, a tedy omezení dopadu právní úpravy ochrany osobních údajů. V případě, že bychom pojem osobních údajů interpretovali subjektivně, znamenalo by to, že pokud daný správce nemůže sám ztotožnit subjekt údajů, může s daty nakládat, jak se mu zlíbí, včetně například volné publikace online. To může představovat zásadní riziko pro práva a zájmy subjektů údajů, protože jak ukázal případ Netflix, moderní výpočetní technologie výrazně usnadňují propojování informací do nových kontextů. Vzhledem k tomu je nezbytné k osobním údajům přistupovat z pozice extenzivního objektivního přístupu.[501] Nezbytnost

499 Rozsudek Nejvyššího soudu ze dne 17. 12. 2015, sp. zn. 21 Cdo 367/2015, č. 45/2017 Sb.NS.

500 K problému subjektivního a objektivního přístupu k osobním údajům viz též NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*, 2015, roč. 23, č. 12.

501 K nezbytnosti širokého vymezení pojmu osobní údaje shodně též HERT, Paul de a Vagelis PAPAKONSTANTINOU. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 183; PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* [online]. 2018, roč. 10, č. 1, s. 42.

široké intepretace pak vyplývá rovněž přímo z účelů práva na ochranu osobních údajů textu Obecného nařízení[502] i rozhodovací praxe SDEU.[503] Vrátíme-li se zpět k problematice anonymizace, je tradičním problémem plynutí času a riziko budoucího opětovného ztotožnění, které je podmíněno neočekávatelným technickým vývojem.[504] Jakmile jsou data jednou zveřejněna, je velmi obtížné je z internetu odstranit. Pokud bychom k osobním údajům přistupovali subjektivně, mohlo by to opět znamenat snížení ochrany subjektu údajů, protože by mohla nastat situace, kdy už existuje taková technologie, která umožňuje opětovnou identifikaci, ale kterou třeba původní správce nedisponuje, a proto by se pro něj nejednalo o osobní údaje. Subjekt údajů by v takovém případě neměl možnost, jak dosáhnout ochrany svých práv. Objektivní přístup tento nedostatek postihuje a nutí správce údajů patřičně reagovat.

K objektivnímu přístupu k osobním údajům se přihlásil i SDEU v rozsudku ve věci Breyer.[505] Ačkoli je toto rozhodnutí známé zejména díky tomu, že v něm soud explicitně potvrdil a odůvodnil, že dynamickou IP adresu je potřeba považovat za osobní údaj, obsahuje rovněž detailnější popis toho, co znamená identifikovatelnost. V případu se jednalo o IP adresy, které zaznamenával a uchovával poskytovatel online mediálních služeb. Ten sám neměl možnost přímo IP adresy k identifikaci subjektů údajů využít. Chybějící střípek, který by propojení umožnil, měli k dispozici poskytovatelé služeb elektronických komunikací. SDEU odmítl subjektivní přístup k osobním údajů, když s odkazem na bod 26 odůvodnění směrnice 95/46/ES uvedl: *„Jelikož tento bod odůvodnění odkazuje na prostředky, které mohou být rozumně použity jak správcem, tak ‚jakoukoli jinou osobou', znění tohoto bodu odůvodnění nasvědčuje tomu, že aby určitý údaj mohl být kvalifikován jako ‚osobní údaj' ve smyslu čl. 2 písm. a) uvedené směrnice, není požadováno, aby se všechny informace umožňující identifikovat subjekt údajů musely nacházet v rukách jediné osoby."*[506] SDEU se tak přihlásil k objektivnímu přístupu, který ovšem mírně limitoval požadavkem,

502 Viz požadavek na zajištění vysoké úrovně ochrany osobních údajů uvedený v bodech 6 a 10 odůvodnění Obecného nařízení.

503 Srovnej část 2.4 této knihy.

504 Srovnej NARAYANAN, Arvind, Joanna HUEY a Edward W. FELTEN. A Precautionary Approach to Big Data Privacy. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, s. 357–485.

505 Rozsudek Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer,* C-582/14.

506 Ibid., bod 43.

že proces ztotožnění subjektu údajů musí být rozumně předpokládatelný. Soud dodává, že se možnost nepřímé identifikace nevztahuje na situace, kdy by byla identifikace subjektu údajů protiprávní nebo prakticky neproveditelná, protože by vyžadovala nepřiměřené úsilí nebo náklady.[507] Tato svrchní limitace, kterou SDEU jednoznačně identifikoval, je nesmírně důležitá, protože zamezuje absurdním důsledkům, které by bezbřehý objektivní přístup k osobním údajů mohl přinést, jako například situace, kdy by všechny informace mohly být osobním údajem.

Objektivní přístup k osobním údajů je podmíněn nezbytností extenzivního výkladu definičních pojmů v rámci systému ochrany osobních údajů. Obdobně je třeba přistupovat i k pojmu zpracování osobních údajů. Zatímco bývalá právní úprava v podobě zákona č. 101/2000 Sb. obsahovala výjimku z působnosti předpisu v podobě nahodilého zpracování,[508] Obecné nařízení takovou výslovnou výjimku neobsahuje a je třeba jej aplikovat na veškeré procesy nakládání s osobními údaji, které probíhají za pomoci zcela nebo částečně automatizovaných prostředků.[509] Vzhledem k tomu si můžeme jen obtížně představit situaci, ve které je s osobními údaji nakládáno za využití jakékoli moderní technologie, která by zároveň nespadala pod působnost Obecného nařízení.[510] Na základě právě uvedeného se domnívám, že není možné, aby se naopak restriktivní přístup k těmto pojmům (osobní údaj, zpracování osobních údajů, správce osobních údajů) stal základem řešení problémů, které byly nastíněny ve třetí kapitole této knihy.

507 Ibid., bod 46.

508 Viz § 3 odst. 4 zákona č. 101/2000 Sb.

509 Viz čl. 2 odst. 1 Obecného nařízení. Ohledně absentující výslovné výjimky nahodilého zpracování autorský kolektiv komentáře k Obecnému nařízení uvádí následující: *„S ohledem na definici zpracování osobních údajů jako do velké míry systematické činnosti vykonávané za určitým účelem však nahodilé, neúmyslné získání osobních údajů, které nebudou nijak dále využívány, do působnosti Nařízení rovněž nebude spadat."* (NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Dostupné z: ASPI [Právní informační systém]. Souhlasím s nimi, že požadavek určité systematičnosti do značné míry vyplývá přímo z podmínky stanovení účelu zpracování. Na druhou stranu se však domnívám, že rychlé shrnutí této změny do jedné věty není dostatečné a zasloužilo by hlubšího prozkoumání. Tato otázka však již leží za hranicí této publikace a nechávám ji tak otevřenou dalšímu výzkumu.

510 Shodně hodnotí s odkazem na Christophera Kunera též Orla Lynskey (viz LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 584–585).

4.2 Nevymáhání práva

Za doby účinnosti předchozí právní úpravy se pokoušely dozorové orgány ochrany osobních údajů vypořádat s problémy právní úpravy nastíněnými ve třetí kapitole této publikace rovněž druhým způsobem. Tím bylo rozhodnutí nevymáhat problematické praktiky, které sice dle litery zákona porušovaly pravidla ochrany osobních údajů, ale z nějakého více či méně dobrého pragmatického důvodu je bylo třeba zachovat v chodu. Je možné uvést hned několik takových případů, z nichž většina byla zmíněna ve třetí kapitole této knihy.

Pracoviště kybernetické bezpečnosti zpracovávaly IP adresy, tedy osobní údaje zaznamenané v průběhu monitorování činnosti na kontrolovaných sítích. Předchozí právní úprava nenabízela žádnou výjimku z informační povinnosti správce údajů, kterou by bylo možné na takové situace aplikovat. Přesto – nepodařilo se mi objevit jediný případ, kdy by tato praxe byla sankcionována, nebo alespoň označena za nevhodnou.

Výraznějším příkladem mohou být internetové vyhledávače, které indexují na stránkách třetích stran citlivé osobní údaje a pak je nabízejí svým uživatelům jako výsledky vyhledávání. Pro zpracování citlivých osobních údajů však provozovatelé internetových vyhledávačů neměli vhodný právní titul, protože žádná z možností, kterou nabízel čl. 8 směrnice 95/46/ES,[511] se na danou situaci nemohla aplikovat.[512] Pokud by dozorové úřady postupovaly dle psaného práva, musely by dojít k závěru, že provozovatelé internetových vyhledávačů neplní své povinnosti správce a náleží jim proto odpovídající sankce. Žádná sankce však nepřišla. Pragmatickým argumentem zřejmě bylo, že internetové vyhledávače hrají v moderní společnosti důležitou roli pro umožnění práva na informace a svobodu projevu.[513]

Nejzásadněji se však tendence nevymáhat vybrané povinnosti vyplývající z předpisů ochrany osobních údajů projevila jako následek rozhodnutí

511 Odpovídal mu § 9 zákona č. 101/2000 Sb.

512 Pokud členský stát nevyužil výjimku obsaženou v čl. 8 odst. 4 směrnice 95/46/ES. Řada členských států, včetně České republiky, tak ale neučinila.

513 Srovnej shodně rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

SDEU ve věci *Schrems*.[514] SDEU v říjnu 2015 prohlásil za neplatné rozhodnutí Komise č. 2000/520, které vytvářelo rámec pro tzv. Bezpečný přístav předávání osobních údajů do Spojených států amerických. Evropská právní úprava ochrany osobních údajů obecně zapovídá předávání osobních údajů mimo oblast Evropské unie a Evropského hospodářského prostoru, ledaže by se správce údajů mohl spolehnout na některou z výjimek, které právní úprava nabízí.[515] Jednou z těchto výjimek je rozhodnutí Komise o adekvátnosti úrovně ochrany osobních údajů ve třetí zemi.[516] Rozhodnutí Komise č. 2000/52 pak umožnovalo předávání osobních údajů správcům údajů ve Spojených státech, kteří se zapsali do seznamu a tím deklarovali, že dodržují úroveň ochrany odpovídající evropskému standardu. V rozhodnutí ve věci *Schrems* SDEU nejprve zdůraznil, že je nezbytné provádět pravidelné kontroly faktického stavu ochrany osobních údajů ve třetí zemi ze strany Komise, jestliže Komise vydala rozhodnutí umožňující předávání dat.[517] Soud dále připomněl interpretační striktnost, která je nutná vždy, když jsou v evropské ochraně osobních údajů aplikovány jakékoli výjimky. Na základě zhodnocení skutečného stavu, kdy například mohly být veškeré údaje předávány americkým bezpečnostním a informačním složkám,[518] pak rozhodnutí Komise č. 2000/520 zrušil. Tento krok odůvodnil právě faktickou nedostatečnou úrovní ochrany osobních údajů ve Spojených státech amerických.

Po zrušení bezpečného přístavu nastalo právní vakuum, kdy Evropská komise začala okamžitě jednat o zavedení nového systému předávání osobních

514 Viz rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2015 ve věci *Schrems*, C-362/14. Uvědomuji si, že tento případ neřešil přímo otázku škálovatelnosti povinností správce nebo šíře interpretace definičních ustanovení (byť v kontextu předávání údajů do zahraničí a extrateritoriality evropských předpisů je možné o tomto tématu rovněž uvažovat, jak ukazuje např. SVANTESSON, Dan Jerker B. A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4). Důvod, proč tento případ uvádím, je, že se jedná o nejkřiklavější ukázku praxe nevymáhání určitých povinností správců údajů, která nebyla výjimečná.

515 Detailně k tématu viz KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford, New York: Oxford University Press, 2013.

516 V současné době je status adekvátní úrovně přiznán 12 zemím včetně Argentiny, Kanady, Izraele, Švýcarska a Nového Zélandu (viz Adequacy decisions. *Evropská komise* [online]. [cit. 30. 6. 2020]).

517 Bod 76 rozsudku Soudního dvora Evropské unie ze dne 6. 10. 2015 ve věci *Schrems*, C-362/14.

518 Srovnej tamtéž bod 86.

údajů do USA, kterým se nakonec stal Privacy Shield.[519] V této době však často probíhal de iure nezákonný transfer dat do Spojených států, pokud správci údajů rychle nezareagovali a nepodařilo se jim nahradit tento institut nějakým jiným, který směrnice 95/46/ES nabízela (například standardní smluvní doložky). Z hlediska legality však nastal poměrně zásadní problém v tom, že se řada orgánů ochrany osobních údajů v EU rozhodla tento protiprávní stav neřešit a nevymáhat. WP 29 ve svém vyjádření z 16. října 2015 nepřímo vyjádřila, že do konce ledna 2016 nebudou národní úřady ochrany osobních údajů sankcionovat předávání údajů, které dále ze setrvačnosti probíhalo v režimu zrušeného rozhodnutí Komise č. 2000/52.[520] Některé národní úřady pak v této praxi pokračovaly i po uplynutí uvedeného termínu, jako například britský ICO, který ve svém vyjádření k rozhodnutí ve věci *Schrems* z února 2016 uvedl: *„We are not rushing to use our enforcement powers.“*[521] Jiné, jako například Hamburský úřad, pokuty začaly ukládat.[522, 523]

Rozhodnutí nevymáhat určité případy porušení povinností je krajně problematické, jakkoli racionálně a pragmaticky zní vysvětlení, proč padlo. Důvodů, proč je takovou praxi třeba odmítnout, je hned několik a je možné

519 Viz Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. 7. 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (oznámeno pod číslem C(2016) 4176).

520 Srovnej PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement of the Article 29 Working Party. *Evropská komise* [online]. 16. 10. 2015 [cit. 30. 6. 2020]. Srovnej rovněž AHS, James M. European Commission Announces New U.S.–EU Safe Harbor Agreement. *HuschBlackwell.com* [online]. [cit. 30. 6. 2020].

521 Viz Information commissioner's office. Data transfers to the US and Safe Harbor – interim guidance. *Ico.org.uk* [online]. 2016, s. 3 [cit. 30. 6. 2020].

522 PROUST, Olivier. EU–U.S. Privacy Shield comes into force. *Privacy, Security and Information Law* [online]. 2016 [cit. 30. 6. 2020].

523 Jako poznámku ležící již mimo časový záběr této publikace je nicméně třeba zmínit, že rozhodnutím ve věci *Schrems II* došlo rovněž ke zrušení režimu Privacy Shield (viz rozsudek Soudního dvora Evropské unie ze dne 16. 7. 2020 ve věci *Schrems II*, C-311/18). Krom toho, byť soud nezrušil nástroj standardních smluvních doložek jako takový, uvedl, že národní úřady mohou zakročit proti předávání údajů prováděného na základě standardních smluvních doložek, pokud v cílové jurisdikci není zaručena adekvátní úroveň ochrany. To přitom musí v souladu s principem odpovědnosti posoudit správce údajů, který přenos dat iniciuje. Pokud cílová jurisdikce nemůže zaručit adekvátní úroveň ochrany, není možné aplikovat ani standardní smluvní doložky. V konkrétním případě předávání údajů do USA pak SDEU již dvakrát odůvodnil, že tento transfer není bezpečný a záruky nejsou dostatečné. Vzhledem k tomu mám za to, že v současné době (září 2020) není možné legálně předávat osobní údaje do USA, ledaže by se správce spolehl na existující výjimky dle čl. 49 Obecného nařízení.

je řadit od konkrétních po abstraktní. Nejkonkrétnějším důvodem je přesné vymezení pravomocí dozorového orgánu. Budeme-li se pohybovat v českém kontextu, tak pravomoci a úkoly Úřadu pro ochranu osobních údajů byly stanoveny v zákoně 101/2000 Sb. a nyní jsou upraveny zákonem 110/2019 Sb. Úřad, jakožto orgán výkonu státní moci, je vázán zásadou legality a smí tedy činit jen v rozsahu a způsobem, jaký mu zákon ukládá.[524] Tomu ovšem odpovídá i povinnost činit tak, jak stanoví zákon.[525] Jednou ze základních zásad dobré správy je princip legitimního očekávání. Dle něj má mít každý možnost získat představu, jak správní orgán bude v konkrétních situacích jednat.[526] Pokud právní předpis nestanoví možnost diskrece správního úřadu, nemůže dojít k rozhodnutí, že některé typové případy nebudou vymáhány.

Druhý, již poněkud abstraktnější důvod, je možné vyjádřit odkazem na Fullerovy principy dobrého (morálního) práva.[527] Posledním z jeho osmi požadavků je nezbytnost souladného úředního postupu, který odpovídá zákonem stanoveným povinnostem. Bez efektivního vymožení daná norma *de facto* přestává být právem. *Ad hoc* rozhodnutí, že určité případy nebudou vymáhány, tak podrývají legitimitu daného systému jako celku. Nevymáhání povinností správce údajů je jedním z největších problémů, kterému celý systém ochrany osobních údajů čelí. Dokazuje to například text Lucase Bergkampa z roku 2002: *„In the past, business could survive under European privacy legislation only because enforcement was extremely lax and the government could grant ad-hoc privileges in any event… Monitoring or verifying compliance with data protection rules, of course, requires thorough and laborious audits of a data controller's data collection, use, and management practices. The government agencies responsible for data protection have only limited powers and resources, and enforcement tends not to be their first priority. As a result, regulated entities do not have appropriate incentives*

524 Viz čl. 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů a čl. 2 odst. 2 Listiny základních práv a svobod (usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů).

525 Srovnej § 2 zákona č. 500/2004 Sb., správní řád.

526 Srovnej HENDRYCH, Dušan a kol. *Správní právo: obecná část*. 7. vyd. Praha: C. H. Beck, 2009, s. 817.

527 Srovnej FULLER, Lon L. *The morality of law*. Rev. vyd. New Haven: Yale University Press, 1978, s. 33 a násl.

to comply with the law."[528] Zajištění efektivnější kontroly a vymáhání povinností pak bylo důvodem pro zakotvení možnosti astronomicky vysokých sankcí v Obecném nařízení. Rozhodnutí správních úřadů o tom, že se některé povinnosti nebudou dotýkat vybraných zpracování, však veškeré snahy o zlepšení stavu vymáhání práva na ochranu osobních údajů podrývaly.[529]

Konečně třetím důvodem, který na předchozí přímo navazuje, je požadavek na právní jistotu jako jeden z nejzákladnějších právních principů a účelů práva.[530] Pokud má být kdokoli vystaven sankci, je dle zásad *nullum crimen sine lege* a *nulla poena sine lege* nezbytné, aby jak škodlivé chování, tak sankce byly nejprve vyjádřeny v zákoně. Důležité přitom je, že musí být součástí zákona materiálně (nikoli jen formálně) a musí být tedy vymáhány.[531] *Ad hoc* rozhodnutí, které nemá oporu v zákoně, že některé povinnosti nebudou vymáhány, znemožňuje skutečné poznání platného a účinného práva na straně povinných subjektů a podrývá jejich právní jistotu.

Z důvodů uvedených v této podkapitole se domnívám, že byť v některých případech byla za doby účinnosti minulé právní úpravy z pragmatického hlediska nevymáhání určitých povinností pochopitelným rozhodnutím, dalece přesahovalo možnosti dané právními předpisy a obecnými právními zásadami. V důsledku toho jej není možné považovat za vhodné a možné řešení problémů, které byly nastíněny ve třetí kapitole této publikace.

4.3 Shrnutí kapitoly

Extenzivní interpretace definičních ustanovení systému ochrany osobních údajů vedla k mohutné šíři aplikace této právní úpravy. To se projevilo

528 BERGKAMP, Lucas. EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *Computer Law & Security Review* [online]. 2002, roč. 18, č. 1, s. 37.

529 Více k nezbytnosti vymáhání práva na soukromí též REIMAN, Jeffrey H. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer and High-Technology Law Journal*, 1995, roč. 27, č. 1, s. 36.

530 Právní jistota je například přímo součástí trojlístku účelů práva dle Gustava Radbrucha (citováno dle HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, s. 132) a stojí rovněž na pozadí Fullerových principů morálního práva.

531 K argumentaci nezbytnosti znalosti skutečného stavu zákona před uvalením sankce viz rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb.NSS (rozhodnutí ve věci *Ryneš*).

v hraničních případech, na které sice právní úprava dopadla, ale v nichž plnění povinností správce bylo vzhledem k povaze zpracování nepřiměřené nebo zcela nemožné. V době bývalé právní úpravy jsme měli možnost potkat se se dvěma způsoby řešení tohoto problému. Prvním byla restriktivní interpretace definičních pojmů tak, aby právní úprava ochrany osobních údajů na tyto problematické případy nedopadla. Druhou cestou bylo nevymáhání povinností ze strany dozorových orgánů. Tato kapitola se postupně oběma způsobům věnovala a dovodila, že ani jeden není možné aplikovat pro zásadní nedostatky, které představují.

5 ZÁSADA ODPOVĚDNOSTI SPRÁVCE A REGULACE ZALOŽENÁ NA RIZIKU

Třetí kapitola této knihy demonstrovala základní strukturální problémy, které v sobě nesla stará právní úprava ochrany osobních údajů představovaná směrnicí 95/46/ES a zákonem č. 101/2000 Sb. Šlo zejména o nedostatečnou flexibilitu právní úpravy, která byla způsobena nízkou škálovatelností a granularitou povinností správce osobních údajů. To se v důsledku projevilo buď v nepřiměřené zátěži správců údajů, nebo přímo v protiprávnosti určitých zpracování, která byla vzhledem k nepředvídanému technologickému vývoji na samé hranici možností bývalé právní úpravy. Čtvrtá kapitola analyzovala dvě možné varianty řešení tohoto problému v podobě „zúžení vstupu do systému zpracování", tedy limitace interpretačního rozsahu pojmů *osobní údaj* a *zpracování osobních údajů*, a „limitace na výstupu", tedy rozhodnutí správních úřadů vybrané prohřešky proti ochraně osobních údajů nesankcionovat. Obě tyto varianty je třeba odmítnout, protože buď kolidují se základními zásadami, principy a účelem právní úpravy ochrany osobních údajů (první případ), nebo jsou v zásadním střetu s Fullerovými pravidly vnitřní morálky práva a mohou vzhledem k porušení zásady dělby moci představovat zásah až na ústavní úrovni (druhý případ).

Tato kapitola se zabývá třetí variantou řešení, která spočívá v takové regulaci ochrany osobních údajů, která umožní škálovatelnost a granularitu povinností správce údajů, aby zůstal zachován široký výkladu pojmů *osobní údajů* a *zpracování osobních údajů* a zároveň, aby povinnosti správců odpovídaly povaze probíhajícího zpracování. Cílem této kapitoly je analyzovat text Obecného nařízení a vyhodnotit, zda umožňuje interpretaci odpovídající této třetí variantě. A pokud ano, jaké výzvy taková aplikace přináší správci údajů, dozorovému úřadu a soudům.

První část této kapitoly vychází zejména z textů Caryho Coglianese a představuje způsob právní regulace prostřednictvím performativních pravidel, která slouží jako prostředek k zajištění flexibility výkonu povinností subjektů dotčených danou regulací. Tento regulatorní přístup byl totiž evropským zákonodárcem využit při tvorbě Obecného nařízení v podobě zavedení zásady odpovědnosti správce a přístupu založeném na riziku. Ty představují

hlavní regulatorní změnu, kterou Obecné nařízení přineslo. Druhá a třetí část této kapitoly se proto detailně věnují těmto dvěma prvkům, které společně fungují jako nástroj, jímž zákonodárce zajišťuje, že regulace dopadne na každý povinný subjekt způsobem odpovídajícím povaze prováděného zpracování. Čtvrtá část této kapitoly analyzuje vybraná ustanovení Obecného nařízení ve světle fungování zásady odpovědnosti správce a hodnocení rizik, hodnotí míru jejich škálovatelnosti a určuje jako limit práva subjektů údajů, která není možné vyloučit ani v případě málo rizikových zpracování. Konečně pátá část této kapitoly upozorňuje na možné problémy a výzvy, které interpretace Obecného nařízení vycházející ze zásady odpovědnosti správce a hodnocení rizik přináší.

5.1 Performativní regulace

Pokud se zákonodárce pokouší normativně upravit fungování (zejména) nových technologií, bude se potýkat s řadou problémů. Obecným a zřejmě nezbytným problémem je zaostávání legislativy za technologickým vývojem.[532] Pokud však tento problém pomineme, je velkou výzvou pro zákonodárce, že vytvoření takové právní úpravy předpokládá hlubokou a detailní znalost konkrétních technologií a jejich fungování. I v případech, že je tento předpoklad splněn, může zákonodárce snadno narazit na to, že tradiční metody regulace, které konkrétně stanoví, jak má regulovaný subjekt postupovat, nebudou odpovídat potřebám regulované materie z hlediska dostatečné flexibility, která povinným subjektům umožní, aby mohly své povinnosti adekvátně naplnit. Jak uvádí Coglianese, častou námitkou proti tomuto regulatornímu přístupu přezdívanému rovněž *„command-and-control"*,

532 Anekdotickým příkladem takového případu, kdy se zákonodárce pokusil předvídat vývoj technologií, což vyústilo v jednorázový a dnes fakticky nepoužívaný institut, je právní ochrana polovodičových výrobků dle zákona č. 529/1991 Sb., o ochraně topografií polovodičových výrobků. Od 1. ledna 1992, kdy zákon nabyl účinnosti, získalo tuto ochranu celých sedm topografií polovodičových výrobků a následně institut upadl v zapomnění. Viz Rejstřík topografií polovodičových výrobků. *Úřad průmyslového vlastnictví* [online]. [cit. 30. 6. 2020]; Více viz MÍŠEK, Jakub. Konflikt technologického vývoje a práva na příkladu autorského práva. *Právník*, 2015, roč. 154, č. 10.

případně *„means-based regulation"* (dále „regulace metody")[533] je jeho náročnost a neekonomičnost, protože nepřiměřeně zatěžuje povinné subjekty, po kterých požaduje použití konkrétního postupu nebo technologie, byť by objektivně nebyly v konkrétním případě vzhledem k účelu právní úpravy nezbytné.[534]

Princip performativní regulace oproti regulaci metody spočívá v tom, že zákonodárce nestanoví konkrétní cestu, jejíž splnění vede k dosažení regulací sledovaného cíle, ale naopak určí cílový stav a nechá regulované subjekty, aby si samy určily, jak takového zákonem stanoveného cíle dosáhnou. To potvrzuje Peter May, když uvádí: *„[I]t is useful to consider performance-based approaches to regulation as a reaction to the perceptions of overly rigid rules and inflexible enforcement. As discussed above, critics argue that these regulatory shortcomings impose unnecessary burdens and limit innovation."*[535] Tento druh regulace je proto populární zejména v souvislosti s právní úpravou nových technologií, byť – jak uvádí Greg Foliente – příklad performativní normy bychom mohli nalézt v kontextu stavebnictví již v Chamurappiho zákoníku, který stanovil bez další specifikace postupu povinnost stavět domy tak, aby nespadly.[536] Jako výhody performativní regulace se tradičně uvádějí vyšší flexibilita regulovaných subjektů, která jednak umožní dosáhnout kýženého výsledku s nižšími

533 Viz např. COGLIANESE, Cary. Performance-Based Regulation: Concepts and Challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative law and regulation: understanding the global regulatory process*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, s. 415; Research handbooks in comparative law. Ve svém starším textu tento typ regulace Coglianese nazývá *„technology-based"* (COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review,* 2003, roč. 37, č. 4, s. 694); Můžeme se však setkat rovněž s označením *„specification-based"* regulace (viz CHINANDER, Karen R., Paul R. KLEINDORFER a Howard C. KUNREUTHER. Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks. *Risk Analysis* [online]. 1998, roč. 18, č. 2, s. 135).

534 Viz COGLIANESE, Cary. Performance-Based Regulation: Concepts and Challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative law and regulation: understanding the global regulatory process*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, s. 403, Research handbooks in comparative law.

535 MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4, s. 387.

536 Foliente cituje anglický překlad čl. 229 *„The builder has built a house for a man and his work is not strong and if the house he has built falls in and kills a householder, that builder shall be slain."* FOLIENTE, Greg C. Developments in performance-based building codes and standards. *Forest Products Journal*, 2000, roč. 50, č. 7–8, s. 13.

náklady a zároveň nechá otevřené okno pro inovace, které mohou dané odvětví dále posunout.[537] Coglianese uvádí jako příklad *performance-based*[538] pravidla normu, která upravuje bezpečnostní uzavírání léku tak, že 85 % dětí nesmí být schopno otevřít nádobu do pěti minut.[539] Druhým příkladem performativní regulace může být novozélandská právní úprava stavebnictví, která nestanovila přesně jaké technologie se mají během stavby používat, ale naopak poměrně přesně určila parametry, které stavba měla po dokončení splňovat.[540] O performativní regulaci můžeme hovořit i tehdy, když jsou parametry výsledku nastaveny tak, že jim v době zavedení regulace odpovídá pouze jediná technologie. Stále je totiž možné, aby povinné osoby v budoucnu vynalezly jinou, adekvátní a možná vhodnější technologii, kterou svoji povinnost splní.[541]

V českém prostředí se performativní regulaci věnuje převážně Radim Polčák a to zejména v kontextu regulace kyberprostoru.[542] Propojuje Coglianesovu teorii s konceptem definičních autorit, tedy subjektů, které fakticky vykonávají kontrolu nad určitou oblastí (zejména) technické infrastruktury kyberprostoru[543] a mají proto nejlepší přehled o tom, jak se dané prostředí chová a jak

537 Viz např. COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 723; Argument snížení nákladů na implementaci rovněž viz CHINANDER, Karen R., Paul R. KLEINDORFER a Howard C. KUNREUTHER. Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks. *Risk Analysis* [online]. 1998, roč. 18, č. 2, s. 136.

538 Dobrý český překlad nabídl ve své disertační práci Jakub Harašta, když uvádí *„performance-based rules"* jako pravidla *„založená na výkonu a projevech"*. Viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti*. Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, 2018, s. 53.

539 COGLIANESE, Cary. Performance-Based Regulation: Concepts and Challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative law and regulation: understanding the global regulatory process*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, s. 406, Research handbooks in comparative law.

540 Detailně viz MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy,* 2003, roč. 25, č. 4.

541 Z tohoto důvodu je jako argument ve prospěch performativní regulace uváděn pozitivní vliv na technologický vývoj, nebo minimálně jeho nebrždění. Viz COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 711.

542 Např. POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 13–16.

543 POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 137 a násl., Téma.

je možné zajistit jeho efektivní regulaci.[544] Polčák uvádí: *„Performativní pravidlo tak má charakter obecně (až teleologicky) definované povinnosti ukládající definiční autoritě vytvoření a technickou implementaci konkrétních pravidel, přičemž jejich obsah je ponechán úvaze definiční autority v návaznosti na parametry příslušného systému nebo sítě. Různé definiční autority mohou na své fyzické nebo logické infrastruktuře dle svého uvážení implementovat obsahově zcela různá pravidla, jejichž fungování však vede k témuž cíli.“*[545] Definiční autorita si na základě vytyčeného cíle stanoví vlastní vnitřní normy v podobě vnitropodnikových pravidel, ujednání ve smlouvě nebo počítačového kódu,[546] které by měly vést k naplnění vůle zákonodárce a které jsou pak kontrolovány kompetentními úřady.[547] Polčák dále uvádí tři generické znaky, které jsou dle něj společné oblastem, u nichž se performativní regulace nabízí jako vhodné řešení. Za prvé jde o oblasti, v nichž má definiční autorita vyšší úroveň znalostí regulované materie, za druhé v těchto oblastech platí, že definiční autorita může fakticky dosáhnout regulace snadněji než stát, protože má v porovnání se státem vyšší úroveň práv a za třetí, zájmy definiční autority a státu musí být synergické.[548] Jako příklady aplikace performativní regulace v českém právním prostředí uvádí pak kybernetickou bezpečnost a ochranu osobních údajů.[549]

Coglianese nahlíží na performativní regulaci z širšího hlediska, přičemž, byť si vybírá jako příklady zejména právní normy z oblasti práva životního prostředí, jsou jeho závěry šířeji použitelné. Všímá si, že je možné performativní pravidla dělit podle šesti kategorií:[550]

1. Dělení podle konkrétnosti. Toto dělení reflektuje, zda je cíl, kterého má regulovaný subjekt dosáhnout, formulován spíše obecně

544 Viz POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 89.

545 Např. POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 14.

546 Za touto úvahou stojí skutečnost, že definiční autority mohou normovat chování svých uživatelů tím, jak programově nastaví prostředí, které ovládají. Více k tomu POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 188, Téma; Dále zejména viz LESSIG, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.

547 Více viz POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník,* 2019, roč. 158, č. 1, s. 89.

548 POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 14.

549 Ibid.

550 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3, s. 537–541.

(např. „stroj musí být způsobilý k letu“), nebo konkrétně (např. výše uvedený příklad s uzávěrem léků, který nesmí 85 % dětí otevřít rychleji než za pět minut).

2. Dělení podle vzdálenosti mezi konkrétní právní normou a cílem právní úpravy. Toto dělení rozlišuje případy, kdy je performativní pravidlo formulováno v blízkosti konečného cíle dané právní úpravy (např. může taková performativní norma znít „povinný subjekt musí zajistit ochranu zdraví svých zaměstnanců“), nebo naopak relativně vzdáleně (Coglianese uvádí příklad britské regulace, která s konečným cílem ochránit zdraví zaměstnanců přesně stanoví maximální množství koncentrace formaldehydu ve vzduchu na pracovišti, kterému může být zaměstnanec v určitém časovém úseku vystaven).[551]
3. Dělení podle toho, jak je hodnoceno splnění výkonu a naplnění uloženého cíle. V tomto případě je možné kontrolovat splnění uloženého cíle buď konkrétním měřením a pozorováním výsledků činnosti povinného subjektu, testováním v podobných podmínkách, nebo počítačovou simulací. Ty jsou využívány zejména v případech, kdy testování není možné, jako je tomu například při zavádění protipožární ochrany.[552]
4. Dělení dle stanovení standardu cíle. Performativní pravidlo může buď cílit na ideální stav („ochrana veřejné bezpečnosti“), nebo na reálně dosažitelnou úroveň snesitelného rizika.
5. Dělení dle měřených jednotek. V tomto případě rozdíl spočívá v tom, zda má být cíle dosaženo u každého jednoho prvku z větší množiny (například emise u každého jednoho vyrobeného vozu nesmí přesáhnout určitý přesně stanovený limit), nebo zda je cíl definován jako průměrná agregovaná hodnota všech prvků (emise všech vyrobených vozů nesmí průměrně přesáhnout určitou hodnotu).[553]
6. Dělení dle důkazního břemene. Performativní pravidla se mohou lišit dle toho, zda důkazní břemeno na prokázání jejich porušení spočívá na kompetentním státním orgánu, nebo naopak, zda povinné subjekty mají prokazovat, že své povinnosti plní.

551 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3, s. 538.
552 Ibid., s. 539.
553 Ibid., s. 540.

Současná právní úprava ochrany osobních údajů je postavena na performativní regulaci, protože Obecné nařízení zakotvilo zásadu odpovědnosti správce údajů jako jednu ze základních zásad, na kterých spočívá. Tato zásada ukládá správci osobních údajů povinnost zaručit, že dané zpracování probíhá s přihlédnutím na jeho povahu a rizika, která představuje, v souladu s právní úpravou ochrany osobních údajů. Zároveň pak musí být schopný svoji souladnost (*compliance*) doložit.[554] Ani čl. 5, ani čl. 24, které tuto zásadu upravují, neuvádí, jakým konkrétním způsobem má správce osobních údajů tohoto cíle dosáhnout. Vzhledem k uvedeným kategoriím je možné určit, že se jedná o obecně formulované performativní pravidlo cílící na ideální stav, které je relativně blízko konečnému cíli právní úpravy ochrany osobních údajů a jehož hodnocení na úrovni konkrétních zpracování provádí dozorový úřad, přičemž důkazní břemeno spočívá na straně správce údajů.

Performativní regulace není jediný druh regulace, který nabízí flexibilitu na straně povinného subjektu v tom, jak konkrétně své povinnosti provede. Coglianese uvádí několik dalších typů, které se od performativní regulace v některých aspektech odlišují. Prvním z nich je seberegulace. Princip seberegulace spočívá v tom, že povinný subjekt (například v podobě soukromé společnosti nebo zájmového sdružení právnických osob) vydává vlastní normy, kterými sám sebe a své členy zavazuje a reguluje jejich chování.[555] Proto pokud zákon upravuje seberegulaci, tedy nařizuje povinnému subjektu vytvořit si vlastní vnitřní normy, můžeme hovořit o tzv. meta-regulaci.[556] Normy, které takto vydá, však mohou svým charakterem odpovídat jak performativní regulaci, tak standardní regulaci metody, která bude konkrétně určovat jakými způsoby má být cíle dosaženo, nebo jakékoli jiné regulační metodě. Z toho důvodu není možné seberegulaci s performativní regulací ztotožňovat.

554 K problematice *compliance* včetně oblasti ochrany osobních údajů viz HURYCHOVÁ, Klára a Michal SÝKORA. *Compliance programy (nejen) v České republice*. Praha: Wolters Kluwer, 2018.

555 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform,* 2017, roč. 50, č. 3, s. 535.

556 Viz COGLIANESE, Cory a Evan MENDELSON. Meta-Regulation and Self-Regulation. In: BALDWIN, Robert, Martin CAVE a Martin LODGE (eds.). *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2012, s. 146–168.

Coglianese dále odlišuje *management-based* regulaci, která má s performativní regulací společnou velkou míru flexibility. Na rozdíl od performativní regulace však zákonodárce po povinném subjektu nevyžaduje dosažení vytyčeného cíle, ale pouze vytvoření analýz a naplánování postupů a fungování povinného subjektu, které – pokud jsou následovány – spějí k naplnění účelu právní úpravy.[557] *Management-based* regulace totiž nestanoví ani cíl, kterého má povinný subjekt dosáhnout, ba ani prostředky, kterými má cíle dosáhnout. Prostřednictvím *management-based* regulace je ukládána povinnost provést vnitřní hodnocení fungujících a plánovaných procesů a nastavit je prostřednictvím autonomně vytvořených norem tak, aby byly konzistentní s účely právní úpravy.[558] *Management-based* regulace pak ani nemusí stanovovat povinnost použít plán, který byl jejím prostřednictvím vytvořen. Důležitý je akt sběru informací a plánování.[559] Účel *management-based* regulace pak spočívá v tom, že má motivovat povinné subjekty, aby samy upravily své prostředí tak, aby co nejvíce odpovídalo cílům právní úpravy, například pod vlivem obecné preventivní povinnosti. Coglianese dodává: *„Under management-based regulatory strategies, firms are expected to produce plans that comply with general criteria designed to promote the targeted social goal. Regulatory criteria for management planning specify elements that each plan should have, such as the identification of hazards, risk mitigation actions, procedures for monitoring and correcting problems, employee training policies, and measures for evaluating and refining the firm's management with respect to the stated social objective."*[560] Prvky *management-based* regulace v ochraně osobních údajů je možné objevit například v povinnosti správce osobních údajů vést záznamy o zpracování dle čl. 30 Obecného nařízení, případně v povinnosti postupovat dle zásad záměrné a standardní ochrany osobních údajů dle čl. 25 Obecného nařízení.

557 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 535–536.

558 Shodně viz SNYDER BENNEAR, Lori. Evaluating Management-Based Regulation: A Valuable Tool in the Regulatory Toolbox?. In: COGLIANESE, Cary a Jennifer NASH (eds.). *Leveraging the private sector: management-based strategies for improving environmental performance*. Washington, DC: RFF PRess, 2006, s. 52.

559 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform,* 2017, roč. 50, č. 3, s. 536.

560 COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review,* 2003, roč. 37, č. 4, s. 694.

Rozdíl mezi performativní regulací, regulací metody[561] a *management-based* regulací odpovídá různým fázím činnosti povinného subjektu. Pokud zákonodárce reguluje fázi plánování, hovoříme o *management-based* regulaci. Pokud reguluje samotný výkon činnosti, hovoříme o regulaci metody a konečně pokud zákonodárce svojí regulací určuje cíl, kterého má být dosaženo, jde o performativní regulaci.[562]

Je důležité zdůraznit, že performativní nebo *management-based* regulace i přes jejich nespornou výhodu ve velké míře flexibility nebudou vhodné pro použití v každé situaci. Naopak, performativní regulace nese řadu překážek, se kterými se zákonodárce, případně orgán dozoru, musí vypořádat. První problém performativní regulace spočívá v tom, že pokud zákonodárce opomene širší kontext a nevhodně nastaví výsledný cíl, může dojít k tomu, že povinný subjekt splní svoji povinnost, ale výsledný efekt bude mít negativní vedlejší účinky. Coglianese uvádí jako příklad takové situace výše zmíněnou regulaci bezpečnosti uzávěrů nádob s léky, které sice zabránily 85 % dětí uzávěr otevřít, zároveň ale měly stejný efekt na 70 % seniorek a 40 % seniorů.[563] Jiným příkladem nevhodně stanovené performativní normy byla snaha zajistit funkčnost a bezpečnost airbagů v autě. Její hodnocení se provádělo prostřednictvím testovací figury o velikosti dospělého člověka. Vedlejším efektem jinak normu splňujících produktů byla naprosto nulová efektivita v případě, že na místě v době nehody sedělo dítě.[564] Druhým problémem performativní regulace je, že ačkoli obecně panuje shoda na tom, že se jedná o způsob regulace, který umožňuje snížení nákladů povinných subjektů tím, že upraví způsob dosažení cíle přesně dle potřeb konkrétního případu,[565] může zejména v případě malých povinných subjektů docházet k situacím,

561 Tento druh regulace je nazývaný různými autory různě: „means-based", „technology-based", „specification-based" a „command and control" regulace.

562 COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review,* 2003, roč. 37, č. 4, s. 694.

563 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 555.

564 Ibid., s. 556.

565 Např. MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4, s. 387; Dále též COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 707–708.

kdy si samy nedokáží s performativní regulací poradit. Investice ke splnění povinnosti tak bude větší než v případě jasně určeného postupu v podobě standardní regulace metody. Povinné subjekty tak například naplňují povinnosti přísněji, než by bylo potřeba, aby měly jistotu, že nebudou sankcionovány. Tak tomu bylo v případě nástupu účinnosti Obecného nařízení.[566]

Hlavní výzva v případě performativní regulace však spočívá v zajištění efektivního vymáhání performativních norem, a to zejména tehdy, když jsou formulovány obecně. Performativní regulace klade na státní aparát výrazně vyšší nároky, než standardní způsob právní úpravy, a to jak vzhledem k nezbytné expertíze osob, které musí být schopny posoudit, zda došlo k naplnění zákonem vytyčeného cíle, tak vzhledem k finančním nákladům vynaloženým na kontrolu splnění povinností.[567] To je ještě zesíleno v případě velmi různorodé skupiny povinných subjektů, na kterou dopadají stejná pravidla. Čím je skupina povinných subjektů různorodější, tím více mohou v součtu povinné subjekty ušetřit na nákladech *compliance*, protože mají možnost si upravit konkrétní povinnosti vzhledem ke konkrétní situaci. Zároveň ale s rostoucí různorodostí povinných subjektů rostou rovněž náklady na straně státního dozoru, protože je obtížnější zkontrolovat, že povinný subjekt provedl interpretaci povinnosti a její implementaci opravdu správně. Zajištění odpovědnosti regulovaného subjektu je však naprosto klíčovým předpokladem pro fungování performativní regulace. Peter May ve své studii popisuje, jak nesprávně a nedostatečně prováděné kontroly performativní regulace upravující stavbu budov na Novém Zélandě vedly k zásadní krizi ve stavebnictví, projevující se obrovským množstvím zatékajících budov. Doslova uvádí: *„Accountability is a fundamental and thorny issue for performance-based regulations and as such is the Achilles' heel of this form of regulation… Performance-based approaches seek accountability for results, but… observing or predicting results can be costly or even infeasible. In the New Zealand case,*

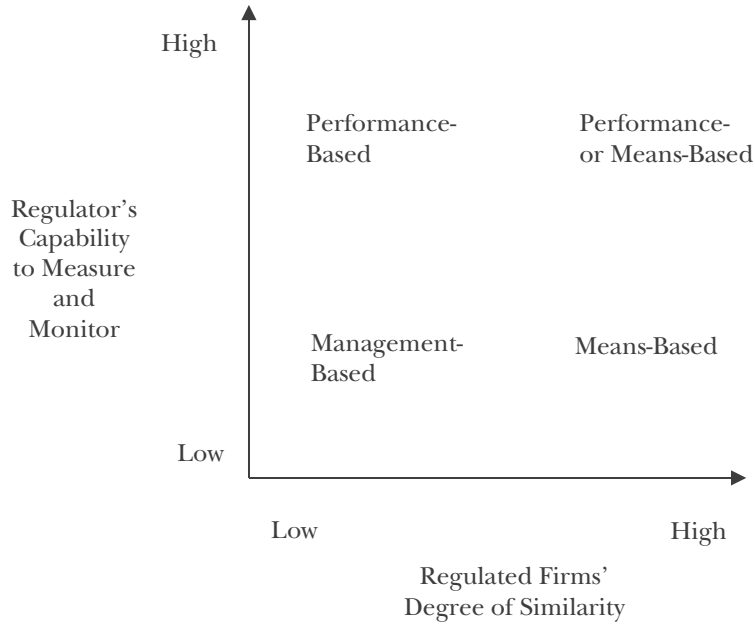
566 Srovnej POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 15; Dále viz též CHINANDER, Karen R., Paul R. KLEINDORFER a Howard C. KUNREUTHER. Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks. *Risk Analysis* [online]. 1998, roč. 18, č. 2, s. 136.

567 Shodně též COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform,* 2017, roč. 50, č. 3, s. 548.

the problem was less a question of feasibility and more one of not wanting to invest the necessary resources given the twin desires to reduce the scope of government and to lessen enforcement burdens for regulated entities. These forces contributed to over-reliance on poorly trained third-party certifiers and to lax review of alternative building products. In short, there was a naive faith that „the market" would help correct deficiencies in building practices."[568] Příklad novozélandských zatékajících budov jasně ukazuje, že aby mohla fungovat flexibilní regulace, je naprosto nezbytné, aby byl přítomný silný princip odpovědnosti regulovaného subjektu, stejně jako možnost a schopnost právního vymožení povinnosti.

Výše uvedené přehledně shrnuje následující Coglianesův přehled vztahů mezi různými způsoby regulace a jejich vhodnosti pro různé varianty regulované materie.[569]

Obrázek 2: Přehled druhů regulace



568 MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*. 2003, roč. 25, č. 4, s. 397–398.

569 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 547.

Coglianese porovnává celkovou ekonomickou nákladnost jednotlivých způsobů regulace. Zahrnuje do ní jak stranu povinných subjektů, tak stranu dozorových orgánů. V případech, kdy jsou si regulované subjekty vzájemně podobné, se zavedením performativní regulace jejich náklady nesníží, protože stejně všechny budou postupovat víceméně stejně. Naopak na straně státního dozoru dojde ke zvýšení nákladů, protože performativní regulace i v takových případech klade na výkon práva vyšší nároky. Vzhledem k tomu se v oblastech s podobnými povinnými subjekty obecně nevyplatí zavádět performativní regulaci, protože zvýšené náklady na straně státního dozoru a vymáhání práva přebijí malé snížení nákladů na straně povinných subjektů.[570] Zároveň však není vhodné performativní regulaci používat v případech, kdy stát není schopen zajistit efektivní kontrolu regulovaného subjektu a toho, jak performativní normy naplňuje. Pro takové situace se dle Coglianese hodí využít spíše *management-based* regulace.[571]

Jak hlouběji ukážou následující části této kapitoly, ochrana osobních údajů v podobě, v jaké ji zakotvilo Obecné nařízení, silně spočívá na performativní regulaci, byť obsahuje rovněž normy spadající spíše do oblasti regulace metody nebo *management-based* regulace. Rozhodnutí evropského zákonodárce založit základní metodu právní úpravy osobních údajů na principech performativní regulace je v souladu s Coglianesovým doporučením, že performativní regulace je vhodná v případech, kdy je regulováno množství nesourodých subjektů. Vybraná regulatorní metoda tak má potenciál adresovat nedostatky popsané v třetí kapitole této knihy. Problematické však zůstává zajištění vymáhání těchto pravidel. Základní otázky, které je tak třeba zodpovědět, spočívají v tom, jakým způsobem Obecné nařízení definuje cíl, kterého mají regulované subjekty (tedy správci údajů) dosáhnout a zda, případně jakým způsobem normativně přispívá k tomu, aby kontrola plnění povinností správců byla efektivní.

570 COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 549.

571 COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review*. 2003, roč. 37, č. 4, s. 725–726.

5.2 Zásada odpovědnosti správce údajů

Když směrnice 95/46/ES procházela v roce 2009 svým finálním hodnocením, uvedla pracovní skupina WP 29 jako jedno z hlavních zjištění, že ačkoli jsou i přes technologický vývoj její základní principy stále platné, je třeba využít možností, které chystaná reforma nabízí a zavést nové nástroje, které aplikaci právního režimu ochrany osobních údajů usnadní a přizpůsobí potřebám jednadvacátého století.[572] Jedním z doporučovaných nových nástrojů pak byl *„principle of accountability"*, do češtiny překládaný jako *„zásada odpovědnosti správce osobních údajů"*. Je to právě tato zásada *accountability*, která představuje hlavní zdroj zarámování právní úpravy ochrany osobních údajů do podoby systému stojícího na performativních pravidlech.

Anglický pojem *accountability* je sice tradičně překládán jako „odpovědnost", význam těchto pojmů se však podstatně liší. Zjednodušeně je možné říci, že v českém právním prostředí je pojem „právní odpovědnost" obecně chápán jako *„povinnost snést zákonem danou újmu* [sankci, pozn. JM] *v případě, že nastane zákonem stanovená skutečnost"*.[573] Tomuto chápání pojmu odpovědnost odpovídá spíše anglický výraz *„liability"*.[574] *Accountability* v současné době v anglickém diskurzu nese významové konotace, které se s českým významem pojmu „odpovědnost" nepojí.[575] Český překlad *„zásada odpovědnosti správce osobních údajů"*, který je univerzálně používán v dokumentech věnovaných této tematice[576], tak zcela neodpovídá původnímu významu jeho anglického ekvivalentu. Vzhledem k tomu se z něj vytrácejí tyto pro správnou interpretaci podstatné významové konotace. Pro přehlednost a významovou jednoznačnost proto v kontextu této publikace používám nepřeloženou podobu *„accountability"*.

572 PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, s. 6 [cit. 30. 6. 2020].

573 KNAPP, Viktor. *Teorie práva*. 1. vyd. Praha: C. H. Beck, 1995, s. 200, Právnické učebnice.

574 Srovnej Liability. *The Law Dictionary* [online]. [cit. 30. 6. 2020].

575 Čeština v tomto ohledu není rozdílná od jiných evropských jazyků, které rovněž nemají přesný významový ekvivalent slova accountability. Srovnej MULGAN, Richard. 'Accountability': An Ever-Expanding Concept? *Public Administration* [online]. 2000, roč. 78, č. 3, s. 555.

576 Např. Obecné nařízení, nebo dokumenty WP 29 (Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, 19 s. [cit. 30. 6. 2020]; a Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, 28 s. [cit. 30. 6. 2020].

Výraz *accountability* v sobě významově nese určení, že povinný subjekt *za něco* aktivně odpovídá, tedy že povinný subjekt nese odpovědnost za správnost nějakého postupu nebo fungování věci. Současně s tím pojem *accountability* však nese význam odpovědnost *vůči někomu*, tedy že se povinný subjekt zodpovídá nějaké autoritě, která nad ním má moc nebo ho může kontrolovat. Správné nastavení toho, vůči komu je odpovědnost vykazována, je zcela zásadní pro zajištění efektivní kontroly vymáhání povinností. Vhodně to vysvětluje Richard Mulgan: *„The concept of 'account-ability' includes an implication of potentiality, literally an 'ability' to be called to 'account'. It may thus refer to the potential for external scrutiny under which most expert professionals work, however independent they may be in their day-to-day decisions. Every medical doctor, for instance, knows that any action he or she takes (or does not take) could potentially become the object of disciplinary investigation or a legal action. In this respect, professionals are literally accountable in their professional actions because they are able to be called to account later for any of their actions."*[577] Těžiště *accountability* leží v prokázání toho, že uložená povinnost je opravdu vykonávána. S tím se dále pojí nezbytný požadavek na ověřitelnost, tedy aktivní ověřování, že povinný subjekt své povinnosti plní.[578] V rámci zajištění *accountability* povinného subjektu je proto přítomný prvek interakce nebo dialogu mezi povinným, který vysvětluje a odůvodňuje své počínání, a externím subjektem, který se táže, hodnotí a obecně kontroluje, zda jsou povinnosti plněny řádně.[579] To představuje první zásadní rozdíl od právní odpovědnosti, jak ji běžně rozumíme v českém diskurzu. Druhým zásadním rozdílem je, že *accountability* je oproti právní odpovědnosti (ve smyslu následku porušení primární povinnosti) preventivní a proaktivní. Povinný subjekt nečeká pasivně, až dojde k porušení práva, nebo až ho někdo vyzve k plnění, ale sám aktivně hledá vhodné řešení, a to včetně

577 Viz MULGAN, Richard. 'Accountability': An Ever-Expanding Concept? *Public Administration* [online]. 2000, roč. 78, č. 3, s. 560.

578 Srovnej bod 21 in PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, s. 7 [cit. 30. 6. 2020]; Dále též viz v kontextu ochrany osobních údajů např. BUTIN, Denis, Marcos CHICOTE a Daniel Le MÉTAYER. Strong Accountability: Beyond Vague Promises. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 344.

579 Srovnej RAAB, Charles. The Meaning of 'Accountability' in the Information Privacy Context. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 18–19.

nastavení svých vnitřních procesů a mechanismů.[580] Tyto závěry pak korespondují s výstupy *Galway Accountability Project,* ve kterém došlo k identifikaci následujících základních prvků *accountability* v prostředí ochrany soukromí a osobních údajů:

„1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

3. Systems for internal, ongoing oversight and assurance reviews and external verification.

4. Transparency and mechanisms for individual participation.

5. Means for remediation and external enforcement.“[581]

Důraz na transparentnost jako jednu ze základních součástí zásady *accountability* rovněž koreluje s obecným požadavkem na transparentnost zpracování osobních údajů. Zásada *accountability* tak představuje přesun od slepé důvěry k důvěře založené na skutečné znalosti situace.[582]

Vztah mezi odpovědností v běžném českém chápání a *accountability* v kontextu osobních údajů je možné vyjádřit rovněž následovně. *Accountability* zakládá správci údajů povinnosti zajistit vhodné nastavení procesů zpracování a být schopen prokázat, že toto nastavení opravdu vhodné (v souladu se zákonem) je. Právní odpovědnost ve smyslu povinnosti snést sankci se aktivuje tehdy, kdy správce údajů povinnosti vyplývající z *accountability* nesplní.

---

580 Viz např. ALHADEFF, Joseph, Brendan Van ALSENOY a Jos DUMORTIER. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 71.

581 Data Protection Accountability: The Essential Elements A Document for Discussion. *The Centre for Information Policy Leadership, Hunton & Williams LLP.* [online]. 2009, 21 s. [cit. 30. 6. 2020]; Uvedených pět kategorií v zásadě odpovídá pěti koncepcím *accountability*, jak je představil Jonathan Koppell, když jako součást *accountability* identifikoval transparentnost, odpovědnost (*liability*), kontrolovatelnost, zodpovědnost (*responsibility*, Koppell má na mysli obecné následování pravidel) a responzivitu. Viz KOPPELL, Jonathan G. S. Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder". *Public Administration Review* [online]. 2005, roč. 65, č. 1, s. 96.

582 Je to právě aspekt účasti zvenčí, který dle de Herta tvoří rozdíl mezi pouhou compliance (tedy splněním uložených povinností) a ověřitelnou odpovědností ve smyslu accountability. Viz HERT, Paul de. Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 199.

Byť je zásada *accountability* jednou z nejzásadnějších novinek, které Obecné nařízení přineslo,[583] není v kontextu ochrany osobních údajů zcela nová.[584] Vyskytovala se totiž již v Pravidlech OECD z roku 1980, která v čl. 14 obsahují stručné zanesení zásady odpovědnosti ve znění: *„A data controller should be accountable for complying with measures which give effect to the principles stated above."*[585] Úmluva 108 ani směrnice 95/46/ES zásadu odpovědnosti výslovně neobsahovaly. Úspěšnější však bylo její šíření mimo evropskou oblast. Pravidly OECD se inspiroval například kanadský zákonodárce, který zásadu odpovědnosti zanesl do čl. 4.1 přílohy 1 *Personal Information Protection and Electronic Documents Act* (PIPEDA) z roku 2000.[586] V roce 2005 pak v duchu doporučení OECD vyšla doporučení pro ochranu soukromí (Privacy Framework) organizace APEC (Asia-Pacific Economic Cooperation), která zásadu odpovědnosti rovněž zahrnula.[587]

V evropském kontextu stojí za zmínku zejména tzv. *„Accountability projects"*, jejichž cílem bylo určit, zda panuje v rámci široké debaty dotčených subjektů (včetně zástupců z oblasti technologických společností, neziskového sektoru, legislativy i odborných dozorových úřadů) shoda na tom, co přesně pojem *accountability* obnáší a co pro povinný subjekt znamená „být odpovědný" (ve smyslu *accountable*).[588] Na první, výše již zmíněný *Galway accountability project* (2009) navázala druhá fáze v podobě Pařížského a třetí v podobě

583 Shodně viz např. HERT, Paul de a Vagelis PAPAKONSTANTINOU. The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. *Computer Law & Security Review* [online]. 2014, roč. 30, č. 6, s. 638.

584 Dobře zpracovaný přehled vývoje zásady odpovědnosti správce viz ALHADEFF, Joseph, Brendan Van ALSENOY a Jos DUMORTIER. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 52–64.

585 Čl. 14 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD* [online]. [cit. 30. 6. 2020]. Jde o poslední článek druhé části Doporučení, která je tak formulována analogicky k čl. 5 Obecného nařízení.

586 Personal Information Protection and Electronic Documents Act (PIPEDA, Kanada). *Justice Laws Website* [online]. 2000.

587 Asia-Pacific Economic Cooperation (APEC). *APEC Privacy Framework* [online]. 2005, s. 28 [cit. 30. 6. 2020].

588 Viz ALHADEFF, Joseph, Brendan Van ALSENOY a Jos DUMORTIER. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 59.

Madridského *accountability* projektu. Společně vytvořily prostor pro vznik preciznějšího vymezení pojmu *accountability* a identifikaci doporučení, kterými se mají řídit jak zákonodárci, tak následně povinné subjekty.[589] V roce 2009 se španělská národní autorita ochrany osobních údajů (*Agencia Española de Protección de Datos*) pokusila ve spolupráci s dalšími evropskými institucemi navrhnout minimální standard ochrany osobních údajů, který měl zafungovat jako prostředek k šíření a sjednocování režimu ochrany osobních údajů po celém světě.[590] Tato snaha vyústila do publikace Madridské rezoluce, která obsahuje minimální společný standard ochrany osobních údajů. Její čl. 11 upravuje zásadu *accountability* následovně: *„The responsible person shall: a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23."*[591] Konečně poslední dokument, který je v kontextu zásady odpovědnosti třeba zmínit, je stanovisko WP 29 č. 3/2010 k zásadě odpovědnosti,[592] ve kterém WP 29 identifikovala zásadu *accountability* správce a její posílení jako jeden ze základních kamenů, na kterém je možné modernizovanou podobu systému ochrany osobních údajů postavit. Obecné nařízení pak obsahuje *accountability* pod českým názvem „zásada odpovědnosti" výslovně uvedenou v čl. 5 odst. 2 a v čl. 24.

Při aplikaci zásady *accountability* na ochranu osobních údajů je do role povinného subjektu postaven správce údajů, který odpovídá za správnost a legálnost svého zpracování osobních údajů. Jak správně podotýká Colin Bennet, je zajímavostí, že praktický v žádném z dokumentů, které se věnují zásadě

589 Výstupy z projektů jsou online k dispozici na stránkách The Information Accountability Foundation. Viz Publications. *The Information Accountability Foundation* [online]. [cit. 30. 6. 2020].

590 Viz ALHADEFF, Joseph, Brendan Van ALSENOY a Jos DUMORTIER. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 61.

591 Čl. 11 Madridské rezoluce. International Conference of Data Protection and Privacy Commissioners (5. 11. 2009). *International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution* [online]. 2009, s. 13 [cit. 30. 6. 2020].

592 PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, 19 s. [cit. 30. 6. 2020].

odpovědnosti, není uvedeno, vůči komu je *accountability* vykazována.[593] Výjimku představuje výše citovaná Madridská rezoluce, která identifikovala *accountability* správce vůči dozorovému orgánu, do jehož gesce ochrana osobních údajů spadá, a rovněž vůči subjektům údajů. Druhou výjimkou je pak WP 29, která v dokumentu *Future of privacy* uvedla, že reforma ochrany osobních údajů má přinést rámec úpravy *accountability* správce údajů, který má zajistit, aby správce dodržoval v průběhu zpracování zásady ochrany osobních údajů a vhodně nastavil vnitřní mechanismy tak, aby mohl prokázat dodržování svých povinností vnějším subjektům včetně úřadů pro ochranu osobních údajů.[594] Obecné nařízení však přesné určení, vůči komu je *accountability* vztažena, neobsahuje.

Vzhledem k tomu, že text Obecného nařízení výslovně neidentifikuje role dalších zúčastněných stran *accountability* vztahu (tedy komu správce údajů odpovídá), je při jejich určení nezbytné vycházet ze vzájemných právních vztahů přítomných v rámci zkoumané právní úpravy. Předně zde figuruje dozorový orgán v podobě úřadu ochrany osobních údajů. V tomto případě je možnost kontroly správce údajů úřadu ochrany osobních údajů dána jednoznačně Obecným nařízením a zákonem, které pravomoci dozorových úřadů stanoví. Úřad je tak k dohledu nad činností správce údajů zmocněn, může provádět kontroly a může sankcionovat nedodržení zákonných požadavků. Vedle toho se v souladu s Madridskou rezolucí domnívám, že *accountability* správce je vykonávána rovněž vůči subjektům údajů, jejichž osobní údaje správce zpracovává.[595] Tento vztah je založen subjektivními pozitivními právy subjektů údajů.[596] Subjekt údajů má v první řadě právo být informován o probíhajícím zpracování, o tom, jaká data jsou jakým způsob a za jakými účely zpracovávána a dále má kupříkladu právo namítat zpracování v případě, že se domnívá, že probíhá protiprávně, nebo vyžadovat smazání dat,

593 BENNET, Colin J. Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 42–43.

594 Viz PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, s. 3 [cit. 30. 6. 2020].

595 Shodně dále viz RAAB, Charles. The Meaning of 'Accountability' in the Information Privacy Context- In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 18.

596 Více viz část 2.3 této publikace.

která již správce nemá důvod uchovávat.[597] Správce má oproti tomu odpovídající povinnost konat tak, aby tato práva byla naplněna. Krom toho, jak bylo argumentováno v části 2.3 této publikace, subjekt se těchto svých práv nemůže vzdát, nemůže je smluvně omezit a tím spíš je nemůže vyloučit jednostranně správce údajů.

Základní otázky *accountability*, tedy „kdo odpovídá", „komu odpovídá" a „za co odpovídá", je tak možné shrnout tak, že správce údajů odpovídá dozorovému orgánu a subjektům údajů, jejichž údaje zpracovává za to, že zpracování probíhá v souladu s požadavky Obecného nařízení.

Zásada *accountability* je v Obecném nařízení vyjádřena v druhém odstavci čl. 5 tak, že správce osobních údajů odpovídá za dodržení ostatních základních zásad zpracování osobních údajů a musí být schopen jejich splnění doložit. Více je pak tato zásada rozvedena v čl. 24, jehož první odstavec zní následovně: *„S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována."*[598] Jedná se o performativní regulaci, protože ustanovení určuje správci údajů cíl zajistit, aby probíhající zpracování bylo v souladu s Obecným nařízením. Již však neupravuje, jaké konkrétní kroky a jakým způsobem má správce podniknout ke splnění stanoveného cíle, a nechává tedy toto rozhodování na něm. Je pouze specifikováno, že konkrétní postup je třeba vztáhnout k povaze, rozsahu, kontextu, účelům zpracování a zejména pak vzhledem k rizikům, která zpracování představuje pro práva a svobody subjektů údajů.[599] Zásada *accountability* správce tak vzhledem ke svému jedinečnému a silnému postavení v rámci systému ochrany osobních údajů umožňuje, aby správce údajů přizpůsobil zpracování své konkrétní situaci. Tím je pak zajištěna nezbytná vnitřní flexibilita právní úpravy. *Accountability*

597 K možnosti výkonu kontroly subjektu údajů nad jeho osobními údaji srovnej rovněž LYNSKEY, Orla. *The foundations of EU data protection law*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2015, s. 179 a násl., Oxford studies in European law.

598 Čl. 24 odst. 1 Obecného nařízení.

599 Tento přístup se rovněž nazývá přístup založený na riziku a detailněji se mu věnuje následující podkapitola. Srovnej například GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2.

ve spojení s hodnocením rizik[600] zpracování umožňuje vytvoření dostatečné škálovatelnosti a granularity povinností správce tak, aby správce opravdu musel plnit jen to, co je nezbytné vzhledem k povaze zpracování a zejména rizikům, které představuje. Čím větší rizika představuje probíhající zpracování pro práva a svobody subjektů údajů, tím extenzivnější prostředky musí správce vynaložit pro to, aby svoji povinnost zajistit bezpečné zpracování splnil. Z uvedeného pak nutně vyplývá i opačná trajektorie. Čím nižší rizika zpracování představuje, tím menší nároky mají být na správce údajů kladeny.[601] Pokud jsou pak rizika minimální, aplikace zásady *accountability* umožňuje, aby na správce vůbec nedopadly povinnosti, které jsou vzhledem k minimální míře rizika nadbytečné a nepřiměřeně zatěžující.[602]

Interpretační závěr připouštějící možnost snížení zatížení povinnostmi v případě nízkého rizika zpracování je nezbytným výsledkem vzhledem k účelům a základním premisám ochrany osobních údajů. Ochrana osobních údajů je preventivní nástroj, který má při pragmatickém přijetí nezbytnosti existence zpracování osobních údajů umožnit a zajistit to, že probíhající zpracování osobních údajů bude vůči subjektům údajů spravedlivé a korektní.

Kapitola 2 této publikace argumentovala, že účelem právní úpravy ochrany osobních údajů je umožnění zpracování a jeho limitace, aby nepřiměřeně nezasahovalo do práv subjektů údajů. Zároveň, jak ukázala kapitola 4 této knihy, zúžení definic klíčových pojmů ani svévolné rozhodnutí nevymáhat určité případy není systematicky přijatelným řešením problému správce údajů v podobě nízké škálovatelnosti povinností.[603] Vzhledem k tomu je pragmaticky třeba identifikovat mechanismus, kterým je vnitřní škálovatelnost

600 K hodnocení rizik více do detailu viz následující část této kapitoly.

601 Shodně viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, s. 13 [cit. 30. 6. 2020]; Opačný názor zastává např. Gonçalves, která tvrdí, že správce může míru zapojení různých ochranných nástrojů jen navyšovat. Viz GONÇALVES, Maria Eduarda. The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research* [online]. 2019, s. 5.

602 Shodně viz QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 504.

603 Zúžením definic klíčových pojmů by došlo k nepřiměřenému snížení ochrany subjektů údajů, protože by zcela ztratily možnost se v daných případech bránit. Nevymáhání je pak klíčový problém z hlediska právní jistoty a zajištění vnitřní konzistence a morálky práva.

povinností uvnitř systému ochrany osobních údajů umožněna. Tímto mechanismem je právě performativní regulace v podobě silné zásady *accountability* zahrnující hodnocení rizik, která se promítá do dalších konkrétních povinností stanovených Obecným nařízením. Případná svévole správce údajů je limitována tlakem, který je na něj vytvářen tím, že je odpovědný (*accountable*) vůči externím subjektům, konkrétně vůči dozorovému orgánu a zejména vůči subjektům údajů. Práva subjektů údajů jsou odrazem práva na informační sebeurčení a plní zásadní roli v limitaci rizika, že by správce údajů snížil míru svých povinností nepřiměřeně vzhledem k probíhajícímu zpracování.[604] Institut zásady *accountability* správce tedy umožňuje, aby správce přizpůsobil danému zpracování konkrétní podmínky zpracování a konkrétní způsob splnění povinností vyplývajících z Obecného nařízení (včetně jejich snížení, nebo až vyloučení) a zároveň byla zachována ochrana a práva subjektů údajů.

Výše uvedené ukazuje, že zásada *accountability* správce má širší dosah a hlubší význam než jen povinnost vést záznamy o zpracování. Není tedy pouhou alternativou k dřívější povinnosti registrace u dozorového orgánu, jak se občas tvrdí. Zásada *accountability* správce představuje fundamentální přesun od nevyhovujícího statického chápání zpracování osobních údajů jako držby informací zafixované okamžikem sběru údajů a udělení souhlasu[605] k dynamickému chápání zpracování jako procesu probíhajícího v čase.[606] Pokud totiž dojde během probíhajícího zpracování k událostem, které způsobí změnu v povaze zpracování a hodnocení jeho rizik, má správce údajů možnost a povinnost zasáhnout a proces zpracování adekvátně upravit. Správce údajů proto musí vyhodnocovat plnění svých povinností vyplývajících ze zásady *accountability* i průběžně, zatímco ke zpracování dochází, a upravovat adekvátně své kroky a postupy. Konkrétní provedení povinností identifikovaných při hodnocení zpracování ve světle zásady *accountability*

604 Právě uvedené je možné demonstrovat tím, že Obecné nařízení vyšší sazbu sankce stanoví za porušení povinností vyplývajících z práv subjektů údajů. Viz čl. 83 odst. 5 Obecného nařízení.

605 Viz POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 2 [cit. 30. 6. 2020].

606 Shodně viz WEITZNER, Daniel J. et al. Information Accountability. *Communications of the ACM* [online]. 2008, roč. 51, č. 6, s. 87.

však musí být skutečné a hmatatelné.[607] Správce údajů svoji povinnost nesplní, pokud pouze formálně (byť perfektně) povede záznamy o zpracování, které by však byly jen seznamem zaškrtaných políček neodpovídajících konkrétním požadavkům daného zpracování.[608] Pro řádné fungování principu *accountability* je pak nezbytné zajištění a umožnění efektivní kontroly činnosti správce, a to jak ze strany dozorového úřadu, tak ze strany subjektů údajů. Bez fungujícího dozoru a efektivních sankcí by mohlo hrozit, že proces plnění povinností vyplývajících ze zásady *accountability* se stane jen formálním postupem, aniž by byly naplněny cíle právní úpravy.[609]

Zásada *accountability* je performativním pravidlem, když stanoví, že každý správce má vzhledem k reáliím konkrétního zpracování uzpůsobit jeho podmínky tak, aby byly patřičně splněny další požadavky vyplývající z Obecného nařízení. Jak vyplynulo z části 5.1 této knihy, zcela zásadní otázkou při aplikaci performativních pravidel je, jak je formulovaný cíl, kterého má povinný subjekt dosáhnout. Vůči jakému standardu se jeho plnění poměřuje. V případě zásady *accountability* je tímto standardem primárně riziko, které zpracování osobních údajů představuje pro práva a svobody subjektů údajů. Zásada *accountability* správce tedy umožňuje vzhledem k povaze zpracování a riziku, které představuje, „vyplnit mezery" tam, kde by jinak vznikaly přísně taxativně určeným seznamem povinností. Hodnocení rizika, které zpracování přináší, je proto základním nástrojem při aplikaci performativního pravidla

607 Tento aspekt například dokazuje, že regulace prostřednictvím zásady odpovědnosti je ve skutečnosti opravdu regulací performativní v přísném Coglianesově významu performance-based regulace a nikoli management-based. O tu by se jednalo tehdy, pokud by splnění povinnosti cílilo primárně na provedení analýzy chystaného zpracování a nikoli na výsledek.

608 Shodně viz QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 503; Dále též KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*. 2012.

609 Obdobně srovnej HERT, Paul de. Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 222.

zásady *accountability*. I vzhledem k tomu je současná právní úprava v podobě Obecného nařízení označována jako přístup založený na riziku.[610]

5.3 Jádro principu odpovědnosti: Rizikovost zpracování

Tato podkapitola je věnována otázce, jak se hodnocení rizik projevuje ve spojitosti se zásadou *accountability* správce při interpretaci ustanovení Obecného nařízení. Je třeba předeslat, že není jejím cílem zabývat se konkrétně tím, jak hodnocení rizik zpracování osobních údajů provádět.[611] Naopak, cílem této kapitoly je analyzovat, jakým způsobem se riziko představované zpracováním osobních údajů projevuje při interpretaci ustanovení Obecného nařízení.

Ačkoli hodnocení rizik bylo v omezené míře přítomné již v předcházející právní úpravě,[612] klíčovým prvkem regulace se stalo až s příchodem Obecného nařízení. Pojem „riziko" podléhá celé řadě vymezení. Definici kombinující běžné a vědecké chápání pojmu riziko nabídl Lawrence B. Gratt: *„The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment; estimation of risk is usually based on the expected result of the conditional probability of the event occurring times the consequence of the event given that it has occurred."*[613] Obdobně přistupují k riziku Vladimír Smejkal a Karel Rais, když o riziku hovoří jako o *„situaci, v níž existuje možnost nepříznivé*

610 Srovnej například GONÇALVES, Maria Eduarda. The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research* [online]. 2019; GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2; MACENAITE, Milda. The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3.

611 V kontextu praktického provádění hodnocení rizik je možné odkázat např. na Handbook on Security of Personal Data Processing. *ENISA* [online]. 2017, 68 s. [cit. 30. 6. 2020]; Privacy Impact Assessment (PIA). *CNIL* [online]. 2018, 109 s. [cit. 30. 6. 2020]; nebo ČSN ISO/IEC 29134, Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí.

612 Novák připomíná, že na vhodném vyhodnocení rizika spočívalo správné splnění § 13 zákona č. 101/2000 Sb., který byl věnován povinnostem správce při zabezpečení osobních údajů (viz NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Dostupné z: *ASPI* [Právní informační systém, text aktuální k 1. 7. 2017]).

613 GRATT, Lawrence B. Risk Analysis or Risk Assessment; A Proposal for Consistent Definitions. In: COVELLO, Vincent T. et al. (eds.). *Uncertainty in risk assessment, risk management, and decision making*. New York; London: Plenum Press, 1987, s. 244.

odchylky od žádoucího výsledku".[614] Důležitým aspektem rizika je dle této autorské dvojice rovněž čas, během nějž hodnocený proces probíhá a během kterého může dojít ke zmíněné nepříznivé odchylce.[615] O riziku pak nemusíme mluvit jen v kontextu s negativními odchylkami, ale rovněž o činnosti s nejasným budoucím výsledkem, který může být pozitivní.[616] Riziko v kontextu s ochranou osobních údajů vhodně minimalisticky vymezuje István Böröcz jako pravděpodobnost události znásobená mírou jejího důsledku.[617]

Ochrana osobních údajů není jedinou oblastí právní úpravy, ve které dochází k intenzivnímu zapojení hodnocení rizika do regulatorního rámce. Již dříve se tento přístup objevil v celé řadě oblastí od zdravotnictví, ochrany životního prostředí, finančnictví až po právní ochranu dětí.[618] Henry Rothstein tento proces nazývá kolonizací rizik (*„risk colonization"*),[619] Milda Macenaite pak *„riskifikace"*.[620] Je však důležité rozlišit regulaci rizik (*„risk regulation"*) a regulaci postavenou na riziku (*„risk based regulation"*). První jmenovaný označuje snahu zákonodárce prostřednictvím přijatých předpisů riziku zabránit, omezit jej, případně snížit na přijatelnou míru rizika hrozícího obyvatelům nebo statkům a zájmům, kterých se norma dotýká. Z tohoto pohledu je Obecné nařízení regulací rizik, protože jeho účelem je snížení nežádoucích dopadů zpracování na subjekty údajů.[621] Oproti tomu druhý jmenovaný

614 SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada, 2006, s. 79.

615 Viz Ibid.

616 Viz ROTHSTEIN, Henry, Michael HUBER a George GASKELL. A theory of risk colonization: The spiralling regulatory logics of societal and institutional risk. *Economy & Society* [online]. 2006, roč. 35, č. 1, s. 92; Totéž uvádějí i Smejkal s Raisem v kontextu podnikatelského rizika (viz SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada, 2006, s. 80).

617 BÖRÖCZ, István. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 479.

618 Srovnej ROTHSTEIN, Henry, Olivier BORRAZ a Michael HUBER. Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe. *Regulation & Governance* [online]. 2013, roč. 7, č. 2, s. 216.

619 Viz ROTHSTEIN, Henry, Michael HUBER a George GASKELL. A theory of risk colonization: The spiralling regulatory logics of societal and institutional risk. *Economy & Society* [online]. 2006, roč. 35, č. 1.

620 MACENAITE, Milda. The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3.

621 Pro více příkladů viz HOOD, Christopher et al. Explaining risk regulation regimes: exploring the "minimal feasible response" hypothesis. *Health, Risk & Society* [online]. 1999, roč. 1, č. 2.

fenomén spočívá v regulatorní metodě, která pracuje s rizikem jako s metodou zajištění efektivního plnění povinností regulovanými subjekty. Obecné nařízení je podloženo zásadou *accountability* správce provázanou s regulací postavenou na riziku.[622] To se projevuje tak, že správce údajů má přizpůsobit konkrétní způsob provedení daného zpracování rizikům, která představuje pro práva a zájmy (nejen) subjektů údajů. Zde je nutné připomenout, že čl. 24 Obecného nařízení hovoří o různě závažných rizicích pro práva a svobody fyzických osob.[623] Rozsah možného zásahu způsobeného zpracování je tak výrazně širší a při hodnocení rizik je nutné brát v potaz rovněž práva a zájmy jiných osob, včetně zájmů společenských, a vůči nim přizpůsobit chystané a probíhající zpracování.[624] V kontextu Obecného nařízení je dále možné říct, že přístup založený na riziku rovněž umožňuje přiměřené a škálovatelné splnění povinností (*compliance*) z něj vyplývajících.[625]

Rozdíl mezi regulací rizik a regulací postavenou na riziku v kontextu ochrany osobních údajů je možné demonstrovat ještě na příkladu hodnocení rizik v průběhu legislativního procesu. V souladu s legislativními pravidly vlády[626] a s Obecnými zásadami pro hodnocení dopadů regulace (RIA)[627] má zákonodárce povinnost provést v průběhu legislativního procesu hodnocení rizik nové úpravy na právo na soukromí a ochranu osobních údajů. Jedná se samozřejmě o obecné zhodnocení, zda na základě nového předpisu dochází

622 Viz QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 510–11.

623 Detailněji je aspekt rizika v kontextu ochrany osobních údajů rozebrán v bodě 75 odůvodnění Obecného nařízení.

624 Shodně viz BÖRÖCZ, István. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 480.

625 Viz MACENAITE, Milda. The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3, s. 517; Claudia Quelle nazývá plnění povinností, které si regulovaný subjekt sám *de facto* stanovuje na základě vyhodnocení rizika zpracování, *„compliance 2.0"*. Viz QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 518 a násl.

626 Viz čl. 4 odst. 3 písm. g) a čl. 9 odst. 2 písm. h) Legislativních pravidel vlády (Legislativní pravidla vlády, ve znění pozdějších usnesením vlády. *Vláda České republiky* [online]. [cit. 30. 6. 2020]).

627 Obecné zásady pro hodnocení dopadů regulace (RIA). *Vláda České republiky* [online]. 2016, 34. s. [cit. 25. 6. 2019].

ke zpracování osobních údajů a pokud ano, zda je takové zpracování ústavně konformní a přiměřené plánovanému účelu úpravy. Jde tedy o typický příklad regulace rizik. Jiná situace nastává v okamžiku, kdy je takováto úprava účinná a dopadne na povinný subjekt, který se tak dostává do pozice správce údajů. Vzhledem k tomu nese za zpracování odpovědnost (ve smyslu obecném i *accountability*) a v rozsahu, který zákon neupravuje, musí přizpůsobit své zpracování podmínkám a rizikům, které představuje. V tomto případě se aplikuje Obecné nařízení jako případ regulace postavené na rizicích. Netřeba zdůrazňovat, že se jedná o dva zcela odlišné procesy s rozdílnými východisky i výstupy, které není možné zaměňovat.

Velice překvapivé a problematické je proto § 10 zákona č. 110/2019 Sb., který stanoví, že *„Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést."*[628] Je třeba dále připomenout, že pojem „hodnocení rizik", o kterém tato část pojednává, a posouzení vlivu na ochranu osobních údajů, které je jako zvláštní povinnost správce údajů upraveno v čl. 35 Obecného nařízení, jsou dva odlišné postupy. Hodnocení rizik, které bychom mohli označit jako „malé", musí vždy provést každý správce, protože je nedílnou součástí zásady *accountability*. Správce odpovídá za své zpracování a za to, že bude probíhat dobře. V tom se neliší situace, kdy zpracovává na základě zákonné povinnosti a kdy na základě jiného právního titulu. Pokud na základě tohoto „malého" hodnocení rizik správce zjistí, že chystané zpracování bude mít za následek vysoké riziko, musí provést „velké hodnocení rizik", tedy posouzení vlivu zpracování podle čl. 35 Obecného nařízení.[629] Výsledný dokument má správci údajů napovědět, jak zpracování zabezpečit, aby se rizika minimalizovala. Český zákonodárce se zde generálním vyloučením nutnosti vykonat posouzení dopadů zpracování před jeho zahájením dopustil ve snaze o usnadnění plnění povinností značné zkratky, která může v konečném důsledku vést ke snížení ochrany subjektů údajů.

628 Viz § 10 zákona č. 110/2019 Sb.

629 WP 29 vydala detailní pokyny, na základě kterých je možné určit podmínky, kdy je třeba posouzení vlivu vykonat. Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679. *Evropská komise* [online]. 4. 4. 2017, v revidovaném znění ze dne 4. 10. 2017, č. WP248rev.01, 24 s. [cit. 30. 6. 2020].

Při malé znalosti problematiky na straně správců údajů může totiž dojít k tomu, že řádně neprovedou ani „malé" hodnocení rizik, čímž si fakticky znemožní řádně plnit povinnosti, které jim vyplývají ze zásady *accountability*.

Dalším mírně problematickým aspektem přístupu postaveného na riziku je vymezení, co znamená pojem „riziko pro práva". Niels van Dijk představil se svými kolegy detailní analýzu, ve které se zabývá různými variantami možných vztahů mezi koncepty rizika a práva.[630] To dále rozvedl Böröcz, když v návaznosti na výše uvedenou obecnou definici rizika („pravděpodobnost události znásobená mírou jejího důsledku") uvádí, že rizikem pro právo je jeho omezení. Doslova píše: *„In case of the risk to the right to the protection of personal data the GDPR describes circumstances under which the processing operation is compliant with the rules. Therefore, the severity of this risk should be visualised in a two grade scale: the processing of personal data is either violating or non violating legal provisions."*[631] S uvedenou Böröczovou myšlenkou souhlasím. Pokud je riziko chápáno jako nežádoucí výsledek v podobě zásahu do oblasti zájmu, vůči které se riziko poměřuje, tak v případě „rizika pro právo" musí být nutně tímto nežádoucím výsledkem jedině protiprávní porušení nebo omezení předmětného subjektivního práva. Při hodnocení zpracování osobních údajů z hlediska závažnosti rizika pro práva tak může výsledek nabývat dvou základních hodnot: hrozí porušení a nehrozí porušení. V případě hrozícího porušení je pak možné ještě míru závažnosti rizika upravit případnou intenzitou porušení práva, škodlivými následky, povahou poškozeného (pokud jde např. o dítě nebo jinak znevýhodněnou osobu), povahou zpracovávaných osobních údajů a podobně. Bližší specifikace hrozícího rizika dle těchto faktorů je pak již vyjádřena na tradiční stupnici rizik jako nízké, střední a vysoké riziko. Je však třeba zdůraznit, že tento způsob hodnocení rizika bude ve svém jádru vždy kvalitativní, protože není možné kvantifikovat zásah do práv a test proporcionality.

Výše uvedené je možné propojit do dílčího závěru, že zásada *accountability* správce údajů zakládá jeho povinnost hodnotit před zahájením zpracování

630 DIJK, Niels van, Raphaël GELLERT a Kjetil ROMMETVEIT. A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2.

631 BÖRÖCZ, István. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 476.

i v jeho průběhu rizika spočívající v možnosti různě intenzivního porušení práv a zájmů třetích osob a tomuto hodnocení přizpůsobit průběh zpracování osobních údajů a splnění dalších povinností uvedených v Obecném nařízení tak, aby byla rizika minimalizována a aby zpracování odpovídalo jejich intenzitě. Je zde tedy přímo přítomná škálovatelnost a granularita povinností správce údajů. V případě vyššího rizika musí správce údajů škálovat své povinnosti a jejich splnění nahoru (nebo v rámci granularity povinností začít plnit povinnost novou) a podnikat kroky navíc, kterými riziko sníží (např. zavést více ochranných prostředků, nebo jmenovat pověřence údajů dle čl. 37 Obecného nařízení). V případě nižšího rizika naopak může škálovat povinnosti související se zpracováním dolů a určité povinnosti plnit méně důkladně, nebo je v určitých případech nemusí plnit prakticky vůbec.[632] Obdobně pak bude platit, vzhledem k formulaci zásady *accountability* jako jednoho ze základních principů, na kterém Obecné nařízení spočívá, že by dozorový úřad měl udělovat v případě málo rizikových zpracování minimální až nulové sankce, zatímco v případě vysoko rizikových zpracování může sáhnout po celé škále, kterou má k dispozici.

Jak uvádí Raphaël Gellert, s přibývajícím teoretickým zájmem, který se novému přístupu postaveném na riziku z řad autorů dostával, docházelo nezbytně k hodnocení vztahu mezi ním a předcházejícím principem regulace, který byl následně nazván *„přístup založený na právech"*.[633] Tím je za prvé myšleno, že se právo na ochranu osobních údajů vztahuje na všechny případy zpracování osobních údajů bez ohledu na jejich rizikovost a za druhé, že v případě střetu dvou práv je výsledek určen na základě jejich poměřování a testu proporcionality. Vystavění pevné hranice mezi přístupem postaveným na riziku a na právech by však bylo chybou. Neplatí, že by s příchodem

632 Stejný názor zastává např. bývalý Evropský inspektor ochrany údajů Peter Hustinx [viz HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 160]; Ve stejném duchu se vyjadřuje rovněž WP 29 (PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, odst. 45 a 47, s. 12–13 [cit. 30. 6. 2020]).

633 GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 483.

Obecného nařízení právní úprava zcela rezignovala na práva a nadále při řešení střetů mezi různými zájmy jen porovnávala rizika. Metoda regulace postavená na zásadě *accountability* a hodnocení rizik není oddělená od úpravy založené výhradně na jasně formulovaných právech a povinnostech, jak tomu bylo v případě směrnice 95/46/ES. Nenahrazuje ji, naopak na ní staví a doplňuje ji, díky čemuž jí dodává dostatečnou flexibilitu v podobě granularity a škálovatelnosti povinností správce při probíhajícím zpracování.[634]

Právě uvedené je možné ukázat na dvou příkladech. Za prvé, je třeba odmítnou názor, že by na základě hodnocení rizikovosti zpracování bylo určováno, zda se na daný proces bude nebo nebude právní úprava ochrany osobních údajů vůbec aplikovat. S tímto návrhem přišla Eloise Gratton, když ve svém textu z roku 2014 navrhovala za osobní údaje (a tedy informace podléhající režimu ochrany osobních údajů) považovat pouze ty, jejichž zpracování představuje riziko újmy pro subjekty údajů.[635] Tento přístup však v kontextu ochrany osobních údajů není možný, a to hned ze dvou důvodů. Krom toho, že nemá oporu v textu předpisu, je druhým a zásadnějším důvodem prevenční princip ochrany osobních údajů. Obecně platí, že riziko není nikdy možné zcela vyloučit, lze ho jen minimalizovat.[636] Navíc i v případech, kdy je riziko zcela zanedbatelné, je vzhledem k zachování možnosti vykonávat právo na informační sebeurčení (tedy vzhledem k zajištění jednoho z účelů právní úpravy ochrany osobních údajů) zcela nezbytné, aby subjekt údajů měl možnost vykonávat svá subjektivní práva. Pokud bychom přijali jako možnost, že by se za osobní údaje považovaly jen takové informace,

634 Srovnej BENNET, Colin J. Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 46; Shodně též PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement on the role of a risk-based approach in data protection legal frameworks. *Evropská komise* [online]. 30. 5. 2014, č. 14/EN, WP 218, 4 s. [cit. 30. 6. 2020]. Jako praktický příklad může posloužit povinnost správce zabezpečit zpracování osobních údajů. Tam kde § 13 zákona č. 101/2000 Sb. stanovil jednoznačný seznam procesů, které správce musí vykonat, aby zabezpečil své zpracování, dává nyní čl. 32 Obecného nařízení správci volnou ruku, aby si sám zvolil, co je pro jeho zpracování nezbytné.

635 Viz GRATTON, Eloise. If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm Is the Key: A Proposed Method for Determining What Counts as Personal Information. *Albany Law Journal of Science & Technology,* 2014, roč. 24, č. 1, s. 88.

636 Viz GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law* [online]. 2015, roč. 5, č. 1, s. 15–16.

jejichž zpracování představuje riziko, dostali bychom se do podobné situace jako v případě subjektivního přístupu k definici osobních údajů. Jak ukázala kapitola 4 této publikace, je nutné takové závěry odmítnout.

Za druhé, i v případě přístupu založeného na riziku jsou standardní metody poměřování různých práv stále relevantní. „Riziko pro právo" znamená riziko jeho porušení v podobě protiprávního zásahu. Z uvedeného vyplývá, že tam, kde k porušení práva nedochází nebo kde takové porušení nehrozí, není ani přítomné riziko pro právo. V případech střetu dvou práv je proto třeba před vyhodnocením existence rizika nejprve provést standardní test proporcionality a až na základě jeho výsledku je možné přizpůsobit zpracování údajů a splnění souvisejících povinností tak, aby případnému riziku a jeho velikosti odpovídalo. Pro příklad je možné uvést tradiční střet ochrany soukromí a osobních údajů s právem na informace v podobě nálezu ÚS ve věci sp. zn. I. ÚS 517/10, ve kterém soud rozhodl o oprávněnosti zveřejnění informací o soudcích, kteří byli před rokem 1989 členy KSČ.[637] V takovém případě nepředstavuje samotný izolovaný akt zveřejnění osobních údajů žádné riziko, protože je v souladu s právem. Riziko bychom však mohli najít například v případě chybného záznamu, kdyby správce údajů umožnil neoprávněnému člověku přístup do zveřejňované databáze soudců a její editaci, nebo pokud by zveřejněné údaje byly dále užity neproporcionálním způsobem. Přístup postavený na riziku představuje ruku v ruce se zásadou *accountability* správce *de facto* nadstavbu nad standardním hodnocením jednotlivých práv zúčastněných subjektů. Tento fakt vystihla Claudia Quelle, když tvrdí: *„The risk-based approach does not replace the principles and rules of data protection. Instead, it requires controllers to calibrate what it means, according to the law, to protect the rights and freedoms of data subjects. In other words, the risk-based approach, as we know it, does not reduce data protection law to risk analysis. Instead, it uses the notion of risk to regulate how controllers should implement the law in practice."*[638] Proto v případech, kdy zpracování představuje větší riziko pro práva dotčených osob, musí správce údajů dělat více a plnit své

637 Nález Ústavního soudu ze dne 15. 11. 2010, sp. zn. I. ÚS 517/10, č. N 223/59 SbNU 217.

638 QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 512.

povinnosti zodpovědněji. A naopak, v případech, kdy je riziko malé, může správce údajů v plnění svých povinností polevit.[639]

Detailnímu rozboru, které povinnosti správce údajů uvedené v Obecném nařízení je možné škálovat, je věnována následující podkapitola. Již nyní je ale nezbytné upozornit na zásadní oblast, která možnosti přizpůsobení povinnosti na základě rizikovosti zpracování nepodléhá. Jedná se o subjektivní pozitivní práva subjektu údajů formulovaná v kapitole III Obecného nařízení (čl. 12–23), a to pro roli, kterou hrají v systému ochrany osobních údajů.[640] Jak bylo dovozeno v kapitole 2 této publikace, tato práva umožňují subjektu údajů vykonávat své právo na informační sebeurčení, jsou hlavním prostředkem pro narovnání informační asymetrie mezi správcem a subjektem údajů a není je proto možné omezit, ani se jich vzdát. V kontextu principu *accountability* a přístupu založeném na riziku pak hrají rovněž zásadní roli jako nástroj umožňující kontrolu, kterou subjekt údajů může nad správcem vykonávat. Díky nim se správce osobních údajů zodpovídá svým subjektům (je *„accountable to"*). Vzhledem k těmto důvodům je nezbytné, aby je měl subjekt údajů možnost využít, když si to bude přát.

Obecné nařízení nabízí několik výjimek a modifikací těchto práv v případě, že správce provádí zpracování, které bychom mohli označit jako málo rizikové. Např. čl. 14 odst. 5 písm. b) umožňuje výjimku z informační povinnosti správce, pokud by poskytnutí informace o zpracování nebylo možné, nebo by vyžadovalo nepřiměřené úsilí. Stejně tak čl. 11 poskytuje obecnou výjimku z povinností, pro jejichž splnění by správce musel získat osobní údaje, které jinak vzhledem k účelu svého zpracování nepotřebuje. Všechny výjimky, které se týkají práv zakotvených v kapitole III Obecného nařízení, jsou však jednoznačně formulovány a neobsahují odkaz na hodnocení rizik konkrétního zpracování.

639 Srovnej rovněž GONÇALVES, Maria Eduarda. The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research* [online]. 2019, s. 5.

640 Ohledně důležitosti pozitivních subjektivních práv subjektu údajů viz část 2.3 této publikace.

5.4 Praktické dopady hodnocení rizik v Obecném nařízení

Dílčím závěrem minulých částí této kapitoly je, že performativní regulace v podobě zásady *accountability* správce ve spojení s regulací postavenou na riziku, které Obecné nařízení nově přineslo, umožňuje škálovatelnost a granularitu povinností, které Obecné nařízení správcům údajů ukládá. Jinými slovy na základě toho, jaké riziko dané zpracování představuje pro práva a zájmy subjektů údajů nebo dalších fyzických osob, musí správce údajů určit, jaké povinnosti popsané v Obecném nařízení se ho týkají (granularita povinností) a jakým způsobem mají být splněny (škálovatelnost povinnosti). Čím větší riziko zpracování osobních údajů představuje, tím větší jsou na správce kladeny požadavky, které musí splnit, aby byl v souladu s Obecným nařízením. A naopak, čím je riziko menší, tím méně toho správce musí plnit.

K výše uvedenému závěru dojdeme z textace čl. 24 Obecného nařízení. Jeho první odstavec zní: *„S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.“*[641] Citovaný odstavec na první pohled připomíná bývalou úpravu v podobě čl. 17 odst. 1 směrnice 95/46/ES.[642] Na rozdíl od ní se však čl. 24 Obecného nařízení netýká pouze otázky zabezpečení zpracování, ale komplexně všech povinností uvedených v Obecném nařízení, jak vyplývá z formulace na konci první věty, která požaduje zajistit soulad s celým Obecným nařízením.[643] Čl. 24 sám, respektive jeho porušení, nemůže posloužit jako základ pro sankci podle čl. 83 Obecného nařízení. To potvrzuje jeho „provozní“ povahu. Působí tedy primárně jako prostředek zanesení hodnocení rizika do plnění dalších povinností správce údajů.

641 Čl. 24 odst. 1 Obecného nařízení.

642 Ten zněl: *„Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování. Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti.“*

643 Shodně viz MACENAITE, Milda. The “Riskification” of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3, s. 524.

Vzhledem k tomu, že při různých zpracováních osobních údajů identifikujeme různá rizika různé výše, a vzhledem k tomu, že (jak ukázala zkušenost regulace směrnicí 95/46/ES) neplatí, že by se ke všem zpracováním dalo přistupovat totožně,[644] musíme uvažovat o různých úrovních povinností.[645] Některé povinnosti správce uvedené v Obecném nařízení se aplikují pouze v případě přítomnosti vyšší míry rizika, další není při nižší míře rizika třeba aplikovat vůbec (granularita). Většina povinností správce může být splněna různými způsoby a je pouze na správci údajů, aby vybral vhodný způsob odpovídající konkrétnímu zpracování a riziku, které představuje (škálovatelnost).[646] Obecné nařízení obsahuje rovněž povinnosti správce, na které úprava vyplývající z míry rizika zpracování vůbec nedopadá. V každém případě má však správce údajů povinnost hodnotit, jak se situace mění v čase, a podle toho plnění svých dalších povinností náležitě upravovat.

Jako příklad je možné uvést hned několik základních zásad zpracování osobních údajů formulovaných v čl. 5 Obecného nařízení. Pro připomenutí – jeho druhý odstavec (zásada odpovědnosti ve smyslu *accountability)* vnáší do plnění zásad uvedených v odstavci prvním performativní princip, který se pak v souladu s čl. 24 odvíjí (mimo dalších faktorů) primárně od rizikovosti zpracování údajů. Žádná ze zásad není rizikem zpracování ovlivněna ve smyslu granularity, tedy že by se některá na základě míry rizika začala nebo přestala aplikovat. Všechny zásady jsou aplikovatelné v každém případu zpracování údajů. Míra rizika zpracování se však projeví na škálovatelnosti povinností vyplývajících z těchto zásad. Obecně škálovatelné budou povinnosti vyplývající ze zásady korektnosti (správce sice musí zajistit,

644 Jak uvádí Colin Bennet: *„One size does not fit all – therefore we can adapt, bend, massage, interpret, and perhaps weaken the standards."* BENNET, Colin J. Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 44.

645 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement on the role of a risk-based approach in data protection legal frameworks. *Evropská komise* [online]. 30. 5. 2014, č. 14/EN, WP 218, s. 3 [cit. 30. 6. 2020].

646 Claudia Quelle používá obdobné dělení povinností správců údajů. Uvedené kategorie označuje jako „Obligations which Require a Risk-Oriented Result" a „Obligations which Require a Risk-Oriented Effort". Viz QUELLE, Claudia. The 'Risk Revolution' in EU Data Protection Law: We can't Have Our Cake and Eat it, Too. In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 56–57.

aby v daném kontextu bylo zpracování korektní, stále je třeba mít na paměti i druhý účel právní úpravy osobních údajů v podobě umožnění korektního zpracování), integrity a důvěrnosti (čím rizikovější je zpracování osobních údajů, tím více musí správce investovat do zajištění jeho zabezpečení a naopak). Škálovatelnost však najdeme, byť v omezené míře, rovněž v zásadách zákonnosti (zde se projevuje hodnocení rizika v případě právního titulu oprávněného zájmu správce),[647] účelového omezení[648] a přesnosti. Posledně jmenovaná zásada je specifická v tom, že už její samotné porušení vytváří riziko pro práva a zájmy subjektů údajů. Škálovatelnost v jejím případě tak určitě nemůže spočívat v tom, že by měl správce možnost zpracovávat nepřesné údaje v případě málo rizikových zpracování. Můžeme ji ale spatřit v míře nezbytných investic vynaložených na identifikaci a opravu chybných údajů. Čím rizikovější je dané zpracování osobních údajů, tedy čím závažnější jsou případné negativní dopady pro subjekty údajů, tím víc musí správce investovat do kontroly svých dat.

Zásady minimalizace údajů a omezení uložení budou naopak vůči škálovatelnosti imunní. K tomuto závěru je třeba dojít, pokud vezmeme v potaz účely a principy právní úpravy ochrany osobních údajů, jak byly pojednány v druhé kapitole této publikace. Zásada minimalizace údajů působí jako maxima limitující zpracování, když stanoví správci povinnost pracovat jen s údaji, které nezbytně potřebuje. Podobně jako v případě zásady přesnosti představuje existence údajů, které správce vzhledem k účelu zpracování nepotřebuje, sama o sobě riziko pro práva a zájmy subjektu údajů. Na rozdíl od zásady přesnosti zde ovšem není možné uvažovat o plnění této povinnosti jako o procesu, do kterého je možné investovat více či méně dle potřeby a míry rizika. Správce buď zpracovává, nebo nezpracovává data, která vzhledem k účelu zpracování nepotřebuje a není zde možnost volby třetí cesty. To samé pak platí i pro zásadu omezení uložení.

Typickými příklady škálovatelných povinností správce osobních údajů, u kterých není třeba pochybovat o možnosti (a nezbytnosti) přizpůsobení konkrétního provedení dané situaci, je povinnost záměrné ochrany osobních

647 Detailnější argumentace viz dále.

648 Míra rizika je jedním z faktorů, který se projevuje při hodnocení možnosti zpracování pro jiný účel dle čl. 6 odst. 4 Obecného nařízení. Detailnější argumentace viz dále v části 5.5.

údajů (*data protection by design*) dle čl. 25[649] a povinnost zabezpečení zpracování dle čl. 32. Obě tyto povinnosti se uplatní při každém zpracování osobních údajů, ovšem jejich specifické provedení záleží na povaze a rizicích konkrétního zpracování. Obě povinnosti se pak vzájemně doplňují. Pokud například správce bude investovat více prostředků do přípravy svého procesu zpracování a pečlivého dodržení povinnosti záměrné ochrany osobních údajů, dojde k celkovému snížení rizikovosti zpracování jako takového a tím pádem bude povinnost vyplývající z čl. 32 dostatečně splněna vynaložením nižších nákladů.

Jako příklad granularity povinností, kdy se na základě míry rizikovosti zpracování určité povinnosti správce začínají nebo naopak přestávají aplikovat, je možné uvést čl. 34, který při vysokém riziku v případě porušení zabezpečení osobních údajů zakládá povinnost správce přímo informovat o této události postižené subjekty údajů. Příkladem granularity povinností, která se ubírá opačným směrem a s nižším rizikem zakládá výjimky, je čl. 27 Obecného nařízení. Tento článek v odst. 1 zakládá povinnost správce osobních údajů, na kterého dopadá extrateritoriální působnost Obecného nařízení dle čl. 3 odst. 2, aby jmenoval na území Evropské unie svého zástupce. Tato povinnost se však nevztahuje na případy, kdy zpracování představuje nízké riziko.[650]

Jak vyplývá z předchozích odstavců, správce osobních údajů je v důsledku použití zásady *accountability* a hodnocení rizika postaven do situace, kdy musí být sám schopen určit, které konkrétní povinnosti vyplývající z Obecného nařízení má plnit, a zároveň, jakým způsobem je má plnit.[651] To celé na základě vyhodnocení, jakým způsobem může svým zpracováním zasáhnout do práv a zájmů subjektů údajů. Dobře tuto situaci vystihla Claudia Quelle: *„The risk-based approach requires controllers to calibrate, and even to second-guess, the rules*

649 Více k principům *data protection by design* a *privacy by design* například viz BALBONI, Paolo a Milda MACENAITE. Privacy by design and anonymisation techniques in action: Case study of Ma3tch technology. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 4; HILDEBRANDT, Mireille a Laura TIELEMANS. Data protection by design and technology neutral law. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5; JASMONTAITE, Lina et al. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. *European Data Protection Law Review (EDPL)*. 2018, roč. 4, č. 2; KLITOU, Demetrius. *Privacy-invading technologies and privacy by design*. New York, NY: Springer Berlin Heidelberg, 2014.

650 Analogicky srovnej argumentaci k výjimce z povinnosti vedení záznamů o zpracování dle čl. 30 Obecného nařízení, viz část. 5.4.2 dále.

651 Součástí *compliance* s režimem ochrany osobních údajů je tak v první řadě identifikace konkrétních povinností, které na správce opravdu dopadají.

put in place by the legislature. It accords to them a responsibility that they did not formally possess before: the responsibility to ensure that data protection law sufficiently protects the rights and freedoms of individuals without imposing disproportionate burdens or limitations."[652] Obecné nařízení tak ve své podstatě normalizovalo to, co formuloval SDEU v rámci rozhodnutí ve věci *Google Spain*, tedy že správce údajů musí provádět test proporcionality.[653] Připomeňme, že riziko pro právo nebo zájem je riziko, že dané právo nebo zájem budou porušeny. Správci osobních údajů musí při nastavení svého zpracování aktivně hodnotit riziko, které může představovat pro práva subjektů údajů, což znamená, že musí aktivně pracovat s proporcionalitou konfliktních práv a zájmů. Správce údajů zároveň v souladu se zásadou *accountability* musí být schopen prokázat dozorovému úřadu a subjektům údajů, že způsob, který zvolil pro splnění svých povinností (tedy jaké povinnosti a jakým konkrétním způsobem), je vzhledem k povaze a rizikovosti probíhajícího zpracování správný.

Následující podkapitoly jsou věnovány detailnějšímu popisu vybraných konkrétních institutů ochrany osobních údajů, ve kterých se hodnocení rizika při jejich aplikaci projeví.[654]

5.4.1 Oprávněný zájem správce

Oprávněný zájem správce nebo třetí strany je posledním právním titulem jmenovaným v čl. 6 odst. 1 Obecného nařízení, který může oprávnit probíhající zpracování. Text tohoto právního titulu, tak jak je přítomný v Obecném nařízení, se drobně odlišuje od podoby, v jaké byl uveden v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Ten uváděl, že správce údajů může údaje zpracovávat *„pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního*

652 QUELLE, Claudia. The 'Risk Revolution' in EU Data Protection Law: We can't Have Our Cake and Eat it, Too. In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 53, Law, Governance and Technology Series, volume 36.

653 Viz rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

654 Příklady byly vybrány na základě toho, že dle mého názoru představují klíčové dílčí otázky praktické aplikace přístupu postaveného na riziku a je jim proto třeba věnovat větší prostor.

života."[655] V případě Obecného nařízení je však třeba na straně subjektu údajů vážit možný zásah do všech jeho práv, svobod a zájmů, tedy nejen do práva na ochranu soukromého a osobního života. Tento posun reflektuje účel práva na ochranu osobních údajů v podobě ochrany fyzických osob před zásahem do jejich práv a svobod nekorektním zpracování osobních údajů a osamostatnění práva na ochranu osobních údajů jako základního práva. Díky tomu je také poskytnuta vyšší úroveň ochrany subjektům údajů a třetím osobám, které by mohly být zpracováním negativně zasaženy.

Správce údajů se na právní titul oprávněného zájmu může spolehnout pouze tehdy, když v daném případě nemají před zájmy správce (nebo třetí strany) přednost práva a zájmy subjektu údajů. Před zahájením zpracování osobních údajů na základě tohoto právního titulu tak správce údajů musí provést test proporcionality, ve kterém srovná zájmy subjektu údajů a zájmy stojící na straně zpracování.[656] Oprávněný zájem musí být reálný (nesmí být spekulativní) a musí správci údajů svědčit na základě existence práva nebo svobody, pro jehož realizaci je zpracování údajů nezbytné.[657] Bod 47 odůvodnění Obecného nařízení ukazuje, že nová právní úprava přistupuje k otázce oprávněného zájmu správce otevřeněji, než úprava minulá, když připouští aplikaci tohoto právního titulu i pro účely přímého marketingu.[658] Kořeny této otevřenosti a relativně široké aplikovatelnosti právního titulu oprávněného zájmu můžeme sledovat ve francouzské a belgické tradici právní úpravy ochrany osobních údajů, které před příchodem směrnice 95/46/ES nepracovaly s konceptem souhlasu se zpracováním.[659]

Zájmy mohou svědčit buď přímo správci (v takovém případě může jít například o zájem na ochraně zdraví a majetku),[660] nebo mohou být prospěšné pro spo-

655 Viz § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

656 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. *Evropská komise* [online]. 9. 4. 2014, s. 33 a násl.

657 Velmi restriktivní přístup k oprávněnému zájmu argumentuje na základě analýzy rozhodovací praxe SDEU např. Federico Ferretti. Viz FERRETTI, Federico. Data Protections and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights. *Common Market Law Review*, 2014, roč. 51, č. 3, s. 868.

658 Bod 47 odůvodnění Obecného nařízení, poslední věta.

659 Viz GUTWIRTH, Serge. *Short statement about the role of consent in the European data protection directive* [online]. Brusel: Bepress. 2012 [cit. 30. 6. 2020].

660 Viz rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb. NSS.

lečnost jako celek.[661] Oprávněný zájem může být založený na konkrétním právu (např. právo na majetek) nebo svobodě (svoboda podnikat, svoboda projevu), může ale rovněž vyplývat například z nezávazných mimoprávních dokumentů a doporučení vydávaných orgány veřejné moci.[662] Klíčový aspekt při provádění testu proporcionality je skutečná situace v poměřovaném případě. Z toho důvodu například NSS dovodil, že použití kamery zabírající veřejný prostor a vchod do protějšího domu bylo v případě *Ryneš* adekvátní vzhledem k okolnostem, které aplikaci kamery předcházely (přímé ohrožení a poškození zdraví a majetku správce údajů a jeho předchozí snahy o méně invazivní řešení situace).[663] V případě rozhodnutí č. j. 2 As 140/2017-57 však NSS dal za pravdu ÚOOÚ, když shledal kameru mířící na zahradu souseda správce údajů za neproporcionální vzhledem k tomu, že nebyla prokázána předchozí nebezpečná činnost ze strany obyvatel sousedního domu.[664] V případě ve věci ekolo pak NSS rozhodl, že prodejci, kterému ukradli zboží, nesvědčí právní titul oprávněného zájmu k tomu, aby umístil záznam z kamery na internet ve snaze dopadnout zloděje, protože k tomu má využít služeb orgánů činných v trestním řízení.[665] Internalizovaný test proporcionality přítomný v právní úpravě tohoto právního titulu je tak opravdu nezbytné hodnotit ve vztahu ke všem klíčovým okolnostem konkrétní situace.

Jedním z faktorů hodnocených v testu proporcionality oprávněného zájmu je rizikovost zpracování osobních údajů, které má být tímto právním titulem založeno.[666] Čím je zpracování rizikovější pro práva a svobody subjektů údajů

661 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. *Evropská komise* [online]. 9. 4. 2014, s. 24; Tento argument rovněž použil SDEU jako *obiter dictum* v rozhodnutí ve věci *Google Spain* (rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12).

662 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. *Evropská komise* [online]. 9. 4. 2014, s. 36.

663 Viz bod 84 rozsudku Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb.NSS.

664 Viz bod 23 rozsudku Nejvyššího správního soudu ze dne 20. 9. 2017, č. j. 2 As 140/2017-57.

665 Viz s. 8–9 rozsudku Nejvyššího správního soudu ze dne 8. 6. 2016 č. j. 3 As 118/2015-34.

666 Tento závěr byl platný již v době účinnosti směrnice 95/46/ES (viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. *Evropská komise* [online]. 9. 4. 2014, s. 37–38). Tím spíše pak musí být platný v současné době, kdy hodnocení rizik zpracování je zásadním principem, na kterém je Obecné nařízení vystavěno.

(nebo třetích osob), tím spíše správce údajů tento právní titul využít nemůže. To však nutně musí platit i naopak, tedy čím méně rizikové zpracování je, tím spíše se na něj správce spolehnout může. Tento aspekt činí z právního titulu oprávněného zájmu velice flexibilní nástroj. Pokud správce údajů bude postupovat v maximální možné míře tak, aby při svém zpracování ochránil práva a svobody dotčených osob (např. řádně nastaví proces zpracování v souladu se zásadami záměrné a standardní ochrany osobních údajů, přísně dodrží zásadu minimalizace a omezeného uložení, dostatečně zapojí další organizační a technické prostředky ochrany), může napomoci tomu, aby hodnocení testu proporcionality vychýlil ve svůj prospěch. V právním titulu oprávněného zájmu proto můžeme vidět prostředek, který významně napomáhá vyvažování dvou základních cílů právní úpravy ochrany osobních údajů v podobě zájmů správců na zpracování osobních údajů na jedné straně a ochraně práv subjektů údajů (na dalších fyzických osob) na straně druhé.[667]

5.4.2 Vedení záznamů o zpracování

Povinnost vést záznamy o probíhajícím zpracování vyplývá z čl. 30 Obecného nařízení. Jejím účelem je za prvé motivovat správce údajů, aby se museli aktivně zamyslet nad probíhajícím zpracováním,[668] a za druhé (a to především) vytvoření dokumentace, která pak může být použita při naplnění zásady *accountability* ve smyslu zodpovídání se externímu subjektu v podobě dozorového úřadu.[669] Čl. 30 zakládá obecnou povinnost správce nebo zpracovatele vést záznamy obsahující všechny informace uvedené v odst. 1 nebo 2. Záznamy tak musí obsahovat informace identifikující správce údajů,

667 K vyvažování zájmů viz POUND, Roscoe. A Survey of Social Interests. *Harvard Law Review* [online]. 1943, roč. 57, č. 1; DIAS, R. W. M. The Value of a Value-Study of Law. *The Modern Law Review*, 1965, roč. 28, č. 4.

668 V tom můžeme spatřovat projevy *management-based* regulace (srovnej část 5.1 této publikace a COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review*. 2003, roč. 37, č. 4).

669 Srovnej bod 21 in PRACOVNÍ SKUPINA ZŘÍZENÉ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, s. 7 [cit. 30. 6. 2020]; Dále též viz v kontextu ochrany osobních údajů např. BUTIN, Denis, Marcos CHICOTE a Daniel Le MÉTAYER. Strong Accountability: Beyond Vague Promises. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 344.

účely zpracování, popis kategorií subjektů údajů, kategorie příjemců údajů (pokud jsou), informace o předávání údajů do třetích zemí, plánované lhůty pro výmaz (pokud je to možné) a obecný popis technických a organizačních bezpečnostních opatření dle čl. 32 (pokud je to možné). Aplikací přístupu založeného na riziku však správce údajů může tuto povinnost škálovat a tím ji přizpůsobit potřebám svého zpracování. Vždy bude třeba, aby informoval o všech uvedených oblastech, ale velikost rizika ovlivní například to, jak detailně je třeba nezbytné informace zpracovat. V případě menšího rizika bude dostačovat obecnější přehled, v případě většího rizika bude nezbytné, aby dokumenty byly zpracovány pečlivě. To bude platit zejména v případě kategorií uvedených v čl. 30 odst. 1 pod písmeny e), f) a g).[670]

Pátý odstavec zakládá výjimku z povinnosti vést záznamy. Střední a malé podniky s méně než 250 zaměstnanci (SME) nemusí tuto povinnost plnit, ledaže *„zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů"*.[671] Výjimka výslovně pracuje s konceptem hodnocení rizika. Pro přehlednost je možné textaci výjimky obrátit následovně: SME nemusí vést dokumentaci v případě příležitostného zpracování údajů, které nespadají do zvláštních kategorií údajů podle čl. 9 Obecného nařízení, pokud takové zpracování nepředstavuje pravděpodobné riziko pro subjekty údajů. Přístup založený na riziku zakládá granularitu této povinnosti. Aplikace této výjimky bude častější, než by se na první pohled mohlo zdát, protože dle statistik Eurostatu tvoří SME 99,8 % podniků v rámci EU.[672] Z ustanovení bohužel není na první pohled zcela jasné, jak vysoké riziko může být, aby bylo možné výjimku aplikovat.[673] Domnívám se však, že toto ustanovení není možné vykládat tak, že by pro aplikaci výjimky požadovalo nulové riziko. Vzhledem k tomu, že riziko nikdy není možné zcela vyloučit, byl by požadavek

670 Jde o informace o předání osobních údajů do třetích zemí, plánované lhůty pro výmaz jednotlivých kategorií údajů a popis technických a organizačních bezpečnostních opatření.

671 Čl. 30 odst. 5 Obecného nařízení.

672 Viz EUROSTAT. Statistics on small and medium-sized enterprises. *Europa.eu* [online]. [cit. 30. 6. 2020]; V České republice dosahuje poměr stejné hodnoty (viz Ibid.).

673 Český komentář k Obecnému nařízení se této otázce také nevěnuje. Viz NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Dostupné z: ASPI [Právní informační systém].

na nulové riziko absurdním, protože by výjimku nebylo nikdy možné aplikovat. Domnívám se proto, že výjimky z vedení záznamů mohou SME využít i tehdy, když bude zpracování představovat nízké až střední riziko.[674]

Proti tomuto závěru je možné argumentovat tím, že záznamy o zpracování jsou hlavním prostředkem naplnění základní zásady *accountability* ve smyslu čl. 5 odst. 2, který stanoví povinnost doložit dozorovému úřadu splnění povinností vyplývajících z ostatních zásad. Mám však za to, že tento argument je možné odmítnout s poukázáním na to, že dané ustanovení neuvádí, jakým způsobem má správce své plnění doložit. V případě zpracování osobních údajů, které jsou povahou málo rizikové, je možné očekávat, že půjde o nenáročné procesy, které správce snadno doloží pouhým popisem nebo vysvětlením. Formalistické lpění na vytváření dokumentace i v případech, kdy to není nutné, by naopak mohlo vést k bezmyšlenkovitému vytváření nových a nových dokumentů, které by však neplnily žádnou reálnou funkci. Praxi vytváření dokumentů pro dokumenty je třeba jednoznačně odmítnout.

Na čl. 30 Obecného nařízení je možné dobře ukázat, jak se vyhodnocení rizika projeví jak v granularitě povinnosti (výjimka se aplikuje nebo ne), tak v její škálovatelnosti (jak precizně je nezbytné povinnost plnit).

5.4.3 Povinnosti vyplývající z vyššího rizika

Obecné nařízení obsahuje řadu povinností, které se aktivují až v případě, že zpracování osobních údajů představuje vysoké riziko pro práva a zájmy.[675] Jde tedy o projev granularity povinností ve vztahu k rizikovosti zpracování osobních údajů.[676] Správce údajů má povinnost sám si vyhodnotit, zda už jeho zpracování dosahuje takové intenzity, aby bylo nezbytné naplňovat tyto povinnosti. Je třeba dodat, že i v případě těchto povinností je možné v konkrétních případech uvažovat o škálovatelnosti, tedy přizpůsobení

674 Shodně též viz HARTUNG, Jürgen. Art. 30. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 642.

675 V přítomnosti těchto povinností, které jsou vedené principem regulace postavené na riziku, pak můžeme spatřovat přístup evropského zákonodárce k regulaci rizik (jeho cílem bylo vytvoření mechanismů, které sníží společenské riziko spočívající v nekorektním a protiprávním zpracování osobních údajů).

676 Srovnej MACENAITE, Milda. The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3, s. 525.

konkrétního způsobu splnění povinnosti tak, aby odpovídala povaze a rizikovosti zpracování.

Prvním příkladem je povinnost hlásit případy, kdy dojde k porušení zabezpečení osobních údajů, kterou Obecné nařízení zakládá v čl. 33 (hlášení dozorovému úřadu) a 34 (hlášení subjektům údajů). V této povinnosti, která je inspirována obdobnou povinností z oblasti kybernetické bezpečnosti,[677] můžeme spatřovat projev požadavku na transparentnost zpracování a důležitou součást zásady *accountability*, tedy zodpovídání se vnější autoritě. Obě ustanovení obsahují poměrně podrobný popis, jak má být povinnost naplněna a není v nich proto příliš prostoru pro škálovatelnost. Hodnocení rizika konkrétního zpracování se u povinnosti informovat o případech porušení zabezpečení osobních údajů projevuje v granularitě. Pokud je riziko nízké (zásah do práv subjektů je málo pravděpodobný), může správce údajů využít výjimky uvedené v odst. 1 čl. 33 a incident vůbec nehlásit. Naopak, pokud je riziko pro práva a svobody fyzických osob v důsledku incidentu vysoké, má správce povinnost ohlásit jeho výskyt přímo subjektům údajů.

Druhým příkladem povinnosti, kterou správce musí splnit až v případě vysoké rizikovosti chystaného zpracování, je vypracování plného posouzení vlivu na ochranu osobních údajů (dále *DPIA* z anglického *„Data Protection Impact Assessment"*). Článek 35 Obecného nařízení uvádí, že *DPIA* je třeba provádět v případech, kdy je pravděpodobné, že plánované zpracování osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.[678] Každý správce má povinnost hodnotit rizikovost svého chystaného zpracování, ale pouze v případě že v tomto prvním kroku pojme podezření, že by zpracování mohlo představovat vysoká rizika pro subjekty údajů a další

677 Povinnost hlásit kybernetické bezpečností incidenty (tzv. *data breaches*) v kontextu českého práva vyplývá z § 8 zákona č. 131/2014 Sb., o kybernetické bezpečnosti; K problematice hlášení případů porušení zabezpečení více viz např. MARCUS, Daniel J. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke Law Journal,* 2018, roč. 68, č. 3; MITRAKAS, Andreas. Assessing liability arising from information security breaches in data privacy. *International Data Privacy Law* [online]. 2011, roč. 1, č. 2; ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies* [online]. 2014, roč. 11, č. 1; SCHATZ, Daniel a Rabih BASHROUSH. The impact of repeated data breach events on organisations' market value. *Information & Computer Security* [online]. 2016, roč. 24, č. 1.

678 Viz čl. 35 odst. 1 Obecného nařízení.

osoby, má rovněž povinnost vytvořit plnou *DPIA*. Ta má správci pomoci umožnit vhodné nastavení jednotlivých dílčích procesů probíhajícího zpracování tak, aby bylo riziko, pokud možno, co nejvíce minimalizováno.[679] WP 29 ve svých pokynech věnovaných otázce posouzení vlivu na ochranu údajů stanovila devět kategorií, které naznačují, že zpracování může představovat vysoké riziko pro práva a svobody fyzických osob.[680] Doporučení uvádí, že plnou *DPIA* by správce údajů měl vykonat tehdy, když chystané zpracování bude spadat alespoň do dvou z nich.[681] Vypracování plné *DPIA* je tak čistě preventivní povinnost, která se uplatní, je-li pravděpodobné, že budoucí zpracování bude spadat do kategorie zpracování s vysokým rizikem. Pokud se v průběhu vypracování *DPIA* podezření potvrdí a správce vyhodnotí, že chystané zpracování mezi vysoko riziková opravdu spadá, má na základě čl. 36 provést konzultaci ohledně chystaného zpracování s dozorovým úřadem. V uvedené povinnosti můžeme spatřit jednak na hodnocení rizik postavenou granularitu povinností správce a zároveň projev *accountability* jako povinnosti obsahující silný prvek nezbytné komunikace s externími subjekty, které mají pravomoc na regulovaný subjekt dohlížet.

Posledním příkladem povinnosti, která se aplikuje až v případě vysokého rizika zpracování, je ustanovení pověřence pro ochranu osobních údajů (dále *DPO* z anglického *„Data Protection Officer"*), kterou zakládá čl. 37 Obecného nařízení.[682] DPO představuje spojovací prvek mezi správcem

679 K roli DPIA více viz YORDANOV, Atanas. Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review*, 2017, roč. 3, č. 4; WRIGHT, David. The state of the art in privacy impact assessment. *Computer Law & Security Review* [online]. 2012, roč. 28, č. 1; Detailně se otázce vlivu hodnocení dopadů zpracování osobních údajů věnuje rovněž monografie WRIGHT, David a Paul de HERT (eds.). *Privacy impact assessment*. Dordrecht; New York: Springer, 2012, Law, governance and technology series, volume 6.

680 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679. *Evropská komise* [online]. 4. 4. 2017, v revidovaném znění ze dne 4. 10. 2017, č. WP248rev.01, s. 10–12.

681 Ibid., s. 12; Kriticky citované pokyny zhodnotil Raphaël Gellert, když uvádí, že je škoda, že se WP 29 více nezaměřila na organizační a metodické otázky zpracování osobních údajů. Viz GELLERT, Raphaël. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. *European Data Protection Law Review*, 2017, roč. 3, č. 2.

682 K povaze činnosti DPO viz čl. 38 a 39 Obecného nařízení. Detailně pak viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny týkající se pověřenců pro ochranu osobních údajů. *Evropská komise* [online]. 13. 12. 2016, v revidovaném znění ze dne 5. 4. 2017, č. WP243rev.01, 29 s.

údajů a dozorovým úřadem a v tomto směru je jeho rolí podpořit plnění informační součásti zásady *accountability*.[683] Formulace podmínek, za jakých má správce údajů povinnost jmenovat DPO, se liší od předchozích jmenovaných granulárních povinností, které se aktivovaly až s vysokým rizikem. Čl. 37 ve svém odst. 1 totiž jednoznačně vyjmenovává podmínky, při jejichž splnění musí správce údajů DPO jmenovat bez ohledu na vyhodnocení rizikovosti konkrétního zpracování. Z povahy těchto podmínek je však znatelné, že se týkají zpracování s vysokým rizikem neblahého dopadu na práva a svobody fyzických osob.[684] Jejich rizikovost jednoznačně vyhodnotil již zákonodárce a pokusil se je normativně limitovat zavedením povinnosti jmenovat DPO. Čl. 37 odst. 1 je tedy projevem regulace rizik a nikoli regulace postavené na riziku. Domnívám se však, že v případech, kdy správce údajů vyhodnotí své zpracování jako vysoce rizikové, má bezpochyby možnost jmenovat DPO i pokud do kategorií uvedených v odst. 1 nespadá, pokud jmenování DPO dokáže rizikovost zpracování snížit. Stejně tak je možné si představit situaci vysoce rizikového zpracování osobních údajů, které sice nespadá do kategorií uvedených v odst. 1, ale u kterého by nejmenování DPO mohlo vyvolat správní sankci. Správce údajů má obecnou povinnost přizpůsobit své zpracování požadavkům konkrétní situace. Má povinnost zavést vhodné technické a organizační prostředky, které rizikovost zpracování sníží.[685] Jmenování DPO je pak bezpochyby organizačním prostředkem.

V kontextu vysoko rizikového zpracování osobních údajů je vhodné, aby správci údajů postupovali ve snaze o co nejpreciznější naplnění povinností vyplývajících z Obecného nařízení. Vysoké riziko zpracování tak není jen základem pro aktivaci působnosti nových povinností (aspekt granularity),

683 Shodně viz RECIO, Miguel. Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability Reports: Practitioner's Corner. *European Data Protection Law Review (EDPL),* 2017, roč. 3, č. 1; Náklady související se zavedením DPO v kontextu českých územních samospráv prozkoumali CVIK, Daniela Eva, Radka MacGREGOR PELIKÁNOVÁ a Michal MALÝ. Selected Issues from the Dark Side of the General Data Protection Regulation. *Review of Economic Perspectives* [online]. 2018, roč. 18, č. 4.

684 Jde o následující podmínky: i) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí; ii) hlavní činností správce je zpracování údajů, které vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů; iii) hlavní činností správce je zpracování zvláštních kategorií osobních údajů. Viz čl. 37 odst. 1 Obecného nařízení.

685 Viz např. čl. 25 a 32 Obecného nařízení a na ně navázaný čl. 83 odst. 4 Obecného nařízení.

ale rovněž musí způsobit i zvýšení standardu a nákladů, které správce údajů do plnění investuje (aspekt škálovatelnosti povinností). V případě vysoce rizikových zpracování je tak vysoký standard plnění dílčích povinností správce nezbytný k naplnění požadavků Obecného nařízení jako celku.

5.4.4 Práva subjektů údajů

Subjektivní pozitivní práva subjektů údajů formulovaná v kapitole 3 Obecného nařízení tvoří hranici, na kterou přístup založený na riziku zřejmě nedopadá.[686] Jsou formulována zcela jednoznačně, není možné je právním jednáním mezi subjektem údajů a správcem omezit ani se jich vzdát.[687] Správci údajů proto musí plnit jim odpovídající povinnosti. Určitě tedy není možné zcela vyloučit aplikaci některého z práv subjektů údajů na základě nízkého rizika zpracování (odpovídající povinnosti nejsou v tomto smyslu granulární).

Obecné nařízení z povinností odpovídajícím právům subjektů údajů nabízí několik výjimek, které je však nutné vzhledem k ustálené rozhodovací praxi SDEU[688] interpretovat spíše restriktivně. Předně čl. 11 umožňuje správcům údajů, kteří zpracovávají pseudonymní osobní údaje, že v případech, kdy správce není schopen sám přímo identifikovat subjekt údajů a okolnosti daného zpracování to nevyžadují, nemusí za účelem splnění svých povinností shánět dodatečné informace o subjektech údajů.[689] Obecnou výjimku z povinností souvisejících s právy subjektů nabízí odst. 5 čl. 12, který uvádí, že v případech, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, může správce buď splnění žádosti podmínit přiměřeným poplatkem, nebo může žádost odmítnout. Tato výjimka slouží jako ochrana správce údajů, aby nedocházelo ke zneužívání práva subjekty. Konkrétní práva subjektů údajů pak mají zanesené specifické výjimky, které mají omezit případnou nepřiměřenost nebo zbytečnost jejich aplikace. Takovým

686 Shodně též PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement on the role of a risk-based approach in data protection legal frameworks, *Evropská komise* [online]. 30. 5. 2014, č. 14/EN, WP 218, s. 3.

687 K argumentaci těchto závěrů viz část 2.3 této publikace.

688 Viz kapitola 4 této publikace.

689 Autorský tým pod vedením Michala Nulíčka uvádí jako příklad užití tohoto ustanovení případ logování IP adres zákazníků internetového obchodu. Viz NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Dostupné z: ASPI [Právní informační systém].

příkladem mohou být čl. 13 odst. 4, který umožňuje neposkytnout informace o zpracování, pokud už je subjekt údajů má, nebo čl. 14 odst. 5, který zakládá výjimku z informační povinnosti dle čl. 14, pokud by se ukázalo, že *„poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí"*.[690] Žádná z uvedených možností však neobsahuje výslovný odkaz na rizikovost zpracování osobních údajů.[691] Je tedy otázkou, zda je možné tyto povinnosti dle rizikovosti zpracování škálovat. Domnívám se, že obecně spíše ne, a to ze dvou důvodů. Za prvé, pozitivní subjektivní práva subjektů údajů hrají v systému ochrany osobních údajů zásadní roli kontroly správce a možnosti projevu autonomie vůle subjektů. Za druhé, všechny povinnosti odpovídající těmto právům vyžadují konkrétní výsledek, jako je například poskytnutí konkrétních informací, oprava informací chybných, nebo výmaz informací, které již správce nemá právo zpracovávat.[692] Povaha plnění této povinnosti výrazně limituje možnost její škálovatelnosti.

Claudia Quelle proto upozorňuje na to, že konkrétní práva subjektu údajů se mohou ocitnout v kolizi s jinými povinnostmi správce, které byly modifikovány (škálovány) na základě nízké intenzity rizika zpracování.[693] Příkladem takové situace je právo na přístup k osobním údajům podle čl. 15 Obecného nařízení, které zakládá správci povinnost poskytnout potvrzení, zda zpracovává údaje o subjektu údajů a pokud ano, tak ho povinuje připojit i celou řadu dalších informací.[694] Předpokladem pro úspěšné splnění této povinnosti je však pečlivé vedení záznamů o zpracování. V případě zpracování, která nepředstavují vysoké riziko, však správci spadající do kategorie SME často záznamy mít nemusí na základě výjimky stanovené v čl. 30 odst. 5. To však může způsobit faktickou nemožnost splnění povinnosti odpovídající právu

690 Viz čl. 14 odst. 5 písm. b) Obecného nařízení.

691 Na druhou stranu je možné vidět v zavedení těchto výjimek úvahu týkající se regulace rizika na straně zákonodárce. Kupříkladu výjimka uvedená v čl. 11 se nutně bude aplikovat jen na případy, ve kterých zpracování představuje minimální riziko pro práva a zájmy dotčených osob.

692 Viz čl. 17 Obecného nařízení. Zde je třeba upřesnit, že konkrétně v případě práva na výmaz se aspekt hodnocení rizika projeví například ve fázi vyhodnocení, zda správci údajů svědčí oprávněný zájem, či nikoli (k argumentaci vztahu míry rizika a oprávněného zájmu viz výše).

693 Viz QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 516.

694 Srovnej čl. 15 Obecného nařízení.

subjektu údajů na přístup. Na druhou stranu, pokud bychom z povinnosti poskytnout informace neumožnili adekvátní výjimku a trvali na nezbytnosti vedení záznamů o zpracování jen za účelem možnosti splnění této povinnosti ve všech případech, bylo by ustanovení čl. 30 odst. 5 zbytečné. To je závěr, který je vzhledem k předpokladu racionálního zákonodárce nutné odmítnout.

Možnou cestu ven z tohoto střetu nabízí výše zmíněná výjimka zakotvená v odst. 5 čl. 12 Obecného nařízení, konkrétně možnost správce odmítnout žádost subjektu údajů, je-li zjevně nedůvodná nebo nepřiměřená. Možnosti odmítnout uplatnění práv subjektu údajů se ve své studii věnovali Monika Matysová s Františkem Nonnemannem a vhodně poukázali na to, že otázku přiměřenosti plnění je třeba chápat jako poměr mezi zájmem subjektu údajů a zájmy správce, přičemž jako v každém případě poměřování protichůdných práv a zájmů je nezbytné hodnotit dopady s ohledem na konkrétní žádost.[695] Nepřiměřenost je pak možné chápat rovněž v kontextu nezbytných vynaložených nákladů na splnění povinnosti, nebo přímo v kontextu nemožnosti technické realizace žádosti.[696] Tento závěr odpovídá rovněž účelům právní úpravy ochrany osobních údajů, tedy zajištění korektního zpracování osobních údajů, které zachová vysokou úroveň ochrany subjektů a nebude nepřiměřeně zatěžovat správce. Prostřednictvím hodnocení přiměřenosti žádosti subjektu údajů se do procesu výkonu jeho práv dostává zpět (byť velmi nepřímo) přístup založený na riziku. Mám ale za to, že by mělo jít spíše o výjimečné a odůvodněné případy. To odpovídá i textaci výjimky v čl. 12 odst. 5, dle které je možné odmítnout žádost pouze tehdy, je-li zjevně nepřiměřená. I s touto možností tak stále obecně platí, že práva subjektu údajů tvoří hranici možné aplikace přístupu založeného na riziku a je nezbytné, aby jejich aplikace byla zachována.

5.5 Temporální aspekty

Aspekt času je důležitým faktorem při zpracování osobních údajů. Fixace hodnocení zpracování osobních údajů k jednomu časovému bodu,

695 Srovnej MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12, s. 425–426.

696 Typickým příkladem nemožnosti technické realizace je žádost o výmaz osobních údajů zaznamenaných v rámci technologie blockchain.

nereflektuje dostatečně přesně pravou podstatu zpracování osobních údajů[697] a může vést v konečném důsledku ke snížení úrovně ochrany subjektů údajů. Zásadně problematické může být statické chápání zpracování osobních údajů s akcentem na souhlas,[698] které vede k pochopení osobních údajů jako quasi věcného práva, kterého je možné se vzdát.[699] Právní ochrana osobních údajů však působí v průběhu celého životního cyklu jejich zpracování a v tomto kontextu je třeba k ní přistupovat. Tato podkapitola se zabývá otázkou, jak se performativní regulace využívající zásady *accountability* správce a přístupu postaveného na riziku projeví v kontextu plynoucího času. Působení času na osobní údaje můžeme v základu rozdělit na dvě roviny. První rovina, které se věnuje první část této podkapitoly, spočívá v působení času na systém ochrany osobních údajů ve smyslu jeho zastarávání v konfrontaci s technologickými novinkami a dříve netušenými možnostmi zpracování osobních údajů. Druhá rovina pak spočívá v působení času na osobní údaje a jejich zpracování správci údajů. Druhá část této podkapitoly je proto věnována změně významu osobních údajů v průběhu času a dotýká se problematiky zapomínání. Tato témata byla vybrána, protože dle mého názoru vhodně demonstrují základní způsoby působení času na systém ochrany osobních údajů.

5.5.1 Odolnost právní úpravy osobních údajů vůči technologickým změnám

Když došlo na podzim 2010 ke zveřejnění třetího hodnocení směrnice 95/46/ES, bylo hlavní výtkou směřovanou na fungování právní úpravy ochrany osobních údajů její zaostávání za technologickým vývojem.[700] Nedostatky pak spočívaly zejména v neschopnosti bývalé právní úpravy adekvátně reagovat na nové způsoby zpracování osobních údajů, jako například technologie velkých dat, zpracování v cloudových uložištích a další způsoby

697 Srovnej POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014, s. 2 [cit. 30. 6. 2020].

698 Více viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9.

699 Jak bylo argumentováno v části 2.3 této publikace, tento závěr není možný.

700 EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Komplexní přístup k ochraně osobních údajů v Evropské unii, č. KOM(2010) 609. In: *EurLex* [online]. 19 s. [cit. 30. 6. 2020].

zpracování přinášející vyšší rizika.[701] Jak ukázala kapitola 3 této publikace, stejný závěr je možné učinit i v případě zpracování v kontextu technologií, které představují rizika nižší. Neschopnost adekvátně obsáhnout technologický pokrok se paradoxně v případě směrnice 95/46/ES objevila i přesto, že její definiční ustanovení jsou technologicky neutrální.[702] Jak ale správně upozorňuje Lyria Bennet Moses, cílem zákonodárce by neměla být pouze technologicky neutrální právní úprava, ale systém, který zachází korektně a efektivně s různými druhy technologií a dokáže adekvátně reagovat na jejich vývoj.[703] Zásadní obtíž bývalé právní úpravy ochrany osobních údajů spočívala v její obecnosti, tedy že dopadala široce na všechna zpracování (včetně těch co se nově objevily), ale zároveň nebyla dostatečně vnitřně flexibilní vlivem nízkých možností škálovatelnosti a granularity povinností.

Druhý problém, který identifikovala mimo jiné WP 29 ve svém stanovisku *The Future of Privacy*, spočíval v nedostatečném dodržování povinností správců údajů a projevoval se o to silněji v kontextu zpracování osobních údajů za použití nových technologií.[704] WP 29 jako možné řešení navrhla zavedení silnější zásady *accountability* správce údajů.[705]

---

701 Viz HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 147; KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*. 2012, s. 14; HERT, Paul de. The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents Editorial. *Utrecht Journal of International and European Law*, 2015, roč. 31, č. 80, s. 1.

702 Výslovně byla na principu technologické neutrality později vystavěna směrnice 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). Viz HILDEBRANDT, Mireille a Laura TIELEMANS. Data protection by design and technology neutral law. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5; KOSTA, Eleni. *Consent in European data protection law*. Leiden: Martinus Nijhoff Publishers, 2013, s. 264 a násl.

703 BENNETT MOSES, Lyria. Recurring Dilemmas: The Law's Race to Keep up with Technological Change. *University of Illinois Journal of Law, Technology & Policy,* 2007, roč. 2007, č. 2, s. 239; Více k technologicky neutrálnímu zákonodárství viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti*. Disertační práce Brno: Masarykova univerzita, Právnická fakulta, 2018, s. 30 a násl.

704 PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, s. 20 [cit. 30. 6. 2020].

705 Ibid.

Principy performativní regulace přítomné v Obecném nařízení pomáhají ve spojení s technologicky neutrálními definicemi klíčových pojmů výše uvedené problémy řešit. Oproti směrnici 95/46/ES totiž na obecné úrovni platí, že se technologicky neutrální přístup v Obecném nařízení neprojevuje jen staticky ve formě technologií nezatížených definic, ale rovněž v průběhu zpracování. Zásada *accountability* správce, tak jak je v Obecném nařízení přítomná, nikterak neupravuje, jak (jakou technologií) má správce údajů dosáhnout dostatečného snížení rizikovosti zpracování, které provádí. To samé pak platí například pro principy záměrné ochrany osobních údajů dle čl. 25.[706] Pro performativní regulaci je navíc typické, že díky své flexibilitě a otevřenosti podporuje (nebo alespoň nebrzdí) technologický pokrok.[707]

Kombinace performativní regulace s technologicky neutrálními definicemi vytvářejí právní úpravu Obecného nařízení dostatečně flexibilní, aby dokázala adekvátně reagovat na nové technologické výzvy. Analogicky je zde možné vidět souvislost s konceptem Norberta Wienera spočívajícím v pravdivých informací, které organizují systém a jsou předpokladem jeho dlouhodobé existence.[708] Pokud není systém regulace dostatečně flexibilní, nedovolí vznik nových pravdivých informací, který by umožnil jeho pokračující (smysluplnou) existenci. Dostatečná míra flexibility systému je tak nezbytným předpokladem pro dlouhodobou existenci regulatorního rámce tváří v tvář technologickému vývoji. Performativní regulace využívající zásady *accountability* správce a přístupu postaveného na riziku v systému ochrany osobních údajů tuto flexibilitu umožňuje. V tomto ohledu je proto nová úprava ve střetu s novými technologiemi vhodnější a má dle mého názoru šanci na delší trvání, než úprava minulá v podobě směrnice 95/46/ES.

706 Více k principu záměrné ochrany osobních údajů viz např. JASMONTAITE, Lina et al. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. *European Data Protection Law Review (EDPL),* 2018, roč. 4, č. 2.

707 Srovnej COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 711.

708 Informační teorie Norberta Wienera spočívá v předpokladu, že všechny organizované systémy se postupně rozpadají do entropie a jediné, co tento proces dokáže zvrátit jsou pravdivé informace, které rozpadající se systém naopak zpět organizují. Schopnost vytvářet pravdivé informace je pak to, co liší živé a neživé organizované systémy. Viz WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích*. Praha: Státní nakladatelství technické literatury, 1960, Teoretická knižnice inženýra; V kontextu práva viz POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 18–41, Téma.

5.5.2 Změna hodnoty osobních údajů v čase a zapomínání

Zpracování osobních údajů je proces probíhající v čase. Je obecně limitováno tak, že správce osobních údajů má povinnost dodržovat zásadu omezení uložení. Ta stanoví, že osobní údaje smí být uchovávány jen po dobu nezbytně nutnou vzhledem k účelu daného zpracování.[709] Za touto zásadou je možné vidět koncept „regulace rizika", neboť nejméně rizikové z hlediska možného nežádoucího zásahu do práv subjektu údajů jsou samozřejmě ty osobní údaje, které byly vymazány.

V případě, že je účel zpracování dlouhodobý, mohou být osobní údaje zpracovávány po celé roky. To platí tím spíš, pokud se jedná o zpracování za účelem archivace, statistiky, nebo vědeckého a historického výzkumu. Dlouhodobé zpracování je pak běžné a (obvykle) přiměřené rovněž v případech zveřejnění osobních údajů v kontextu výkonu práva na svobodu projevu a novinářské profese.[710] Stav, hodnota a význam osobních údajů se v průběhu času může měnit. První zřejmou možností je jejich zastarávání a pozbývání přesnosti. V takovém případě má správce osobních údajů povinnost tyto údaje udržovat aktuální, aby zpracovával přesné osobní údaje v souladu se zásadou přesnosti.[711] Míra nezbytné investice do aktualizace dat se bude odvíjet od účelu zpracování, a hlavně rovněž od jeho rizikovosti pro práva a svobody subjektů údajů a dalších fyzických osob. I v tomto případě se tedy uplatní zásada *accountability* a hodnocení rizika. Pokud se bude jednat o málo rizikové zpracování, nemusí správce údajů vynakládat tolik snahy a investovat do průběžné kontroly svých dat.[712] Pokud naopak bude zpracování velmi rizikové (např. protože bude na jeho základě docházet k automatizovanému rozhodování), bude mít správce povinnost vytvořit takový systém kontrol a ověření, aby udržoval svoji databázi aktuální vždy.

Zastarávání a změna hodnoty osobních údajů však probíhá i tehdy, když jsou údaje přesné a aktuální. Dynamiku změn hodnoty zpracovávaných

709 Viz čl. 5 odst. 1 písm. e) Obecného nařízení.

710 Srovnej rozsudek Evropského soudního dvora ze dne 16. 12. 2008 ve věci *Satakunnan Markkinapörssi a Satamedia*, C-73/07.

711 Čl. 5 odst. 1 písm. d) Obecného nařízení.

712 V případě žádosti subjektu údajů o opravu však musí být schopen vyhovět, ledaže by taková žádost byla zjevně nepřiměřená. Srovnej MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12.

údajů dobře ukázali ve svých studiích Giovanni Sartor[713] a autorský kolektiv pod vedením Paulan Korenhof,[714] a demonstrují ji na příkladu konfliktu práva na ochranu osobních údajů (nebo soukromí) a práva na informace. Při hodnocení testu proporcionality je třeba vůči sobě poměřovat proti sobě stojící zájmy. Na uvedeném příkladě tak může jít o zájem společnosti být informován a zajištění práva na svobodu projevu na jedné straně a ochrana osobnosti a osobních údajů na straně druhé.[715] Zájem veřejnosti (a k němu odpovídající právo) se bude lišit například dle toho, zda se informace týkají veřejně činné osoby, či nikoli. Tento status se však v průběhu zpracování osobních údajů může změnit (dříve činná osoba odejde do ústraní,[716] nebo naopak dříve neznámá osoba začne veřejně působit) a dle toho se dynamicky průběžně vyvíjí rovněž výsledek testu proporcionality. Změna hodnoty osobních údajů může nastat i bez změny statusu dotčené osoby, a to pouhým plynutím času. Čím je informace starší, tím méně se na ni bude vztahovat právo veřejnosti na jejím zveřejnění.[717]

Stejně, jako se v čase mění hodnota zpracovávaných osobních údajů, mění se i míra rizika, kterou zpracování takových údajů představuje. Jediná možnost, jak riziko zcela vyloučit, je vymazání takových údajů v případě, že již nejsou nezbytné pro účel zpracování. Zejména pro zpracování osobních údajů jejich publikací online platí, že určitá míra rizika bude vždy přítomná. Riziko negativního zásahu do práv subjektů údajů v případě starých informací, které jsou nějakým způsobem vzhledem k subjektům údajů citlivé,

713 Viz SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology* [online]. 2016, roč. 24, č. 1.

714 Viz KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European data protection law*. Dordrecht: Springer, 2015, s. 171–201. Giovanni Sartor je rovněž členem tohoto autorského kolektivu, užité příklady tedy nepřekvapivě vychází ze stejného základu.

715 Typický příklad provedení tohoto specifického testu proporcionality viz rozsudek Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci *Von Hannover vs. Německo (No. 2)*, stížnosti č. 40660/08 a 60641/08; a rozsudek Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci *Axel Springer vs. Německo*.

716 Byť jak například uvádí Meg Leta Jones, v kontextu angloamerického práva odchod do ústraní nic neznamená, a soudy většinově nadále přiznávají právní zájem veřejnosti na informace týkající se osob, které již dávno nejsou z hlediska veřejného života činné. Srovnej JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016, s. 55–80.

717 Srovnej SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology* [online]. 2016, roč. 24, č. 1, s. 81.

může být vysoké z hlediska intenzity hrozícího zásahu, nicméně velmi málo pravděpodobné z hlediska jeho realizace. Správce osobních údajů však může vzhledem k technické realitě jen velmi obtížně hlídat měnící se a narůstající riziko u každého jednoho osobního údaje, který zpracovává. Právní úprava ovšem musí umožnit obranu těm subjektům údajů, kteří si ji budou přát vyvolat a uplatnit tak své právo na informační sebeurčení.[718] Obecné nařízení za tímto účelem obsahuje právo subjektu údajů na výmaz („právo být zapomenut"),[719] které (ve zkratce) umožňuje subjektu údajů žádat správce o smazání údajů, které správce (již) nemá oprávnění zpracovávat.

Právo být zapomenut je *buzz word*, který se dostal do povědomí široké odborné i laické veřejnosti v souvislosti s rozhodnutím SDEU ve věci *Google Spain*.[720] Tématu se již detailně věnovala řada autorů, ať již v kontextu přímo uvedeného rozhodnutí,[721] nebo na obecnější úrovni možnosti a oprávněnosti existence práva na výmaz údajů.[722] Právo být zapomenut má výrazně

718 Viz shodně DE TERWANGE, Cécile. The Right to be Forgotten and Informational Autonomy in the Digital Environment. In: GHEZZI, Alessia, Ângela Guimarães PEREIRA a Lucia VESNIĆ-ALUJEVIĆ (eds.). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. Houndmills: Palgrave Macmillan UK, 2014, s. 77–78.

719 Viz čl. 17 Obecného nařízení.

720 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

721 Např. viz AMBROSE, Meg Leta. Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. *Telecommunications Policy* [online]. 2014, roč. 38, č. 8–9; Special issue on Moving Forward with Future Technologies: Opening a Platform for AllSpecial issue on Papers from the 41st Research Conference on Communication, Information and Internet Policy (TPRC 2013); LINDSAY, David. The "Right to be Forgotten" by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling. *Journal of Media Law* [online]. 2014, roč. 6, č. 2; POST, Robert C. Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere. *Duke Law Journal,* 2017, roč. 67, č. 5; VOSS, W. Gregory. After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy in at Time of Change. *Business Lawyer,* 2015, roč. 71, č. 1.

722 Zde je třeba předně upozornit na výbornou disertační práci z pera Jefa Ausloose (AUSLOOS, Jef. *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?* Disertační práce. Leuven: KU Leuven, Faculty of Law, 2018); Dále viz např. HERMSTRÜWER, Yoan a Stephan DICKERT. Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten. *SSRN Scholarly Paper* [online]. ID 2311201. Rochester, NY: Social Science Research Network. 2013 [cit. 30. 6. 2020]; JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016; KRITIKOS, Katie Chamberlain. The Right to Forget, Obliterate, Erase: Defending Personal Data Privacy in the Digital Age. *Journal of Information Ethics,* 2018, roč. 27, č. 2; STENNING, Ashley. Gone But Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impacts of Data Breaches. *San Diego International Law Journal,* 2016, roč. 18, č. 1.

širší dopad než jen na zpracování osobních údajů internetovými vyhledávači. Internet působí jako společná kolektivní paměť naší společnosti.[723] Jinými slovy, jak se populárně uvádí: „internet nezapomíná". Nemyslím tím jen jednoduchou poučku, že co člověk jednou umístí online, to už zřejmě neodstraní, protože pokud se o to pokusí, vystavuje se riziku působení Streisand efektu,[724] a nekonečného množství dalších kopií. Významnějším důsledkem této skutečnosti je, že všechen obsah je přístupný v přítomnosti bez ohledu na to, jak je starý a v jaké době a kontextu vznikl. Tato skutečnost může představovat zásadní riziko zásahu do osobnostních práv subjektů údajů, protože může dojít k šíření informací zcela mimo jejich původní kontext, případně takových informací, které by bez digitálního záznamu již byly dávno zapomenuty. Meg Leta Jones tuto situaci velmi trefně vystihuje jako kopernikánský obrat, zásadní paradigmatický rozdíl oproti době před masově rozšířeným užíváním internetu, protože zatímco dříve bylo základní možností zapomínání, dnes je to naopak uchování informací.[725] Zapomínání je přitom důležitou součástí fungování lidské společnosti, jak dokazuje například fakt, že na principu zapomínání působí rovněž některé právní instituty, jako například zahlazení v trestním právu.[726] Zapomínání umožňuje odpouštění, které by bez něj bylo nesmírně obtížným procesem.[727] Zde pak spočívá hlavní argument pro právo na výmaz, resp. právo být zapomenut. Dokud nejsme jako společnost většinově schopni odpouštět bez zapomnění, je právo na výmaz umožňující faktickou (byť omezenou a nesmírně komplikovanou) realizaci práva na informační sebeurčení zcela klíčové.

Souhlasím s Radimem Polčákem, když argumentuje jako hlavní nedostatek práva na výmaz jeho praktické odmítání reality povahy šíření informací

723 PEREIRAA, Ângela Guimarães, Lucia VESNIĆ-ALUJEVIĆA a Alessia GHEZZIA. The Ethics of Forgetting and Remembering in the Digital World through the Eye of the Media. In: GHEZZI, Alessia, Ângela Guimarães PEREIRA a Lucia VESNIĆ-ALUJEVIĆ (eds.). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. Houndmills: Palgrave Macmillan UK, 2014, s. 9–27.

724 Srovnej např. JANSEN, Sue Curry a Brian MARTIN. The Streisand effect and censorship backfire. *International journal of communication (Online)*. 2015, roč. 9, č. 9.

725 JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016, s. 11.

726 Srovnej MÍŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie*, Česká advokátní komora, 2015, roč. 2015, č. 1–2.

727 Ibid., s. 14–15.

a nemožnosti *„zajistit restriktivní ochranu informační diskrece člověka"*.[728] Lze rovněž na obecné úrovni souhlasit s jeho tvrzením, že *„právo se musí nutně zaměřit nikoli na existenci a dostupnost diskrečních informací, ale na způsoby, kterými jsou tyto informace využity"*.[729] V tomto ohledu by se přísná aplikace zásady *accountability* správce mohla zdát na první pohled jako ideální způsob řešení tohoto problému. Zákonodárce stanovuje povinnost zpracovávat osobní údaje tak, aby bylo minimalizováno riziko zásahu do práv subjektu údajů. Dávné informace, které by měly být zapomenuty, bez pochyb takové riziko představují. Mělo by tedy být na správci údajů zajistit své zpracování osobních údajů tak, aby zabránil jejich nežádoucímu zneužití.[730] Ve většině případů však není možné takovou povinnost po správci spravedlivě požadovat, vzhledem k její technické nerealizovatelnosti, nebo zcela nepřiměřené nákladnosti. Na rozdíl od představy zákonodárců není technologické řešení magickým nástrojem, umožňujícím odstranit všechny problémy co danou oblast práva sužují.[731] Performativní regulace i přes své nesporné výhody v podobě značné volnosti, kterou dává regulovaným subjektům možnost vymyslet nejvhodnější řešení jejich problému, není (alespoň v podobě, v jaké je přítomná v Obecném nařízení) odpovědí na problémy, které se krystalizovaly v právu být zapomenut.

Ideální stav by tak bez pochyby byla společnost, jejíž členové většinově dokáží odpouštět bez zapomínání.[732] Je však třeba souhlasit s Corym Coglianesem a Evanem Mendelsonem, když tvrdí: *„No regulatory tool is perfect, especially under every condition. The appropriate test for a regulatory option is not whether it is perfect. It is whether that approach is better than the alternatives – including the alternative of doing nothing."*[733] V současné době v evropském právním

728 Viz POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012, s. 336*,* Téma.

729 Ibid., s. 337.

730 Jako dobré vodítko může posloužit například soukromí v kontextech dle Helen Nissenbaum (NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010).

731 V tomto kontextu srovnej například debaty, které se vedly na půdě Evropského parlamentu během přijímání směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. 4. 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES.

732 Srovnej POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012, s. 337*,* Téma.

733 COGLIANESE, Cory a Evan MENDELSON. Meta-Regulation and Self-Regulation. In: BALDWIN, Robert, Martin CAVE a Martin LODGE (eds.). *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2012, s. 161.

a společenském prostoru nemáme žádné jiné možnosti, jak adresovat problém, kterým absence procesu zapomínání v online prostředí skutečně je. Dokud nedojde k zásadní změně v možnostech automatizované technické kontroly vhodnosti užití obsahu, nebo paradigmatické proměně společnosti, zůstává právo být zapomenut důležitou součástí instrumentáře systému ochrany osobních údajů. Oproti tomu například právní úprava ve Spojených státech tuto možnost nenabízí prakticky vůbec.[734] Do budoucna otevřenou otázkou tak zůstává, zda z hlediska pravděpodobnosti žádoucího příchodu změny celospolečenského přístupu na „odpouštění bez zapomínání", není americká cesta vhodnější.

5.6 Shrnutí kapitoly

Moderní způsoby regulace, jako jsou například performativní pravidla, nabízejí zákonodárci řadu možností, které mohou být využity pro účinnější nastavení systému práv a povinností. To platí zejména pro oblasti právní úpravy, v nichž přímo dochází ke kontaktu s novými technologiemi. Performativní pravidla umožňují svým adresátům, aby si sami zvolili, jak dosáhnout zákonodárcem předepsaného cíle. Díky tomu mohou povinné subjekty přesněji přizpůsobit konkrétní postupy při plnění svých úkolů a tím dosáhnout efektivního využití své snahy a prostředků v závislosti na povaze konkrétní situace, kterou právě potřebují vyřešit. Velká výhoda performativní regulace spočívá rovněž v tom, že není nikterak navázaná na aplikaci konkrétní technologie, ale naopak dává regulovaným subjektům možnost, aby při snaze o dosažení zákonem předepsaného cíle přicházeli s novými inovativními technickými řešeními, které mohou do budoucna zvýšit jejich efektivitu. Nevýhodou performativní regulace jsou pak vyšší nároky na její efektivní aplikaci a vymáhání.

Evropský zákonodárce zvolil metodu performativních pravidel jako základní regulační východisko, na němž je vystavěno Obecné nařízení. To je provedeno prostřednictvím zásady *accountability* správce osobních údajů, dle níž je správce údajů odpovědný (ve smyslu *accountable*) za zpracování které provádí, má mu přizpůsobit proces zpracování tak aby odpovídal požadavkům

734 Srovnej JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016, s. 55–80.

kladeným Obecným nařízením a musí být schopen tento stav prokázat. Druhým klíčovým prvkem, na němž spočívá konstrukce performativní regulace v nové úpravě ochrany osobních údajů, je nezbytné hodnocení rizik, které zpracování údajů představuje pro práva a svobody subjektů údajů a dalších fyzických osob. Právě vůči míře rizikovosti konkrétního zpracování správce údajů poměřuje, jakým způsobem musí splnit povinnosti, které na něj v souvislosti s ním dopadají. Zde se nachází klíč ke granularitě a škálovatelnosti povinností přítomných v Obecném nařízení. Čím je riziko pro práva a svobody osob ohrožených zpracováním údajů vyšší, tím více povinností na správce dopadá a tím větší úsilí musí při jejich plnění vynaložit. To pak platí i naopak, čím je riziko nižší, tím nižší jsou požadavky na správce údajů ve smyslu nezbytné vynaložené snahy na plnění jeho povinností. Riziko pro práva v základu nabývá dvou hodnot: *zásah do práva a svobod hrozí* a zásah *nehrozí*. V případě ohrožení práv se však jeho intenzita může velice lišit. Vzhledem k tomu i přes tuto základní dualitu můžeme o riziku pro práva uvažovat v tradičních pojmech hodnocení rizik, tedy nízké, střední a vysoké riziko. Je však nezbytné zdůraznit, že hodnocení rizika pro práva bude vždy nutně kvalitativní.

Výsledek hodnocení rizikovosti zpracování správci údajů ukáže, jaké konkrétní povinnosti má jakým způsobem plnit. Vyhodnocené riziko totiž představuje proměnnou hodnotu, kterou je možné (a nutné) upravit takřka každou povinnost založenou v Obecném nařízení. Projeví se tak nejen v případě vysoce rizikových zpracování, kdy má správce údajů povinnost plnit nové povinnosti jako např. provedení plné DPIA, ale rovněž například při hodnocení oprávněnosti zájmu správce na zpracování ve smyslu čl. 6 odst. 1 písm. f) Obecného nařízení. Jedinou oblastí povinností, která je z hodnocení rizik takřka vyňata, jsou povinnosti odpovídající právům subjektů údajů uvedeným v Kapitole III Obecného nařízení. S výhradou velmi striktních výjimek jejich aplikaci správce údajů nikdy nemůže zcela vyloučit nebo omezit.

Závěr kapitoly byl věnován vlivu performativní regulace ochrany osobních údajů na efekty vyvolané tokem času. Analýza ukázala, že zásada *accountability* a přístup založený na riziku, mohou napomoci k dlouhodobější udržitelnosti současné právní úpravy vzhledem k nástupu nových technologií a doposud neznámých způsobů zpracování osobních údajů. Na druhou stranu se však

projevilo, že performativní regulace není a nemůže být univerzálním řešením všech problémů právní úpravy ochrany osobních údajů. V otázce (ne)zapomínání v online prostředí totiž nepřináší žádná nová východiska, která by mohla tuto debatu výrazněji posunout.

6 MODERNÍ REGULATORNÍ METODY OCHRANY OSOBNÍCH ÚDAJŮ: SYNTÉZA A DISKUZE

Publikace se zabývá obecnými otázkami právní úpravy ochrany osobních údajů a systému, který základní právo na ochranu osobních údajů garantuje. Zpracování osobních údajů je v této publikaci chápáno jako dynamický proces probíhající v čase, který právní úprava musí být schopná adekvátně postihnout. Druhá kapitola přednesla základní premisy, na kterých systém ochrany osobních údajů spočívá a které je třeba brát v potaz vždy při interpretaci a aplikaci ustanovení právních předpisů upravujících tuto právní oblast. Jako první premisa byla formulována věcná a funkční samostatnost práva na ochranu osobních údajů jako základního práva, které má vlastní cíle, regulatorní metody a prostředky nezávislé na jiných základních právech, zejména na právu na soukromí. Druhou premisou nezbytnou pro řádnou interpretaci ustanovení ochrany osobních údajů je pragmatický předpoklad vhodnosti a nutnosti zpracování osobních údajů v rámci fungování moderní společnosti, a tedy vytvoření právní úpravy ochrany osobních údajů jako rámce prostředí, v němž zpracování údajů probíhá, umožňuje jej a zároveň stanoví jeho limity. Uvedené rovněž vytváří jeden ze dvou účelů právní úpravy ochrany osobních údajů. Třetí premisa spočívá v druhém účelu ochrany osobních údajů, kterým je ochrana práv a svobod subjektů údajů (a veřejného zájmu na této ochraně), před zásahem, který by mohl vzniknout nezákonným zpracováním osobních údajů. Z této premisy vyplývá významná role subjektivních pozitivně formulovaných práv subjektů údajů, které jsou v analyzované právní úpravě obsaženy. Důležitým dílčím poznatkem, který z druhé kapitoly vyplynul, je, že práva subjektů údajů plní významnou funkci v zajištění kontroly správce údajů po celou dobu probíhajícího procesu zpracování a z toho důvodu se jich není možné vzdát nebo jejich výkon vyloučit. Osobní údaje a jejich zpracování je tak nutné chápat nikoli staticky quasi-majetkově, ale jako dynamický proces probíhající v čase. Konečně, čtvrtou premisou, potvrzenou rozhodovací praxí SDEU, je nezbytný preventivní přístup k ochraně osobních údajů. Ten se prakticky projevuje při interpretaci předpisů upravujících ochranu osobních údajů tak, že definiční ustanovení

zakládající oblast působnosti těchto předpisů je třeba interpretovat extenzivně a ustanovení zakládající výjimky naopak restriktivně.

Jak ukázala třetí kapitola této publikace, bývalá právní úprava (směrnice 95/46/ES a z ní vycházející zákon č. 101/2000 Sb.) nedokázala dostatečně flexibilně reagovat na výzvy, které před ni v průběhu plynutí času kladl technologický vývoj. To i přesto, že byla vystavěna v souladu s principem technologické neutrality. Neobsahovala totiž způsob, jak zajistit potřebnou granularitu a škálovatelnost povinností správce, aby mohl proces zpracování údajů přizpůsobit konkrétní situaci, při níž ke zpracování docházelo.

Při nezbytné aplikaci dříve identifikovaných premis bylo třeba v hraničních případech zpracování interpretačně dojít k absurdním závěrům, které spočívaly v nutnosti plnění dané situaci zcela nepřiměřených povinností správce. Příkladem je použití IP adres v kontextu kybernetické bezpečnosti, kdy dle bývalé právní úpravy měl správce například prakticky nerealizovatelnou povinnost informovat subjekty údajů o probíhajícím zpracování. Provozovatelé internetových vyhledávačů se po rozhodnutí SDEU ve věci *Google Spain*[735] ocitli v pozici správce údajů, když indexovali a dále zpracovávali za účelem poskytování vyhledávacích služeb osobní údaje přítomné na stránkách a v dokumentech třetích osob. Jen obtížně však mohli plnit své povinnosti správce, jako např. informační povinnost. Krom toho bylo toto zpracování osobních údajů protiprávní vzhledem k absenci právního titulu, který by odůvodnil zpracování citlivých osobních údajů, které však součástí indexovaných stránek byly bez pochyby také. Třetí příklad pak ukázal, že důslednou aplikací premis a východisek systému ochrany osobních údajů je třeba dojít k závěru, že pod definici zpracování osobních údajů může být zahrnuto rovněž prosté odkazování na dokument, který dané osobní údaje obsahuje. Opět, splnění všech povinností, které vyžadovala směrnice 95/46/ES a zákon č. 101/2000 Sb., bylo v takovém případě nepřiměřené až nemožné. Jako poslední příklad pak posloužil problém anonymizovaných údajů, kterým hrozí v průběhu času v důsledku zlepšujících se technických možností opětovné ztotožnění subjektů údajů, kterých se týkají. Tento příklad dobře demonstruje statičnost minulého chápání pojmu osobní údaj.

735 Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

Vzhledem k tomu, že předchozí právní úprava neobsahovala možnosti, jak se s těmito nedostatky uspokojivě vypořádat, objevily se dvě cesty, které se pokusily problém vyřešit tak říkajíc „mimo systém" právní úpravy ochrany osobních údajů. První cestou bylo zužování výkladu definičních ustanovení tak, aby na problematické případy právní úprava ochrany osobních údajů vůbec nedopadla. Druhou cestou bylo *ad hoc* rozhodnutí dozorových úřadů nevymáhat případy, které byly takto problematické. Obě naznačené cesty je však nezbytné jako možná řešení problému nedostatečné granularity a škálovatelnosti povinností správce odmítnout. První zmiňovanou cestu není možné aplikovat vzhledem k prevenčnímu přístupu k ochraně osobních údajů a ustálené rozhodovací praxi SDEU. Druhou je pak nezbytné vyloučit pro její základní nedostatky v podobě narušení povinností vyplývajících ze zásady legality a právní jistoty.

Odpovědí na tyto problémy tak musela být taková regulace ochrany osobních údajů, která by splňovala podmínky široké a preventivní aplikace a zároveň umožnila dostatečnou vnitřní flexibilitu v podobě granularity a škálovatelnosti povinností správce. Vzhledem k přímé aplikovatelnosti Obecného nařízení na široké spektrum různých druhů správců a zpracování osobních údajů stál evropský zákonodárce před výzvou, jak takovou flexibilitu zajistit. Moderní regulatorní metodou, která opouští tradiční způsob přímého udělování konkrétních povinností, je performativní regulace. Její podstata spočívá v tom, že regulovaným subjektům určí pouze cíl (který může být jak velmi konkrétní, tak velmi abstraktní), kterého mají dosáhnout, ale již konkrétně neurčuje, jak se to má stát.

Evropský zákonodárce pro Obecné nařízení performativní regulaci metodu zvolil. Provedl ji prostřednictvím zásady *accountability* správce (překládané do češtiny jako zásada odpovědnosti), která v stanoví, že správce je odpovědný (ve smyslu *accountable*) za zpracování, které provádí. Obecné nařízení stanoví správcům údajů cíl provádět zpracování tak, aby jeho konkrétní provedení odpovídalo rizikům, která takové zpracování představuje pro práva a svobody subjektů údajů. Nejzásadnější změnou, kterou přineslo Obecné nařízení, tedy byl přesun základní regulatorní metody z přístupu založeného na právech k přístupu založenému na riziku. Čím větší je riziko, tím více má správce konkrétních povinností vyplývajících z Obecného nařízení

(granularita) a tím pečlivěji je musí plnit (škálovatelnost). A naopak – v případě nižšího rizika některé povinnosti nemusí správce plnit vůbec.[736] Pro povinnosti, které mu i přes nižší riziko zůstaly, pak platí, že čím nižší riziko, tím méně úsilí musí vynaložit pro jejich dostatečné naplnění. Hodnocení rizika zpracování působí jako filtr, který se aplikuje prakticky ve všech případech povinností správce údajů, které z Obecného nařízení vyplývají.

Míra rizika a jeho hodnocení je pak také aspektem, ke kterému mají přihlížet dozorové úřady v průběhu vymáhání povinností a udělování sankcí vyplývajících z Obecného nařízení. Jedinou oblastí, na kterou hodnocení rizika nedopadá (s drobnou výhradou výjimky zakotvené čl. 12 odst. 5 a čl. 14 odst. 5 Obecného nařízení), jsou pozitivní subjektivní práva subjektů údajů formulovaná v Kapitole III Obecného nařízení. Ta tak působí jako spodní hranice možností správce osobních údajů při nastavení parametrů daného zpracování.

Principy performativní regulace zakotvené v Obecném nařízení ve formě široké zásady *accountability* správce v kombinaci s přístupem postaveným na riziku vytváří dostatečný prostor pro správce osobních údajů, aby mohl podmínky zpracování přizpůsobit potřebám konkrétního procesu zpracování. Zároveň díky tomu, že práva subjektů údajů tvoří pro modifikace povinností správce v důsledku vyhodnocení rizik zpracování téměř nepřekonatelnou hranici, je normativně zajištěna ochrana subjektu údajů po celou dobu trvajícího zpracování. Konečně, performativní regulace ve spojení s principy technologické neutrality dávají předpoklad, že Obecné nařízení bude mnohem lépe odolávat času a technologickým změnám, než směrnice 95/46/ES.

6.1 Aplikace zásady accountability správce na modelové situace

Cílem této podkapitoly je prozkoumat, zda je možné ustanovení Obecného nařízení interpretovat tak, aby byly překonány nedostatky a problémy příkladů uvedených ve třetí kapitole této publikace. Smyslem je tedy ověřit, zda Obecné nařízení obsahuje dostatečně škálovatelnou regulaci a výjimky, aby

736 Zhodnocení nízkého rizika pro potřeby granularity provedl přímo zákonodárce a projevil ho zanesením jasně formulovaných výjimek z povinností.

byly povinnosti správce vyplývající z uvedených zpracování osobních údajů splnitelné a vzhledem k povaze těchto zpracování přiměřené.

První případ se týkal CERT týmu, který zpracovává osobní údaje v podobě IP adres za účelem zajištění kybernetické bezpečnosti (například prostřednictvím technologie honeypot). Jako hlavní problémy z hlediska nepřiměřených povinností, které na správce dopadaly, byly identifikovány informační povinnost, povinnost poskytnout údaje na základě žádosti o přístup a striktní požadavky na zavedení zákonem předepsaných prostředků a procesů vedoucích k zabezpečení zpracování. Pro aplikaci Obecného nařízení je třeba uvést, že zpracování IP adres v kontextu kybernetické bezpečnosti obecně představuje jen velmi nízké riziko pro práva subjektů údajů, vzhledem k poměrně nízké šanci neoprávněné identifikace. Právní titul pro zpracování bude stejný jako v případě směrnice 95/46/ES (oprávněný zájem správce). V případě plnění povinností souvisejících s právy subjektu údajů se však CERT tým může spolehnout na výjimky, které mu Obecné nařízení poskytuje. Předně se může odvolat na čl. 11 Obecného nařízení, protože se jedná o zpracování osobních údajů, které nevyžaduje identifikaci subjektu. Pokud by však obdržel žádost od subjektu údajů o poskytnutí zpracovávaných údajů, je možné si představit argumentaci, na základě které správce tuto žádost odmítne pro zjevnou nepřiměřenost.[737] Ve prospěch této argumentace správce bude stát rovněž velice nízké riziko zpracování, které navíc může být umocněno vhodným technickým nastavením celé operace. Další povinnosti správce může CERT přizpůsobit na míru tomuto zpracování. Dá se očekávat, že nezbytně vynaložené úsilí na zabezpečení těchto údajů budou vzhledem k míře rizika spíše minimální. CERT však bude muset vést (alespoň minimální) záznamy o činnostech zpracování dle čl. 30, protože nejde o příležitostné zpracování.

Druhý případ se týkal provozovatelů internetových vyhledávačů a jejich zpracování osobních údajů, které získali indexací v online dokumentech třetích stran a dále je zpracovávali za účelem poskytování vyhledávacích služeb. Zásadní problém v době účinnosti směrnice 95/46/ES spočíval v tom, že tito správci neměli oprávnění takto zpracovávat citlivé osobní

737 Srovnej MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12.

údaje (zvláštní kategorie osobních údajů) a celý proces zpracování byl tak v konečném důsledku nelegální. Obecné nařízení tento problém vyřešilo za prvé tím, že podmínky uvedené v jeho čl. 9 nejsou speciálními právními tituly pro zpracování zvláštních kategorií osobních údajů, ale pouze novými podmínkami, které správce údajů musí splnit nad rámec povinnosti disponovat právním titulem ke zpracování dle čl. 6 Obecného nařízení.[738] Internetový vyhledávač se tak může v základu i nadále spoléhat na právní titul oprávněného zájmu (tak jak předeslal SDEU v rozhodnutí ve věci *Google Spain*), navíc k němu však bude třeba prokázat možnost aplikace jedné z výjimek uvedených v čl. 9 odst. 1. Jako vhodné se jeví výjimka uvedená pod písm. g), které uvádí, že zpracovávat zvláštní kategorie osobních údajů je možné tehdy, pokud je to *„nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů"*.[739] Aplikovatelnost tohoto ustanovení pak potvrdil rovněž SDEU v rozhodnutí ve věci *GC a další* (C136/17).[740] Je totiž nezbytné vzít v potaz důležitost role, kterou internetové vyhledávače fakticky mají pro možnost výkonu takřka všech zaručených informačních práv v kyberprostoru.[741] Zpracování zvláštních kategorií osobních údajů samozřejmě představuje vyšší riziko pro práva subjektů údajů. Tento aspekt musí provozovatel vyhledávací služby zohlednit. To platí jak v případech, kdy se na něj subjekt údajů obrátí se žádostí o výkon svého práva, tak v případech plnění dalších povinností vyplývajících z Obecného nařízení. Proto má dle SDEU správce postupovat tak, že v případě obdržení žádosti o výmaz výsledku vyhledávání, který se týká zvláštních kategorií osobních údajů, povinen až na naprosté výjimky těmto žádostem vyhovět.[742] V kontextu dalších povinností správce je však dále vhodné upozornit na výjimku z informační povinnosti uvedenou v čl. 14 odst. 5 písm. b), dle které správce

738 Srovnej též Guidelines 3/2019 on processing of personal data through video devices. *Evropský sbor pro ochranu osobních údajů* [online]. 2019, s. 14 [cit. 31. 7. 2019].

739 Čl. 9 odst. 1 písm. g) Obecného nařízení.

740 Viz body 61–68 rozsudku Soudního dvora Evropské unie ze dne 24. 9. 2019 ve věci *GC a další*, C-136/17.

741 Tuto roli rovněž výslovně uznal SDEU v rozsudku ve věci *Google Spain*, C-131/12.

742 Viz bod 69 rrozsudku Soudního dvora Evropské unie ze dne 24. 9. 2019 ve věci *GC a další*, C-168/17.

údajů nemusí plnit informační povinnost v případě, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí.

Třetí případ se týkal situace, kdy vytvořením hypertextového odkazu na dokument třetí strany dochází ke zpracování osobních údajů uvedených v cílovém dokumentu. Analýza provedená v části 3.3 této publikace ukázala, že v odůvodněných případech je tato interpretace nutná. Platí to zejména tehdy, použije-li správce údajů hyperlink za účelem šíření osobních údajů, které se nacházejí na druhé straně. Přesuneme-li se do kontextu Obecného nařízení, bude se aplikovat zásada *accountability* správce, která se rovněž projevuje přesunem důkazního břemene na správce. Pokud se osoba, která odkaz vytvořila, bude snažit tvrdit, že není v postavení správce, bude muset prokazovat, a z okolností případu bude muset být zcela jasně dovoditelné, že zpracování osobních údajů na odkazovaném dokumentu neměla v úmyslu, neurčila mu tedy účel a jde o zpracování *de facto* nahodilé. V případě, že bude z okolností zřejmé, že prostřednictvím odkazu daná osoba chtěla šířit osobní údaje umístěné v cílovém dokumentu, bude se zcela jistě jednat o správce údajů. Je obtížné takto abstraktně určit rizikovost takového zpracování, protože bude rovněž záviset na konkrétních osobních údajích, které jsou takto zpracovávány a nikoli jen na způsobu zpracování (odkaz). Právním titulem pro zpracování bude obvykle oprávněný zájem správce v podobě možnosti zajištění svobody projevu nebo práva podnikat. Jisté je, že subjektům údajů budou svědčit práva vyplývající z Kapitoly III Obecného nařízení. Správce údajů při tom může aplikovat výjimky v této kapitole Obecného nařízení uvedené. V kontextu ostatních povinností správce pak dle mého názoru bude moci správce postupovat v minimální nutné míře odpovídající riziku zpracování a technické a faktické realizovatelnosti těchto povinností.[743] Pragmatickou interpretací je v daném případě nutné dojít k závěru, že je klíčové, aby byla zachována možnost subjektů údajů dovolat se svých práv. Plnění dalších povinností správce však bude moci být zcela minimalizováno.

Ve čtvrtém případě jsem se zabýval využitím datových sad obsahujících osobní údaje v aplikacích pracujících s otevřenými daty. Hlavní problém

743 Jak vyplývá z posledních rozhodnutí SDEU, správce může být odpovědný jen za rozsah zpracování údajů, které má fakticky možnost ovlivnit (viz rozsudek Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat*, C-25/17; a rozsudek Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci *Fashion ID*, C-40/17).

spočíval v tom, že bývalá právní úprava nedokázala dostatečně reagovat na vývoj v čase v kontextu rizika opětovného ztotožnění anonymizovaných údajů. Díky tomu, že je Obecné nařízení vystavěné na přístupu postaveném na riziku, je zde mnohem plynulejší a prostupnější cesta mezi kategoriemi anonymní a pseudonymní údaj. Stále platí, že anonymní údaje jsou z aplikace Obecného nařízení zcela vyloučeny. Pokud dojde během životního cyklu využití těchto dat k takovému vývoji, který umožní opětovnou identifikaci subjektu údajů (ať už zlepšením výpočetních možností, nebo faktickou publikací jiných zdrojů dat, které umožní propojení se současnými daty), začne se Obecné nařízení aplikovat. Neznamená to ale bez dalšího, že by správce údajů musel se zpracováním ustat. Pokud k takové situaci dojde, bude záležet na pravděpodobnosti a náročnosti ztotožnění subjektů údajů, povaze daných údajů a dalších aspektech, které ovlivní míru rizika, jaké zpracování představuje. Velmi pravděpodobně pak takové riziko bude velice malé. Správce údajů tedy bude muset prokázat platný právní titul (zřejmě opět oprávněný zájem správce)[744] a plnit povinnosti vyplývající z práv subjektů údajů uvedených v Kapitole III Obecného nařízení (s možností tam uvedených výjimek). Zbylé povinnosti si pak může nastavit v minimální nezbytné podobě dle míry rizika zpracování.

Uvedený přehled aplikace ustanovení Obecného nařízení na problematické případy ukazuje přednosti nové právní úpravy postavené na zásadě *accountability* a přístupu postaveném na riziku. Připouští totiž takový výklad, který dané zpracování nejen dovoluje, ale umožňuje správcům údajů upravit si konkrétní způsob splnění jejich povinností tak, aby odpovídal potřebám konkrétní situace.

6.2 Problémy performativní regulace v kontextu Obecného nařízení

Analýza představená v této publikaci ukázala, že regulace založená na performativních pravidlech, zásadě *accountability* správce a principu postaveném na riziku má potenciál efektivně naplňovat cíle práva na ochranu osobních údajů. Napsaná v textu Obecného nařízení tato právní úprava vypadá velice

744 Srovnej MÍŠEK, Jakub. *Právní aspekty otevřených dat*. Rigorózní práce Brno: Masarykova univerzita, Právnická fakulta, 2019, 172 s., s. 119–131.

dobře a vysoce funkčně. Její realizace prostřednictvím aplikace norem různými zapojenými stranami (subjekty údajů, správci údajů, dozorové orgány i soudy) však přináší praktická úskalí a problémy, kterých je třeba se vyvarovat. Pokud selže praktická realizace nového regulatorního přístupu, které Obecné nařízení přineslo, skutečná každodenní aplikace práva na ochranu osobních údajů se nezlepší.[745] Obecné nařízení by pak zůstalo v pozici hezkého myšlenkového experimentu bez reálného efektu. Tato podkapitola se věnuje dvěma zásadním překážkám, které jsou systematicky přítomné v právní úpravě ochrany osobních údajů postavené na performativních pravidlech.

6.2.1 Problém vymáhání povinností a sankce

Podmínkou úspěšného působení performativní regulace na prostředí, které reguluje, je precizní a důsledné vymáhání povinností, které z ní vycházejí. Jak uvádí Coglianese, efektivní dohled, kontrola a vymáhání povinností jsou naprosto klíčové podmínky pro její dobré fungování.[746] Performativní regulace tak představuje značnou výzvu pro dozorové úřady, které ji mají kontrolovat a vymáhat, protože krom ověření finálního splnění nebo nesplnění konkrétních povinností musí ještě hodnotit, zda povinný subjekt zvolil správnou cestu, jak předepsaného cíle dosáhnout.[747] To samozřejmě na dozorové úřady klade vyšší nároky jak z hlediska nákladů a materiálního zajištění, tak z hlediska znalostí.

Dozorovému úřadu (v ČR jde o ÚOOÚ)[748] přísluší dle textu Obecného nařízení řada kompetencí, které může (a musí) v kontextu kultivace prostředí zpracování osobních údajů vykonávat. Jedním z cílů Obecného nařízení je sjednocení přístupu k vymáhání povinností ze strany dozorových úřadů napříč Evropskou unií, zavedení pokud možno jednotného modelu postupu dozorových úřadů[749] a udělování sankcí tak, aby správce údajů byl

745 Nové přístupy k regulaci kladou vzhledem ke své nezvyklosti vyšší nároky na příjemce norem, a tím vytvářejí vyšší odpor proti správné implementaci. Na tomto projevu je možné velmi dobře demonstrovat performativní podstatu práva (ve smyslu podobném jako umělecká performance). Srovnej MALANÍK, Michal. Performativní povaha právní interpretace. *Jurisprudence*, 2017, roč. 26, č. 5.

746 Srovnej COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3, s. 562–563.

747 Ibid., s. 547.

748 Viz § 50 a násl. zákona č. 110/2019 Sb.

749 Viz čl. 58 odst. 2 Obecného nařízení.

za stejný prohřešek potrestán odpovídajícím způsobem bez ohledu na to, který dozorový úřad kterého členského státu jeho věc projednává.[750] K zajištění jednotného postupu má přispět formalizovaný proces podle čl. 60–63 Obecného nařízení. Přispět však může rovněž Evropský sbor pro ochranu osobních údajů, a to jak zapojením v rámci formalizovaného procesu,[751] tak metodickou činností.[752] Dle čl. 58 odst. 2 mají dozorové úřadu celou řadu nápravných pravomocí, počínaje upozorněním na neoprávněné zpracování a udělením napomenutí za porušení povinností vyplývajících z Obecného nařízení, přes nařízení splnění konkrétní povinnosti, až po uložení správní pokuty. K povaze pokut Obecné nařízení na několika místech velice striktně uvádí, že uložené sankce musí být v každém jednotlivém případě účinné, přiměřené a odrazující.[753] Konkrétní sankce jsou uvedeny v čl. 83 a jsou rozděleny do dvou skupin. Čl. 83 odst. 4 umožňuje udělit sankce za porušení ustanovení, která se týkají zejména různých aspektů zabezpečení zpracování, a to až do výše 10 000 000 €, nebo až do výše 2 % celkového celosvětového ročního obratu za předchozí finanční rok, dle toho, která hodnota je vyšší. Čl. 83 odst. 5 umožňuje udělit sankce za porušení ustanovení Obecného nařízení, které se týkají základních zásad a práv subjektů údajů, a to až do maximální výše, která je dvojnásobná než v předchozím případě.

Obecné nařízení a jeho zásada *accountability* správce přinesly z hlediska kontroly a vymáhání povinností zásadní změnu v podobě přesunutí důkazního břemene na správce údajů.[754] Ten musí být v souladu s čl. 5 odst. 2 schopen doložit a prokázat, že v průběhu svého probíhajícího zpracování údajů dodržuje všechny povinnosti, které mu z Obecného nařízení vyplývají. Jak uvádí Bendan Van Alsenoy, povinnost správce prokázat řádnost jeho plnění je protkána řadou dalších ustanovení Obecného nařízení, jako je např. čl. 7

750 Viz čl. 63 Obecného nařízení. Požadavek rovnocenné úrovně ochrany je rovněž uveden v bodě 10 odůvodnění Obecného nařízení.

751 Viz čl. 65 Obecného nařízení.

752 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679. *Evropská komise* [online]. 3. 10. 2017, č. WP253, 17 s. [cit. 30. 6. 2020].

753 Viz čl. 83 odst. 1, čl. 84 odst. 1 Obecného nařízení.

754 Shodně ALSENOY, Brendan Van. *Data protection law in the EU: roles, responsibilities and liability*. Cambridge: Intersentia, 2019, s. 104–105; VOIGT, Paul a Axel von dem BUSSCHE. *The EU general data protection regulation (GDPR)*. New York, NY: Springer Berlin Heidelberg, 2017, s. 31.

požadující prokázání obdržení platného souhlasu, čl. 11 a 12,[755] a konečně také čl. 24, který jen dále rozvádí obecnou zásadu uvedenou v čl. 5 odst. 2.[756] Pokud má regulace postavená na zásadě *accountability* správce a principu založeném na riziku zpracování opravdu fungovat a přinést benefity, které potenciálně nabízí, je potřeba, aby ke zpracování a jeho přípravě správci údajů přistupovali aktivně a zodpovědně a příprava zpracování se nestala bezduchým zaškrtáváním políček na seznamu bez reálného praktického dopadu.[757]

Tentýž požadavek však nutně platí i pro dozorové orgány. Je samozřejmě jednodušší formálně kontrolovat pochybení vyplývající ze standardní regulace využívající předem jasně vymezených povinností. Performativní regulaci (zajištěné zásadou *accountability* a přístupem založeným na riziku) je však třeba respektovat i ve fázi mocenského působení na správce údajů. Dozorové úřady musí při plnění svých povinností plnit aktivní roli a komunikovat se správci údajů. Při provádění kontrol je nezbytné soustředit se nejen na dopady zpracování ale rovněž na to, jakým způsobem správce údajů využil možností v podobě granularity a škálovatelnosti povinností. Dozorový úřad může určit správnost plnění povinností správce údajů jedině na základě prvotního vyhodnocení, jaké bylo riziko zpracování a jaké mu proto odpovídaly konkrétní povinnosti. Důležitou rolí dozorového úřadu tak je nově rovněž kontrola, zda hodnocení rizik (ve smyslu obecného plnění povinností správce, nikoli DPIA) je provedeno korektně a odpovídá realitě.[758] Získané poznatky úřad následně porovná se skutečným stavem zpracování osobních údajů, které správce údajů provádí.[759] Takový přístup však samozřejmě

755 Správce v tomto případě musí prokázat, že provádí zpracování, které nevyžaduje identifikaci.

756 Srovnej ALSENOY, Brendan Van. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2016, roč. 7, č. 3, s. 282.

757 Srovnej též QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 503; Dále též KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. BNA *Bloomberg Privacy and Security Law Report*. 2012.

758 Shodně viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement on the role of a risk-based approach in data protection legal frameworks. *Evropská komise* [online]. 30. 5. 2014, č. 14/EN, WP 218, s. 4.

759 Srovnej HODGES, Christopher. Delivering Data Protection: Trust and Ethical Culture Discussion. *European Data Protection Law Review*, 2018, roč. 4, č. 1, s. 66–69.

obnáší vyšší nároky na provoz celého úřadu.[760] Krom toho, míra rizika souvisejícího s kontrolovaným zpracování by se dále měla projevit rovněž v případě udělování sankcí a jejich výši.[761] V případě porušení povinností správce při nízkorizikovém zpracování by tak dozorový úřad měl sáhnout spíše po alternativních způsobech nápravy, než rovnou po finanční sankci.

Pro dozorové úřady moderní způsob regulace přítomný v Obecném nařízení přináší dvě zásadní výzvy. První je nezbytnost ochoty a schopnosti změnit náhled na regulatorní principy, na kterých spočívá ochrana osobních údajů, tak aby odpovídal realitě nové právní úpravy. Druhou je získání dostatečného materiálního a personálního zázemí, aby dozorový úřad mohl svoji novou náročnější roli plnit. V tomto veskrze praktickém ohledu spatřuji základní problém nové právní úpravy. Evropský zákonodárce se rozhodl jít cestou performativní regulace, vhodnou z hlediska regulované materie, ovšem bez dostatečného zabezpečení jejího výkonu, protože ten jde (doslova) na účet členských států. To se může projevit jako problém zejména v těch oblastech, ve kterých doposud není silná tradice ochrany osobních údajů vybudována.

Pro řádné fungování systému postaveného na performativní regulaci jsou efektivní dohled, kontrola a vymáhání povinností nezbytné. Nesmí totiž nastat situace, že by správci údajů začali systematicky zneužívat určité volnosti, kterou jim performativní pravidla dávají. V takovém případě by celý systém ochrany osobních údajů byl zcela iluzorní.[762]

760 Viz též QUELLE, Claudia. The 'Risk Revolution' in EU Data Protection Law: We can't Have Our Cake and Eat it, Too. In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 50.

761 Viz PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679. *Evropská komise* [online]. 3. 10. 2017, č. WP253, s. 11 [cit. 30. 6. 2020].

762 Tento problém je obzvlášť viditelný v kontextu ustanovení § 62 odst. 5 zákona č. 110/2019 Sb. Dle něj ÚOOÚ musí upustit od udělení správního trestu za porušení ustanovení Obecného nařízení, pokud se ho dopustili správci uvedení v čl. 83 odst. 7 Obecného nařízení (tedy orgány veřejné moci a veřejné subjekty). Již za krátkou dobu od účinnosti tohoto ustanovení je možné upozornit na dva případy, kdy ÚOOÚ upustil od potrestání Ministerstva vnitra, přičemž případné tresty se pohybovaly řádech vyšších statisíců až nižších milionů korun (viz rozhodnutí předsedkyně ÚOOU ze dne 6. 6. 2019, č. j. UOOU-03469/18-19 a rozhodnutí předsedkyně ÚOOU ze dne 5. 12. 2019, č. j. UOOU-09383/18-17). Nebezpečnost tohoto ustanovení dokládá velice bizarní argumentace Ministerstva vnitra v druhém uvedeném rozhodnutí, ve které se (neúspěšně) snažilo přesvědčit ÚOOÚ, že samotné vedení řízení o přestupku je nehospodárné, protože stejně nemůže vést k sankci, takže by bylo nejlepší, kdyby se nevedlo vůbec.

Vedle dozorových úřadů mohou vymáhání práv pomoci další prostředky a nástroje. Správce údajů se v kontextu zásady *accountability* nezodpovídá jen dozorovému úřadu, ale rovněž subjektům údajů, kteří mohou požadovat výkon svých práv a domáhat se ho rovněž přímo soudní cestou.[763] Bohužel řada subjektů údajů se k tomuto kroku sama nerozhodne. Možným řešením tak může být institut hromadné žaloby.[764] České právo zatím tuto možnost nezná, Ministerstvo spravedlnosti nicméně v současné době návrh zákona o hromadných žalobách připravuje.[765] Vedle hromadných žalob počítá Obecné nařízení rovněž s možností zastupování subjektů údajů neziskovými organizacemi založenými ve veřejném zájmu s účelem ochrany práv subjektů údajů.[766] Odst. 2 čl. 80 Obecného nařízení dokonce dává členským státům možnost stanovit, že tyto neziskové organizace mohou zastupovat subjekty údajů i bez jejich pověření. Tento institut má předpoklad pro to stát se důležitou součástí při zajištění kontroly správců údajů a vymáhání povinností, které jim z Obecného nařízení plynou. Nabízí totiž alternativu ke kontrole prováděné dozorovými úřady, kterým by tak mohl ulehčit jejich pozici. Zároveň na rozdíl od běžných způsobů vymáhání práv subjekty údajů (včetně hromadných žalob) představuje příslib specializovaného znalostně profesionálního řešení. Bohužel český zákonodárce tuto možnost uvedenou v čl. 80 do českého práva neprojevil.

Poslední možností, jak posílit vymáhání povinností souvisejících se zpracováním osobních údajů, může být zavedení efektivní trestněprávní sankce. V současné době obsahuje trestní zákoník skutkovou podstatu protiprávního zpracování osobních údajů v trestném činu neoprávněného nakládání s osobními údaji.[767] Tento trestný čin však dopadá pouze na zpracování osobních údajů, které byly *„shromážděné v souvislosti s výkonem veřejné*

763 Viz čl. 79 Obecného nařízení.

764 Viz EVERETT, Miriam a Lucy McALISTER. Court of Appeal Confirms First Successful UK Class Action for Data Breach. *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, 2018, roč. 2, č. 11; VAN HAL, Timothy J. Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection Note. *Vanderbilt Journal of Entertainment and Technology Law*, 2013, roč. 15, č. 3.

765 Viz Návrh zákona o hromadných žalobách (703/19). *Úřad vlády České republiky* [online]. ODOK [cit. 30. 6. 2020].

766 Viz čl. 80 Obecného nařízení.

767 Viz § 180 zákona č. 40/2009 Sb.

moci“,[768] případně pokud dojde k porušení povinnosti mlčenlivosti při zpracování osobních údajů získaných v souvislosti s výkonem povolání. Tento trestný čin je bohužel nesmírně úzce vymezen.[769] Paradoxně nedopadá na ty nejvíce společensky škodlivé a nebezpečné případy zpracování osobních údajů v podobě protiprávního masového sledování, profilování nebo dalších zneužití osobních údajů v kontextu obchodních praktik, které Shoshana Zuboff nazývá *Surveillance Capitalism*.[770] Rozšíření skutkové podstaty tohoto trestného činu i na takové případy, zejména pak v kontextu trestní odpovědnosti právnických osob, by mohlo představovat vhodné posílení možnosti vymáhání práva na ochranu osobních údajů.

6.2.2 Vysoké nároky na správce údajů

Obecné nařízení a jeho moderní regulatorní přístup neklade vysoké nároky jen na dozorové úřady, ale rovněž (a především) na správce údajů. Tento problém opět vyplývá z podstaty performativní regulace. V minulosti byla performativní regulace používána v oblastech, kde upravovala chování profesionálů, kteří se v dané oblasti dokázali orientovat. Jako příklad je možné uvést oblast kybernetické bezpečnosti,[771] ochrany životního prostředí,[772] energetiky[773] a stavebnictví.[774] Díky svým znalostem dokážou profesionálové vytěžit maximum výhod,

768 § 180 zákona č. 40/2009 Sb., odst. 1.

769 Poměrně překvapivě důvodová zpráva k novému trestnímu zákoníku textaci ustanovení označila za posun vpřed, protože se oproti předchozí právní úpravě tento trestný čin začal dotýkat kontextu celé veřejné moci a nikoli jen veřejné správy. Srovnej Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník. Zvláštní část, § 178. Dostupné z: Beck-online [Právní informační systém]. [cit. 30. 6. 2020].

770 ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. 1. vyd. New York: PublicAffairs, 2019.

771 Srovnej POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1.

772 Srovnej COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Regulation. *Administrative Law Review*, 2004, roč. 55, č. 4; ZARKER, Kenneth A. a Robert L. KERR. Pollution prevention through performance-based initiatives and regulation in the United States. *Journal of Cleaner Production* [online]. 2008, roč. 16, č. 6, Advancing Pollution Prevention and Cleaner Production: USA's Contribution.

773 Srovnej LOWRY, Mark Newton a Lawrence KAUFMAN. Performance-Based Regulation of Utilities. *Energy Law Journal*, 2002, č. 2.

774 Srovnej FOLIENTE, Greg C. Developments in performance-based building codes and standards. *Forest Products Journal*, 2000, roč. 50, č. 7–8; MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4.

které performativní regulace nabízí. Hlavní výhodou je přitom právě flexibilita, protože performativní regulace umožňuje přesné přizpůsobení plnění konkrétních povinností dle potřeb specifické situace. Aby této flexibility dokázal regulovaný subjekt využít, musí v první řadě znát oblast svého působení.

Právě v tom spočívá problém aplikace performativní regulace na Obecné nařízení. Vzhledem ke své obecnosti dopadá tento předpis na širokou škálu různých správců od velkých datových společností až po svazy zahrádkářů. Myslím, že nebude velkou nadsázkou tvrzení, že Obecné nařízení reguluje v naprosté většině zpracování osobních údajů, které provádí laik v oblasti ochrany osobních údajů. Velmi dobře to shrnuje Radim Polčák, když uvádí: *„Zřejmou nevýhodou performativních pravidel je též jejich nezvyklost pro regulované subjekty, které si, stručně řečeno, neumí vládnout samy. Toto riziko se u nás naplno projevilo například s příchodem GDPR. Za vědomé účasti médií se nejprve vytvořilo obecné povědomí o složitosti a drakonickém charakteru nařízení, aby následně povstali experti, kteří za tučný poplatek všechny možné složitosti vyřeší. Ve skutečnosti však v důsledku nezkušenosti a diletantismu většiny nově vyskytnuvších se odborníků došlo k tomu, že konkrétní pravidla často neodpovídala potřebám regulovaných subjektů, byla nesmyslná či formalistická – to zpravidla proto, že byla v rozporu se smyslem nařízení postavena na jednom modelu kopírovaném stále dokola bez ohledu na okolnosti.“*[775] Bývalá právní úprava neflexibilně dopadala svými povinnostmi na všechny povinné subjekty bez rozdílu. Současná právní úprava sice umožňuje větší flexibilitu v podobě granularity a škálovatelnosti povinností, ale po všech správcích údajů vyžaduje stejnou (vysokou) úroveň znalostí a schopností, aby těchto nových výdobytků dokázali plně využít. Problém evropské právní regulace ochrany osobních údajů, který bychom mohli označit jako „jedna velikost nesedí všem“, tak byl jen virtualizován na vyšší informační úroveň.[776] Naštěstí na této vyšší informační úrovni jde o problém výrazně snadněji řešitelný.

Mezi správci osobních údajů je možné identifikovat skupiny typově stejných správců. Bude se jednat zejména o zástupce SME, ale například i o typově stejné správce v oblasti výkonu veřejné správy, kteří budou mít obecně totožné potřeby, co se zpracování osobních údajů týče. Různost procesů

775 POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 15.

776 K virtualizaci jako fenoménu více viz LÉVY, Pierre. *Becoming virtual: reality in the Digital Age*. New York: Plenum Trade, 1998.

zpracování a tedy výhody, které performativní regulace přináší, se objevují až u specializovaných nebo velkých správců údajů. Všichni živnostníci podnikající v oblasti obuvnictví budou mít velice podobné požadavky na zpracování osobních údajů. Stejně tak všechny mateřské školy, všechny malé obce, provozovatelé (malých) e-shopů a podobně. Nová právní úprava pro takové případy nabízí řešení v podobě tzv. kodexů chování (*„codes of conduct"*), které jsou upraveny v čl. 40 Obecného nařízení.[777] Kodexy chování jsou (resp. budou, protože doposud nebyl žádný přijat) dokumenty vytvořené zástupci různých kategorií správců osobních údajů a následně schválené dozorovým úřadem jako modelový příklad dobré praxe.[778] Pokud správci údajů budou zpracovávat údaje za typově odpovídajícími účely a dodrží při tom doporučení vyplývající z kodexu chování, je možné takovou praxi chápat jako prokázání dodržení povinností správce ve smyslu čl. 24 Obecného nařízení.[779]

Kodexy chování mohou nesmírně pomoci správnému fungování performativní regulace v systému ochrany osobních údajů. Mohou zhojit znalostní deficit na straně správců údajů, pro které budou představovat neocenitelnou pomoc pro řádné splnění povinností vyplývajících ze zásady *accountability*. Dokážou však nesmírně usnadnit práci rovněž dozorovým úřadům, a snížit nákladnost a náročnost vymáhání práva.[780] Pro dozorový úřad bude výrazně jednodušší hodnotit stav splnění povinností se vzorem v podobě kodexu chování (obzvláště ve velkém množství typizovaných případů), než kdyby musel při každé jednotlivé kontrole nejprve hodnotit, zda správce údajů vůbec vyhodnotil, jak má nastavit své zpracování vzhledem k riziku, které představuje.

Existenci formalizované právní úpravy kodexů chování, kterou Obecné nařízení obsahuje společně s pobídkou k jejich vytváření, je nutné zcela přivítat. Nezbývá než doufat, že se v brzké době začnou používat i prakticky. Pro řádné fungování performativní regulace využívající zásady *accountability* správce a přístupu postaveného na riziku jsou totiž klíčové.

777 Srovnej též body 98–99 odůvodnění Obecného nařízení.

778 Více viz Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. *Evropský sbor pro ochranu osobních údajů* [online]. 2019, 29 s. [cit. 30. 6. 2020]; Dále též KOŠČÍK, Michal a Matěj MYŠKA. Data protection and codes of conduct in collaborative research. *International Review of Law, Computers & Technology* [online]. 2018, roč. 32, č. 1.

779 Viz čl. 24 odst. 3 Obecného nařízení.

780 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 547.

7 ZÁVĚR

Tato publikace se zabývala obecnými teoretickými problémy právní úpravy ochrany osobních údajů. Vycházela ze čtyř základních premis, na kterých ochrana osobních údajů spočívá, a které byly detailně popsány v druhé kapitole této publikace. Jsou jimi i) věcná a funkční samostatnost práva na ochranu osobních údajů jako základního práva, včetně samostatných účelů a metod regulace, ii) pragmatická nezbytnost zpracování osobních údajů pro fungování moderní společnosti, iii) garantovaná vysoká úroveň ochrany osobních údajů a s ní související silná role práv subjektů údajů a iv) nezbytnost preventivního přístupu k ochraně osobních údajů. Výzkumnou otázkou této knihy bylo, zda Obecné nařízení obsahuje mechanismy, které zajistí škálovatelnost a granularitu povinností správců osobních údajů lepším způsobem než směrnice 95/46/ES tak, aby nedocházelo k nepřiměřenému zatížení správců údajů a zároveň byla zachována dostatečná ochrana práv subjektů údajů. Za účelem jejího zodpovězení byly formulovány čtyři dílčí výzkumné otázky, na které je možné na základě poznatků získaných a formulovaných v samotném textu publikace možné odpovědět následovně:

I) Jaké byly z hlediska granularity a škálovatelnosti povinností hlavní nedostatky směrnice 95/46/ES?

Hlavní nedostatky systému právní úpravy směrnice 95/46/ES z hlediska granularity a škálovatelnosti povinností správce spočívaly v tom, že právní úprava nedokázala dostatečně postihnout potřeby specifických zpracování, na které dopadala. Jednalo se zejména o metody zpracování osobních údajů, které se objevily v důsledku technologického vývoje a na který právní úprava nedokázala dostatečně zareagovat.[781] Bývalá právní úprava obsahovala přehnaně statickou úpravu povinností správce, ze kterých nabízela jen velmi málo výjimek a neposkytovala ani žádné jiné nástroje, které by umožnily

[781] Viz HERT, Paul de. The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents Editorial. *Utrecht Journal of International and European Law,* 2015, roč. 31, č. 80, s. 1; KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*. 2012, s. 14; POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014 [cit. 30. 6. 2020].

jejich škálovatelnost a granularitu. Správce údajů se tak mohl snadno dostat do situace, kdy splnění těchto povinností bylo vzhledem k povaze zpracování a cílům právní úpravy nepřiměřeně zatěžující. Tak tomu bylo v případě zpracování IP adres v kontextu výkonu činností zajišťujících kybernetickou bezpečnost, například prostřednictvím technologie Honeypot.[782] Těmto správcům údajů bývalá právní úprava ukládala prakticky nesplnitelnou povinnost informovat subjekty údajů o probíhajícím zpracování a dále rovněž vzhledem k povaze zpracování nepřiměřenou povinnost vést záznamy o manipulaci s daty. Ještě zásadněji se nedostatek škálovatelnosti a granularity projevil v případech, kdy bylo zpracování osobních údajů od počátku zcela protiprávní, byť existoval silný společenský zájem na tom, aby probíhalo. Takovým případem bylo zpracování osobních údajů indexovaných na stránkách a v dokumentech třetích stran při provozování služeb internetového vyhledávače. Součástí těchto dokumentů byly navíc rovněž citlivé osobní údaje. Bývalá právní úprava nenabízela právní titul, kterým by toto zpracování bylo umožněno, a to i přes nesporně důležitou roli, kterou webové vyhledávače hrají za hlediska zajištění práva na informace a svobodu projevu.[783] Nedostatek vnitřní škálovatelnosti a granularity se objevil i z hlediska nedostatečné flexibility bývalé právní úpravy v otázce přechodu mezi anonymními a pseudonymními údaji. Pokud si mají anonymizované údaje zachovat informační hodnotu, jsou neustále v ohrožení opětovného ztotožnění, které narůstá s plynoucím čase a nárustem použitelné výpočetní a informační kapacity, kterou má každý na dosah ruky. Bývalá právní úprava neumožňovala z hlediska plnění povinností správce žádný plynulý přechod od fáze anonymních údajů, které byly zcela vyloučeny z aplikace směrnice 95/46/ES, do fáze údajů pseudonymních, ve které správce údajů již musel plnit všechny povinnosti vyplývající z právní úpravy, byť praktický rozdíl v riziku opětovného ztotožnění byl v konkrétním případě třeba minimální.

II) Jaká jsou možná řešení těchto nedostatků?

V době účinnosti bývalé právní úpravy se objevila dvě možná řešení uvedených nedostatků, které identifikuje čtvrtá kapitola této publikace. První

782 Srovnej SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security,* 2017, roč. 2017, č. 1.

783 Srovnej vyjádření SDEU v rozsudku ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12.

spočívalo v restriktivním výkladu definičních ustanovení právní úpravy ochrany osobních údajů a tím v omezení její působnosti tak, aby nedopadala na případy, ve kterých by aplikace všech povinností byla vzhledem k jejich povaze neproporcionální. Druhé spočívalo v *ad hoc* rozhodnutí dozorových úřadů nevymáhat případy, které byly takto problematické. Obě tato řešení však bylo nutné odmítnout. První z toho důvodu, že odporuje účelům a základním premisám systému ochrany osobních údajů, kterými jsou zajištění ochrany práv a svobod fyzických osob v kontextu zpracování jejich osobních údajů, umožnění výkonu jejich práva na informační sebeurčení a vytvoření bezpečného prostředí, ve kterém je minimalizované riziko vzniku zásahu do těchto práv a svobod. Z toho pak vyplývá nezbytnost prevenčního principu ochrany osobních údajů, který se projevuje extenzivní interpretací definičních pojmů, a naopak restriktivní interpretací výjimek. Nezbytnost tohoto přístupu potvrzuje rovněž rozhodovací praxe SDEU. Druhé řešení identifikované v kontextu bývalé právní úpravy je nutné odmítnout z toho důvodu, že svévolné nevymáhání povinností vyplývajících z bývalé právní úpravy zcela odporovalo požadavkům na výkon veřejné moci v podobě zásady legality a podrývalo právní jistotu adresátů právních norem. Při pohledu optikou Fullerovy Morálky práva došlo k porušení minimálně dvou z osmi Fullerových požadavků.[784]

Třetí možností vyřešení identifikovaných problémů bývalé právní úpravy tak byla nezbytná změna regulatorní metody, na které právní úprava ochrany osobních údajů spočívá. Tu přineslo Obecné nařízení v podobě regulatorní metody využívající performativních pravidel. Silnou stránkou této regulatorní metody je její flexibilita.[785] Zákonodárce určuje jen cíl, kterého má být dosaženo, a následně umožňuje povinným subjektům, aby si konkrétní

784 Právní norma nesmí uložit povinnost přesahující reálné možnosti povinného subjektu a právní normy musí být vymáhány. FULLER, Lon L. *The morality of law*. Rev. vyd. New Haven: Yale University Press, 1978, s. 39; Dále viz KUNER, Christopher. The 'Internal Morality' of European Data Protection Law. *SSRN Scholarly Paper* [online]. ID 1443797. Rochester, NY: Social Science Research Network. 2008 [cit. 28. 6. 2019].

785 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3; COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4; MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*. 2003, roč. 25, č. 4.

způsob dosažení tohoto cíle zvolily samy. Díky tomu mohou povinné subjekty přesněji přizpůsobit konkrétní postupy při plnění svých úkolů a tím dosáhnout efektivního využití své snahy a prostředků v závislosti na povaze konkrétní situace, kterou právě potřebují vyřešit. Velká výhoda performativní regulace spočívá rovněž v tom, že není nikterak navázaná na aplikaci konkrétní technologie, ale naopak dává regulovaným subjektům možnost, aby při snaze o dosažení zákonem předepsaného cíle přicházeli s novými inovativními technickými řešeními, které mohou do budoucna zvýšit jejich efektivitu. Nevýhodou performativní regulace jsou pak vyšší nároky na její efektivní aplikaci a vymáhání.[786] I přes své nevýhody je však tato regulatorní metoda vhodným nástrojem k překonání výše identifikovaných problémů.

III) Obsahuje Obecné nařízení takovou právní úpravu, která umožňuje překonat problémy identifikované v případě směrnice 95/46/ES, a pokud ano, jak funguje jejich regulatorní metoda?

Metoda performativní regulace je provedena do textu předpisu skrze zásadu *accountability* správce osobních údajů, dle níž je správce údajů odpovědný (ve smyslu *accountable*) za zpracování které provádí, musí mu přizpůsobit způsob provedení svých povinností a následně musí být schopen prokázat, že zpracování probíhá v souladu s požadavky Obecného nařízení. Zásada *accountability* je propojena s přístupem postaveném na riziku, dle kterého má správce hodnotit rizikovost chystaného a probíhajícího zpracování z hlediska rizik, která představuje pro základní práva a svobody subjektů údajů a dalších fyzických osob. Riziko pro práva v základu nabývá dvou hodnot: zásah do práva a svobod hrozí a zásah nehrozí.[787] V případě ohrožení práv se však jeho intenzita může velice lišit. Vzhledem k tomu i přes tuto základní dualitu můžeme o riziku pro práva uvažovat v tradičních pojmech hodnocení rizik, tedy nízké, střední a vysoké riziko. Je však nezbytné zdůraznit, že hodnocení rizika pro práva bude vždy nutně kvalitativní.

Hodnocením rizika se pak nemyslí jen vypracování DPIA. Naopak v souladu s přístupem postaveném na riziku je nezbytné, aby správce údajů prováděl

786 Srovnej COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 547.

787 Viz BÖRÖCZ, István. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*, 2016, roč. 2, č. 4.

hodnocení rizikovosti zpracování vždy, byť by mělo být zcela minimalistické. Konstrukce performativní regulace v nové právní úpravě spočívá na fungující synergii těchto dvou prvků. Právě ta totiž vytváří klíč ke granularitě a škálovatelnosti povinností přítomných v Obecném nařízení. Čím vyšší je riziko zpracování, tím více povinností vedoucích k jeho omezení a tím pečlivěji (s vyššími náklady) je správce údajů musí plnit. Naopak, čím je zpracování méně rizikové pro práva a svobody subjektů údajů a dalších fyzických osob, tím méně povinností a s menším úsilím musí správce postupovat.[788] Jediné povinnosti správce přítomné v Obecném nařízení, které jsou vyňaty z aplikace přístupu založeného na riziku, jsou povinnosti odpovídající právům subjektů údajů uvedeným v Kapitole III Obecného nařízení. Správce údajů je, s výhradou velice úzké výjimky v podobě ustanovení čl. 12 odst. 5 a čl. 14 odst. 5,[789] nemůže o své vůli zcela vyloučit nebo omezit.

Na tuto dílčí výzkumnou otázku je tak třeba odpovědět tak, že nová právní úprava zavedením principů performativní regulace umožňuje překonat problémy formulované v kontextu právní úpravy bývalé.

IV) Jakou roli ve výše uvedeném hraje aspekt plynoucího času?

K osobním údajům není možné přistupovat jako ke statické quasi majetkové kategorii, ale je nutné je vnímat též v kontextu plynutí času.[790] Tento aspekt se projevuje v silné roli, kterou mají subjektivní pozitivní práva subjektu údajů, která Obecné nařízení zakládá, protože umožňují subjektu údajů kontrolu a vliv na zpracování osobních údajů v průběhu jeho celého životního cyklu.

Performativní regulace se jeví jako vhodný prostředek k překonání problémů, které před právní úpravu ochrany osobních údajů staví časový a technologický vývoj, protože dává prostředky pro dlouhodobou udržitelnost právní úpravy Obecného nařízení ve střetu s novými technologiemi,

788 Shodně QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3.

789 Srovnej MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12.

790 Viz POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014 [cit. 30. 6. 2020].

a to právě díky flexibilitě, kterou poskytuje povinným subjektům.[791] Na druhou stranu, v kontextu konkrétního zpracování performativní regulace postavená na zásadě *accountability* a přístupu postaveném na riziku nepřináší žádnou zásadní pozitivní změnu, která by umožnila lépe překonávat výzvy, které na zpracování údajů jako na proces klade plynoucí čas v podobě měnící se kvality a hodnoty osobních údajů, nebo možnosti jejich následného zpracování.

Tato publikace se soustředila na analýzu metody regulace použité v právní úpravě ochrany osobních údajů a ukázala, že regulatorní metoda performativních pravidel je vhodným nástrojem pro regulaci ochrany osobních údajů v moderní informační společnosti, protože dokáže dostatečně flexibilně reagovat na výzvy, které vývoj v čase, nové technologie a jejich aplikace přináší. Přesto i tento způsob právní úpravy přináší zásadní výzvy. Ty byly identifikovány v šesté kapitole této publikace a spočívají vysokých nárocích, které performativní regulace klade na příjemce právních norem. To platí pro dozorové úřady a soudy, které musí být schopny řádně zkontrolovat, že správci údajů správně nastavili a provádějí své zpracování vzhledem k podmínkám a rizikům v jejichž kontextu probíhá. Platí to však rovněž i pro správce údajů, po nichž je požadována expertní znalost, bez níž nemohou naplno rozvinout potenciál, který jim performativní regulace nabízí.

Tato publikace byla zaměřená na analýzu obecných systematických problémů právní úpravy ochrany osobních údajů. To je současně její předností a limitací. Poskytuje popis základního rámu, na kterém právní úprava ochrany osobních údajů spočívá. To znamená, že poznatky uvedené v této publikaci se vztahují ke každému zpracování osobních údajů, ledaže by bylo upraveno zvláštní právní úpravou. Systém právní úpravy ochrany osobních údajů je v Obecném nařízení postaven tak, že každé probíhající zpracování je nezbytně podřízené zásadě *accountability* správce a nezbytnosti hodnotit rizika, která představuje. Stejně tak je pro správné fungování tohoto systému zcela zásadní, aby tento fakt byl respektován dozorovými úřady a soudy při autoritativní aplikaci právních norem Obecného nařízení. Pokud by se tak

791 Viz COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 711.

nestalo, bude Obecné nařízení z hlediska fungování regulace na úrovni směrnice 95/46/ES, jen s vyšší možností pokut. Všechny identifikované problémy, které má možnost performativní regulace vyřešit, by však zůstaly přítomné.

Je zcela zásadní, aby se co nejdříve nový způsob regulace zažil do podvědomí adresátů norem. Krom efektivní aplikace Obecného nařízení totiž tento proces přinese zásadní výhodu v podobě lepšího přijetí pravidel ochrany osobních údajů širší veřejností. Je velký rozdíl v přístupu k právní normě, když na jedné straně leží odmítání pocitově nesmyslných pravidel, která člověku někdo nařizuje,[792] a na druhé straně spočívá flexibilní nástroj, který člověku umožní provádět činnosti, jaké potřebuje. V tomto směru spatřuji velkou výzvu pro budoucí činnost dozorových úřadů i odborné veřejnosti.

Systém ochrany osobních údajů je vzhledem ke své široké a plošné aplikaci plný specifických oblastí, které vyžadují mírně odlišné přístupy a metody, byť vycházejí ze základního rámce popsaného v této publikaci. Jako příklad je možné uvést sektorové regulace nakládání s osobními údaji, jako je oblast elektronických komunikací, nebo další předpisy obsahující zvláštní právní úpravu, která má vůči Obecnému nařízení aplikační přednost. Takovým příkladem je tzv. policejní směrnice č. 2016/680 a z ní vycházející národní právní úprava. Jejich detailní analýza dalece přesahuje možnosti a cíle této publikace. Předkládaná publikace má však za cíl posloužit jako základ pro příští výzkumnou činnost, která se zaměří právě na specifické případy aplikace ochrany osobních údajů v konkrétních kontextech a prostředích, na jejich přesahy, vzájemné souhry a rozdíly.

792 Zde je možné poukázat na to, jak se Obecné nařízení stalo oblíbeným hromosvodem některých členů české politické reprezentace, skrz který formulují svůj odpor k Evropské unii jako instituci.

SUMMARY – MODERN REGULATORY METHODS OF PERSONAL DATA PROTECTION

Monograph Modern regulatory methods of personal data protection deals with general issues of personal data protection legal framework and, in general, the regulatory system that guarantees the fundamental right to personal data protection. In this publication, the processing of personal data is understood as a dynamic process taking place over time, which the legal regulation must be able to address adequately. The second chapter presents the basic premises on which the system of personal data protection is based, and which must always be considered when interpreting and applying the provisions of legal regulations governing this legal area. As a first premise, the substantive and functional autonomy of the right to personal data protection was formulated as a fundamental right, which has its own objectives, regulatory methods and means independent of other fundamental rights, in particular the right to privacy. The second premise necessary for the proper interpretation of personal data protection provisions is a pragmatic premise of the appropriateness and necessity of personal data processing in modern society. Therefore, the personal data protection legal framework ensures an environment in which data processing takes place. It allows it and sets its limits. This fact also creates one of the two purposes of personal data protection legislation. The third premise lies in the second purpose of the personal data protection law, which is to protect the rights and freedoms of data subjects (and the public interest in such protection) against interference that could arise from the illegal (unfair) processing of personal data. This premise implies an essential role for the subjective positively formulated rights of data subjects, which are contained in the analysed legal regulation. A crucial partial finding, which emerged from the second chapter, is that the rights of data subjects play an important role in ensuring control of the data controller throughout the ongoing processing process and therefore it is not possible to waive them or to exclude their exercise. Personal data and their processing must thus be understood not as static quasi-property, but as a dynamic process taking place over time. Finally,

the fourth premise, confirmed by the decision-making practice of the CJEU, is a necessity of a precautionary approach to the protection of personal data. This fact is practically reflected in the interpretation of the regulations governing the protection of personal data in such a way that the defining provisions establishing the scope of these regulations must generally be interpreted extensively and the provisions establishing exceptions must be interpreted as restrictively as possible.

The third chapter of this publication showed that the former legislation (Directive 95/46/EC and the Act No. 101/2000 Sb.) failed to respond flexibly enough to the challenges posed by technological developments over time. This outcome occurred even though the regulation was built in accordance with the principle of technological neutrality. It did not contain a way of ensuring the necessary granularity and scalability of the controller's responsibilities in order to be able to adapt the data processing process to the specific situation in which the processing took place.

In the borderline cases of data processing, when we were applying the previously identified premises, it was necessary to draw absurd conclusions, which consisted in the necessity to fulfil duties of the controller in an entirely disproportionate way to the given situation. An example is the use of IP addresses in the context of cybersecurity, where, according to the former legislation, the data controller had, for example, a practically unfeasible obligation to inform data subjects about the ongoing processing. Following the decision of the CJEU in the *Google Spain* case (C-131/12), internet search engine operators found themselves in the position of the data controllers, indexing and further processing for the purpose of providing search services personal data present on the sites and in the documents of third parties. However, it was difficult for them to fulfil their controller duties, such as the obligation to provide information. Besides, this processing of personal data was illegal in the absence of a legal title that would justify the processing of sensitive personal data, which, however, were undoubtedly also part of the indexed pages. The third example showed that the consistent application of the premises and principles of the personal data protection system must conclude that the definition of personal data processing can also include a simple hypertext reference

to the document that contains the personal data. Again, the fulfilment of all obligations required by Directive 95/46/EC and Act No. 101/2000 Sb., was in such a case disproportionate or even impossible. As a final example, the book pointed to the problem of anonymised data, where was heavily present a risk of re-identification of data subjects over time due to improving technical possibilities. The past regulation could not sufficiently tackle this challenge in a way which would protect the data subjects and, at the same time, which would impose duties on the controller proportionately. This example well demonstrates the static nature of the past understanding of personal data.

Given that the previous legislation did not contain options to deal satisfactorily with these shortcomings, two ways emerged that tried to solve the problem, so to speak, „outside the system" of the personal data protection legal framework. The fourth chapter of this book shows that the first way was to narrow the interpretation of the definition provisions so that problematic cases would not be affected by the legal regulation of personal data protection at all. The second way was an ad hoc decision by the supervisory authorities not to enforce cases that were so problematic. However, it is necessary to reject both indicated paths as possible solutions to the problem of insufficient granularity and scalability of the controller's obligations. The first mentioned path cannot be applied due to the preventive approach to personal data protection and the established case law of the CJEU. The second must be ruled out for its fundamental shortcomings in the form of a breach of the obligations arising from the principles of legality and legal certainty.

The answer to these problems had to be such regulation of personal data protection, which would meet the conditions of wide and preventive application and at the same time which would allow sufficient internal flexibility in the form of granularity and scalability of the controller's duties. Given the direct applicability of the General Regulation to a wide range of different types of controllers and the processing of personal data, the European legislator was faced with the challenge of ensuring such flexibility.

In the fifth chapter, the key part of the book, the author provides an analysis of performance-based regulation; a modern regulatory method chosen

by European legislator as the foundation regulatory framework in the General Data Protection Regulation (no. 2016/679). Its essence lies in the fact that it only determines the goal of regulated entities (which can be both very specific and very abstract), which they are to achieve, but it no longer specifies how this is to happen. The performance-based regulation in the GDPR is based on combining the controller accountability principle with a risk-based approach. That allows the GDPR to provide a sufficiently flexible framework of duties, allowing for their granularity and scalability. GDPR sets the objective for data controllers to carry out processing in such a way that its specific implementation corresponds to the risks that such processing poses to the rights and freedoms of data subjects. The most fundamental change brought about by GDPR was, therefore, the shift of the basic regulatory method from a rights-based approach to a risk-based approach. The greater the risk, the more the obligations arising from GDPR the controller has (granularity) and the more carefully he has to fulfil them (scalability). Conversely, in the case of lower risk, some obligations may not be fulfilled by the controller at all. For the obligations that remain for him, despite the lower risk, then the lower the risk, the less effort he has to make to fulfil them sufficiently. The risk assessment of the data processing acts as a filter, which is applied in practically all cases of the data controller's obligations arising from the General Regulation.

The level of risk and its assessment is also an aspect, which must be taken into account by the supervisory authorities during the enforcement of obligations and the imposition of sanctions arising from GDPR. The only area not covered by the risk assessment (subject to the minor exception in Article 12 (5) and Article 14 (5) of GDPR) are the subjective rights of data subjects formulated in Chapter III of GDPR.

The principles of performance-based regulation enshrined in GDPR in the form of a broad principle of accountability of the controller in combination with a risk-based approach create sufficient space for the controller of personal data to adapt processing conditions to the needs of a specific data processing operation. At the same time, since the rights of data subjects form an almost insurmountable limit for low-end modifications of the controller's obligations even for the least risky data processing operations,

the protection of the data subject is normatively ensured throughout the ongoing processing. Finally, performance-based regulation, in conjunction with the principles of technological neutrality, presupposes that the General Regulation will be much more resistant to time and technological change than Directive 95/46/EC. It provides the means for the long-term sustainability of GDPR in conflict with new technologies, thanks to the flexibility it provides to data controllers.

In conclusion, the book discusses the advantages of this regulatory method and comments on the challenges and obstacles that performance-based regulation poses for the interpretation and application of the GDPR. This book focuses on the analysis of the regulatory method used in personal data protection legislation. It shows that the regulatory method of performance-based rules is a suitable tool for regulating personal data protection in a modern information society because it can respond flexibly enough to the challenges of development of new technologies and their application. Nevertheless, even this type of regulation brings fundamental challenges. These have been identified in the sixth chapter of this publication. They are based on the high demands that performative regulation places on the recipients of legal norms. This fact applies to supervisory authorities and courts, which must be able to properly check that data controllers have set up and processed their data correctly in light of the conditions and risks in which it takes place. However, this also applies to data controllers, who are required to have expert knowledge, without which they cannot fully develop the potential that performative regulation offers them. The system of legal regulation of personal data protection is built-in GDPR in such a way that any ongoing processing is necessarily subject to the principle of accountability of the controller and the need to assess the risks it poses. It is also essential for the proper functioning of this system that supervisory authorities and courts respect this fact during the authoritative application of the legal norms of GDPR. If this were not the case, GDPR would be concerning the functioning of regulation at the level of Directive 95/46/EC, only with a higher possibility of fines. However, all the identified problems that the possibility of performative regulation has to solve would remain present.

The new method of regulation must be accepted by regulated subjects as soon as possible. In addition to the practical application of GDPR, this process will bring a significant advantage in the form of better acceptance of personal data protection rules by the general public. There is a big difference in the approach to the legal regulation when on the one hand there is the rejection of emotionally nonsensical rules that someone commands, and on the other hand, there is a flexible tool that allows a person to perform the activities he needs. In this regard, the book sees a significant challenge for the future activities of supervisory authorities and the professional public.

LITERATURA A DALŠÍ POUŽITÉ ZDROJE

Odborné monografie a články

ACQUISTI, Alessandro, Leslie JOHN a George LOEWENSTEIN. What Is Privacy Worth? *Journal of Legal Studies*, 2013, roč. 42, č. 2, s. 249–274. ISSN 0047-2530.

ADRIAANS, Pieter. Information. In: ZALTA, Edward N. (ed.). *The Stanford Encyclopedia of Philosophy* [online]. Stanford: Metaphysics Research Lab, Stanford University, 2013 [cit. 30. 6. 2020]. Dostupné z: https://plato.stanford.edu/archives/fall2013/entries/information/

ALEXY, Robert a Julian RIVERS. *A Theory of Constitutional Rights*. Oxford, New York: Oxford University Press, 2009, 516 s. ISBN 978-0-19-958423-9.

ALSENOY, Brendan Van. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2016, roč. 7, č. 3, s. 271–288. ISSN 2190-3387.

ALSENOY, Brendan Van. *Data protection law in the EU: roles, responsibilities and liability*. Cambridge: Intersentia, 2019, 694 s. ISBN 978-1-78068-828-2.

ALSENOY, Brendan Van et al. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?* [online]. Rochester, NY: Social Science Research Network, 2013, 74 s. [cit. 30. 6. 2020]. Dostupné z: http://papers.ssrn.com/abstract=2321494

AMBROSE, Meg Leta. Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. *Telecommunications Policy* [online]. 2014, roč. 38, č. 8–9, Special issue on Moving Forward with Future Technologies: Opening a Platform for AllSpecial issue on Papers from the 41st Research Conference on Communication, Information and Internet Policy (TPRC 2013), s. 800–811. ISSN 0308-5961. DOI: 10.1016/j.telpol.2014.05.002

AUSLOOS, Jef. The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review* [online]. 2012, roč. 28, č. 2, s. 143–152. ISSN 0267-3649. DOI: 10.1016/j.clsr.2012.01.006

AUSLOOS, Jef. *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?* Disertační práce. Leuven: KU Leuven, Faculty of Law, 2018.

AUWERMEULEN, Barbara Van der. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law & Security Review* [online]. 2017, roč. 33, č. 1, s. 57–72. ISSN 0267-3649. DOI: 10.1016/j.clsr.2016.11.012

BALBONI, Paolo a Milda MACENAITE. Privacy by design and anonymisation techniques in action: Case study of Ma3tch technology. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 4, s. 330–340. ISSN 0267-3649. DOI: 10.1016/j.clsr.2013.05.005

BALDWIN, Robert, Martin CAVE a Martin LODGE (eds.). *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2012, 668 s. ISBN 978-0-19-956021-9.

BARTOLINI, Cesare a Lawrence SIRY. The right to be forgotten in the light of the consent of the data subject. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 218–237. ISSN 0267-3649. DOI: 10.1016/j.clsr.2016.01.005

BENNETT MOSES, Lyria. Recurring Dilemmas: The Law's Race to Keep up with Technological Change. *University of Illinois Journal of Law, Technology & Policy*, 2007, roč. 2007, č. 2, s. 239–286. ISSN 1532-3242.

BERGKAMP, Lucas. EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *Computer Law & Security Review* [online]. 2002, roč. 18, č. 1, s. 31–47. ISSN 0267-3649. DOI: 10.1016/S0267-3649(02)00106-1

BERLIN, Isaiah, Henry HARDY a Ian HARRIS. *Liberty: incorporating four essays on liberty*. Oxford: Oxford University Press, 2002, 382 s. ISBN 978-0-19-924988-6.

BERNAL, Paul. Collaborative consent: Harnessing the strengths of the Internet for consent in the online environment. *International Review of Law, Computers & Technology* [online]. 2010, roč. 24, č. 3, s. 287–297. ISSN 1360-0869. DOI: 10.1080/13600869.2010.522335

BERNAL, Paul. *Internet privacy rights : rights to protect autonomy*. Cambridge: Cambridge, England, New York, [New York]: Cambridge University Press, 2014, 311 s., Cambridge Intellectual Property and Information Law. ISBN 978-1-139-86317-9.

BERTOT, John Carlo et al. Big data, open government and e-government: Issues, policies and recommendations. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2014, roč. 19, č. 1/2, s. 5–16. ISSN 1570-1255. DOI: 10.3233/IP-140328

BEYLEVELD, Deryck. *Consent in the Law*. Oxford: Hart Publishing, 2007, 388 s. ISBN 978-1-84113-679-0.

BORGESIUS, Frederik Zuiderveen. Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics? *SSRN Scholarly Paper* [online]. ID 2300969. Rochester, NY: Social Science Research Network 2013 [cit. 30. 6. 2020]. Dostupné z: http://papers.ssrn.com/abstract=2300969

BORGESIUS, Frederik Zuiderveen. Informed consent: We can do better to defend privacy. *IEEE Security and Privacy* [online]. 2015, roč. 13, č. 2, s. 103–107. ISSN 1540-7993. DOI: 10.1109/MSP.2015.34

BORGESIUS, Frederik Zuiderveen. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law*, 2015, roč. 5, č. 3, s. 163. ISSN 2044-3994.

BÖRÖCZ, István. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 467–480. ISSN 2364-2831.

BUCKLAND, Michael Keeble. Information as a Thing. *Journal of the American Society for Information Science and Technology*, 1991, roč. 42, č. 5, s. 351–360. ISSN 2330-1643.

BYGRAVE, Lee A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, 1998, roč. 6, č. 3, s. 247–284. ISSN 1464-3693.

BYGRAVE, Lee A. The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal*, 2001, roč. 24, č. 1, s. 277–283. ISSN 0313-0096.

BYGRAVE, Lee A. *Data privacy law: an international perspective*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2014, 233 s. ISBN 978-0-19-967555-5.

BYGRAVE, Lee A. Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxford Journal of Legal Studies*, 2015, roč. 35, č. 1, s. 91–120. ISSN 0143-6503.

CAMENISCH, Jan. Information privacy?! *Computer Networks* [online]. 2012, roč. 56, č. 18, s. 3834–3848. ISSN 1389-1286. DOI: 10.1016/j.comnet.2012.10.012

CANNATACI, Joseph A. a Jeanne Pia MIFSUD-BONNICI. Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information & Communications Technology Law* [online]. 2005, roč. 14, č. 1, s. 5–15. ISSN 1360-0834. DOI: 10.1080/1360083042000325274

CITRON, Danielle Keats a Frank PASQUALE. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, 2014, roč. 89, č. 1, s. 1–33. ISSN 0043-0617.

CLAES, Erik, Antony DUFF a Serge GUTWIRTH (eds.). *Privacy and the criminal law*. Antwerp: Intersentia, 2006, 199 s. ISBN 978-90-5095-545-4.

CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site* [online]. 2016 [cit. 30. 6. 2020]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html

COGLIANESE, Cary. Performance-Based Regulation: Concepts and Challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative law and regulation: understanding the global regulatory process*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, s. 403–429, Research handbooks in comparative law. ISBN 978-1-78254-560-6.

COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 525–564. ISSN 0363-602X.

COGLIANESE, Cary a David LAZER. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals Of General Interest. *Law & Society Review*, 2003, roč. 37, č. 4, s. 691–730. ISSN 1540-5893.

COGLIANESE, Cary a Jennifer NASH (eds.). *Leveraging the private sector: management-based strategies for improving environmental performance*. Washington, DC: RFF PRess, 2006, 269 s. ISBN 978-1-891853-95-1.

COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 705–730. ISSN 0001-8368.

COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Regulation. *Administrative Law Review*, 2004, roč. 55, č. 4, s. 705–729.

COLLINGWOOD, Lisa. Privacy, anonymity and liability: Will anonymous communicators have the last laugh? *Computer Law & Security Review* [online]. 2012, roč. 28, č. 3, s. 328–334. ISSN 0267-3649. DOI: 10.1016/j.clsr.2012.03.002

CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, 250 s., The collected courses of the Academy of European Law. ISBN 978-0-19-880721-6.

CUMBLEY, Richard a Peter CHURCH. Is "Big Data" creepy? *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 601–609. ISSN 0267-3649. DOI: 10.1016/j.clsr.2013.07.007

CVIK, Daniela Eva, Radka MacGREGOR PELIKÁNOVÁ a Michal MALÝ. Selected Issues from the Dark Side of the General Data Protection Regulation. *Review of Economic Perspectives* [online]. 2018, roč. 18, č. 4, s. 387–407. ISSN 1804-1663. DOI: 10.2478/revecp-2018-0020

ČERMÁK, Vladimír. *Otázka demokracie. Svazek 1*. 2. vyd. Praha: Centrum pro studium demokracie a kultury, 2017, 827 s. ISBN 978-80-7325-430-8.

DARIES, Jon P. et al. Privacy, Anonymity, and Big Data in the Social Sciences. *Communications of the ACM* [online]. 2014, roč. 57, č. 9, s. 56–63. ISSN 0001-0782. DOI: 10.1145/2643132

DIAS, R. W. M. The Value of a Value-Study of Law. *The Modern Law Review*, 1965, roč. 28, č. 4, s. 397. ISSN 0026-7961.

DIJK, Niels van, Raphaël GELLERT a Kjetil ROMMETVEIT. A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 286–306. ISSN 0267-3649. DOI: 10.1016/j.clsr.2015.12.017

ERDOS, David. From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection. *Common Market Law Review*, 2015, roč. 52, č. 1, s. 119–153. ISSN 0165-0750.

ESKENS, Sarah. A right to reset your user profile and more: GDPR-rights for personalized news consumers. *International Data Privacy Law* [online]. 2019, s. 1–20. DOI: 10.1093/idpl/ipz007

EVERETT, Miriam a Lucy McALISTER. Court of Appeal Confirms First Successful UK Class Action for Data Breach. *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, 2018, roč. 2, č. 11, s. 8–10.

FERRETTI, Federico. Data Protections and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights. *Common Market Law Review*, 2014, roč. 51, č. 3, s. 843–868. ISSN 0165-0750.

FIALOVÁ, Eva. *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges, 2016, 230 s. ISBN 978-80-7502-150-2.

FIALOVÁ, Eva. Právo na přístup k internetu. *Právník*, 2018, roč. 157, č. 7, s. 545–557. ISSN 0231-6625.

FLORIDI, Luciano. *Information: a very short introduction*. Oxford; New York: Oxford University Press, 2010, 130 s., Very short introductions, 225. ISBN 978-0-19-955137-8.

FOLIENTE, Greg C. Developments in performance-based building codes and standards. *Forest Products Journal,* 2000, roč. 50, č. 7–8, s. 12–21. ISSN 0015-7473.

FULLER, Lon L. *The morality of law*. Rev. vyd. New Haven: Yale University Press, 1978, 262 s. ISBN 978-0-300-01070-1.

GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law* [online]. 2015, roč. 5, č. 1, s. 3–19. ISSN 2044-3994. DOI: 10.1093/idpl/ipu035

GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review*, 2016, roč. 2, č. 4, s. 481–492. ISSN 2364-2831.

GELLERT, Raphaël. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. *European Data Protection Law Review*, 2017, roč. 3, č. 2, s. 212–217. ISSN 2364-2831.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 279–288. ISSN 0267-3649. DOI: 10.1016/j.clsr.2017.12.003

GELLERT, Raphaël a Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 522–530. ISSN 0267-3649. DOI: 10.1016/j.clsr.2013.07.005

GHEZZI, Alessia, Ângela Guimarães PEREIRA a Lucia VESNIĆ-ALUJEVIĆ (eds.). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. Houndmills: Palgrave Macmillan UK, 2014, 143 s. ISBN 978-1-349-49145-2.

GOFFMAN, Erving. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. 1961, 386 s.

GONÇALVES, Maria Eduarda. The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research* [online]. 2019, s. 1–14. ISSN 1366-9877. DOI: 10.1080/13669877.2018.1517381

GONZÁLEZ FUSTER, Gloria a Raphaël GELLERT. The fundamental right of data protection in the European union: In search of an uncharted right. *International Review of Law, Computers and Technology* [online]. 2012, roč. 26, č. 1, s. 73–82. ISSN 1360-0869. DOI: 10.1080/13600869.2012.646798

GONZÁLEZ-FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Cham; New York: Springer, 2014, 274 s. ISBN 978-3-319-05022-5.

GRATTON, Eloise. If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm Is the Key: A Proposed Method for Determining What Counts as Personal Information. *Albany Law Journal of Science & Technology*, 2014, roč. 24, č. 1, s. 105–210. ISSN 1059-4280.

GROSSKLAGS, Jens a Alessandro ACQUISTI. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In: *6th Annual Workshop on the Economics of Information Security, WEIS 2007, The Heinz School and CyLab at Carnegie Mellon University, Pittsburgh, PA, USA, June 7-8, 2007* [online]. 2007 [cit. 30. 6. 2020]. Dostupné z: http://weis2007.econinfosec.org/papers/66.pdf

GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, 292 s. ISBN 978-1-137-03222-5.

GULIJK, Stephanie van a Joris HULSTJIN. Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach. *European Review of Private Law*, 2018, roč. 26, č. 5, s. 635–660. ISSN 0928-9801.

GUTWIRTH, Serge. *Privacy and the information age*. Lanham, Md: Rowman & Littlefield Publishers, 2002, 152 s. ISBN 978-0-7425-1745-5.

GUTWIRTH, Serge. *Short statement about the role of consent in the European data protection directive* [online]. Brusel: Bepress 2012 [cit. 30. 6. 2020]. Dostupné z: https://works.bepress.com/serge_gutwirth/80/

GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, 342 s. ISBN 978-1-4020-9497-2.

GUTWIRTH, Serge et al. (eds.). *European data protection: in good health?* New York: Springer, 2012. ISBN 978-94-007-2902-5.

GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, 440 s. ISBN 978-94-007-5184-2.

GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, 369 s. ISBN 978-94-007-7540-4.

GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European data protection law*. Dordrecht: Springer, 2015, 406 s. ISBN 978-94-017-9385-8.

GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, 476 s. ISBN 978-94-017-7376-8.

GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Computers, privacy and data protection: an element of choice*. Dordrecht; New York: Springer, 2011, 457 s. ISBN 978-94-007-0640-8.

GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Data protection in a profiled world*. Dordrecht; New York: Springer, 2010, 334 s. ISBN 978-90-481-8864-2.

HAGENBACH, Jeanne a Frédéric KOESSLER. The Streisand effect: Signaling and partial sophistication. *Journal of Economic Behavior and Organization* [online]. 2017, roč. 143, s. 1–8. ISSN 0167-2681. DOI: 10.1016/j.jebo.2017.09.001

HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie*, 2013, roč. 4, č. 8, s. 64–94. ISSN 1805-2797.

HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, roč. 6, č. 12, s. 21–42. ISSN 1804-5383.

HARAŠTA, Jakub a Matěj MYŠKA. Budoucnost data retention. *Trestněprávní revue*, 2015, roč. 14, č. 10, s. 238–241. ISSN 1213-5313.

HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti*. Disertační práce Brno: Masarykova univerzita, Právnická fakulta, 2018, 162 s. Dostupné z: https://is.muni.cz/th/agnuc/ [cit. 30. 6. 2020].

HENDRYCH, Dušan a kol. *Správní právo: obecná část*. 7. vyd. Praha: C. H. Beck, 2009, 838 s. ISBN 978-80-7400-049-2.

HERMSTRÜWER, Yoan a Stephan DICKERT. Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten. *SSRN Scholarly Paper* [online]. ID 2311201. Rochester, NY: Social Science Research Network 2013 [cit. 30. 6. 2020]. Dostupné z: https://papers.ssrn.com/abstract=2311201

HERT, Paul de. The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents Editorial. *Utrecht Journal of International and European Law*, 2015, roč. 31, č. 80, s. 1–4.

HERT, Paul de et al. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 193–203. ISSN 0267-3649. DOI: 10.1016/j.clsr.2017.10.003

HERT, Paul de a Vagelis PAPAKONSTANTINOU. The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. *Computer Law & Security Review* [online]. 2014, roč. 30, č. 6, s. 633–642. ISSN 0267-3649. DOI: 10.1016/j.clsr.2014.09.002

HERT, Paul de a Vagelis PAPAKONSTANTINOU. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 179–194. ISSN 0267-3649. DOI: 10.1016/j.clsr.2016.02.006

HILDEBRANDT, Mireille a Bibi van den BERG (eds.). *Information, freedom and property: the philosophy of law meets the philosophy of technology*. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2016, 202 s. ISBN 978-1-138-66913-0.

HILDEBRANDT, Mireille a Laura TIELEMANS. Data protection by design and technology neutral law. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 509–521. ISSN 0267-3649. DOI: 10.1016/j.clsr.2013.07.004

HLOUCH, Lukáš. *Teorie a realita právní interpretace*. Plzeň: Aleš Čeněk, 2011, 348 s. ISBN 978-80-7380-303-2.

HODGES, Christopher. Delivering Data Protection: Trust and Ethical Culture Discussion. *European Data Protection Law Review*, 2018, roč. 4, č. 1, s. 65–79. ISSN 0928-9801.

HOECKE, Mark van (ed.). *Methodologies of legal research: which kind of method for what kind of discipline?* Oxford, Portland: Hart, 2011, 294 s., European Academy of Legal Theory monograph series. ISBN 978-1-84946-170-2.

HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Aleš Čeněk, 2012, 421 s. ISBN 978-80-7380-366-7.

HOOD, Christopher et al. Explaining risk regulation regimes: exploring the "minimal feasible response" hypothesis. *Health, Risk & Society* [online]. 1999, roč. 1, č. 2, s. 151–166. ISSN 1369-8575. DOI: 10.1080/13698579908407015

HOOD, Christopher, Henry ROTHSTEIN a Robert BALDWIN. *The government of risk: understanding risk regulation regimes*. Oxford; New York: Oxford University Press, 2001, 217 s. ISBN 978-0-19-924363-1.

HURYCHOVÁ, Klára a Michal SÝKORA. *Compliance programy (nejen) v České republice*. Praha: Wolters Kluwer, 2018, 287 s. ISBN 978-80-7552-667-0.

CHELLAPPA, Ramnath K. a Raymond G. SIN. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management* [online]. 2005, roč. 6, č. 2–3, s. 181–202. ISSN 1385-951X. DOI: 10.1007/s10799-005-5879-y

CHINANDER, Karen R., Paul R. KLEINDORFER a Howard C. KUNREUTHER. Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks. *Risk Analysis* [online]. 1998, roč. 18, č. 2, s. 135–143. ISSN 1539-6924. DOI: 10.1111/j.1539-6924.1998.tb00925.x

JANEČEK, Václav. Ownership of personal data in the Internet of Things. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 5, s. 1039–1052. ISSN 0267-3649. DOI: 10.1016/j.clsr.2018.04.007

JANSEN, Sue Curry a Brian MARTIN. The Streisand effect and censorship backfire. *International journal of communication (Online)*, 2015, roč. 9, č. 9, s. 656–671.

JASMONTAITE, Lina et al. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. *European Data Protection Law Review (EDPL)*, 2018, roč. 4, č. 2, s. 168–189. ISSN 2364-2831.

JHERING, Rudolf von. *Law as a means to an end*. Překlad Isaac Husik. Boston: The Boston book company, 1913, 564 s.

JONES, Meg Leta. *Ctrl + Z: The Right to Be Forgotten*. New York, London: NYU Press, 2016, 256 s. ISBN 978-1-4798-8170-3.

KAMIRAN, Faisal, Indré ŽLIOBAITE a Toon CALDERS. Quantifying explainable discrimination and removing illegal discrimination in automated decision making. *Knowledge and Information Systems* [online]. 2016, roč. 35, č. 3, s. 613–644. ISSN 0219-1377. DOI: 10.1007/s10115-012-0584-8

KINDL, Milan. K „novátorským" důsledkům zákona o ochraně osobních údajů. *Právní rozhledy*, 2001, roč. 9, č. 2, s. 75–77. ISSN 1210-6410.

KLITOU, Demetrius. *Privacy-invading technologies and privacy by design*. New York, NY: Springer Berlin Heidelberg, 2014, 338 s. ISBN 978-94-6265-025-1.

KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C. H. Beck, 2012, 1687 s. ISBN 978-80-7400-365-3.

KNAPP, Viktor. *Teorie práva*. 1. vyd. Praha: C. H. Beck, 1995, 247 s., Právnické učebnice. ISBN 978-80-7179-028-1.

KOOPS, Bert-Jaap et al. A Typology of Privacy. *SSRN Scholarly Paper* [online]. ID 2754043. Rochester, NY: Social Science Research Network 2016 [cit. 30. 6. 2020]. Dostupné z: http://papers.ssrn.com/abstract=2754043

KOPPELL, Jonathan G. S. Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder". *Public Administration Review* [online]. 2005, roč. 65, č. 1, s. 94–108. ISSN 0033-3352. DOI: 10.1111/j.1540-6210.2005.00434.x

KORBEL, František. *Svobodný přístup k informacím podle zákona č. 106/1999 Sb. – vybrané problémy*. Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, 2005. Dostupné z: https://is.muni.cz/auth/th/9741/pravf_d/ [cit. 30. 6. 2020].

KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law* [online]. Dordrecht: Springer Netherlands, 2015, 20, s. 171–201 [cit. 30. 6. 2020]. ISBN 978-94-017-9384-1. DOI: 10.1007/978-94-017-9385-8_7

KOSAŘ, David a Jan PETROV. Jak vybrat „případy" do případové studie a pracovat s nimi v právu: poznatky z výzkumu na pomezí práva a politologie. *Jurisprudence*, 2016, roč. 25, č. 6, s. 21–30. ISSN 1802-3843.

KOSTA, Eleni. *Consent in European data protection law*. Leiden: Martinus Nijhoff Publishers, 2013, 441 s. ISBN 978-90-04-23235-8.

KOŠČÍK, Michal et al. *Výzkumná data a výzkumné databáze. Právní rámec zpracování a sdílení vědeckých poznatků*. Praha: Wolters Kluwer ČR, 2018, 180 s. ISBN 978-80-7552-952-7.

KOŠČÍK, Michal a Matěj MYŠKA. Data protection and codes of conduct in collaborative research. *International Review of Law, Computers & Technology* [online]. 2018, roč. 32, č. 1, s. 141–154. ISSN 1360-0869. DOI: 10.1080/13600869.2018.1423888

KRAUSOVÁ, Alžběta. Zásada autonomie v ochraně soukromí: možnosti a limity v rozhodování o vlastních biometrických údajích. *Právní rozhledy*, 2018, roč. 26, č. 6, s. 191–197. ISSN 1210-6410.

KRITIKOS, Katie Chamberlain. The Right to Forget, Obliterate, Erase: Defending Personal Data Privacy in the Digital Age. *Journal of Information Ethics*, 2018, roč. 27, č. 2, s. 47–65. ISSN 1061-9321.

KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Beckova edice komentované zákony. Praha: C. H. Beck, 2012, 516 s. ISBN 978-80-7179-226-0.

KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, 1624 s. ISBN 978-3-406-71932-5.

KUMPOŠT, Marek a Václav MATYÁŠ. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU*, 2009, roč. 20, č. 1, s. 13–20. ISSN 1212-0901.

KUNER, Christopher. The 'Internal Morality' of European Data Protection Law. *SSRN Scholarly Paper* [online]. ID 1443797. Rochester, NY: Social Science Research Network 2008 [cit. 28. 6. 2019]. Dostupné z: https://papers.ssrn.com/abstract=1443797

KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *BNA Bloomberg Privacy and Security Law Report*. 2012, s. 1–15.

KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford, New York: Oxford University Press, 2013, 310 s. ISBN 978-0-19-967461-9.

LAH, Frederick. Online and Locational Privacy: Are IP Addresses "Personally Identifiable Information"? *I/S: A Journal of Law and Policy for the Information Society*, 2008, roč. 4, č. 3, s. 676–703.

LAVICKÝ, Petr (ed.). *Občanský zákoník: komentář*. 1. vyd. Praha: C. H. Beck, 2014, 2379 s., Velké komentáře. ISBN 978-80-7400-529-9.

LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, 295 s., Law, Governance and Technology Series, volume 36. ISBN 978-3-319-50796-5.

LESSIG, Lawrence. *Free culture: how big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press, 2004, 345 s. ISBN 978-1-59420-006-9.

LESSIG, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006, 432 s. ISBN 978-0-465-03914-2.

LÉVY, Pierre. *Becoming virtual: reality in the Digital Age*. New York: Plenum Trade, 1998, 207 s. ISBN 978-0-306-45788-3.

LINDSAY, David. The "Right to be Forgotten" by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling. *Journal of Media Law* [online]. 2014, roč. 6, č. 2, s. 159–179. ISSN 1757-7632. DOI: 10.5235/17577632.6.2.159

LITVINOV, Aleksandr V. The Data Protection Directive as Applied to Internet Protocol (IP) Addresses: Uniting the Perspective of the European Commission with the Jurisprudence of Member States. *The George Washington international law review*, 2013, roč. 45, č. 3, s. 579–610. ISSN 1534-9977.

LOWRY, Mark Newton a Lawrence KAUFMAN. Performance-Based Regulation of Utilities. *Energy Law Journal,* 2002, č. 2, s. 399–458.

LUNDEVALL-UNGER, Patrick a Tommy TRANVIK. IP Addresses – Just a Number? *International Journal of Law and Information Technology* [online]. 2011, roč. 19, č. 1, s. 53–73. ISSN 0967-0769, 1464-3693. DOI: 10.1093/ijlit/eaq013

LYNSKEY, Orla. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly* [online]. 2014, roč. 63, č. 3, s. 569–597. ISSN 0020-5893. DOI: 10.1017/S0020589314000244

LYNSKEY, Orla. Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *Modern Law Review* [online]. 2015, roč. 78, č. 3, s. 522–534. ISSN 0026-7961. DOI: 10.1111/1468-2230.12126

LYNSKEY, Orla. *The foundations of EU data protection law*. 1. vyd. Oxford, United Kingdom: Oxford University Press, 2015, 307 s. Oxford studies in European law. ISBN 978-0-19-871823-9.

MACENAITE, Milda. The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation* [online]. 2017, roč. 8, č. 3, s. 506–540. ISSN 1867-299X, 2190-8249. DOI: 10.1017/err.2017.40

MALANÍK, Michal. Performativní povaha právní interpretace. *Jurisprudence*, 2017, roč. 26, č. 5, s. 35. ISSN 1802-3843.

MALGIERI, Gianclaudio a Bart CUSTERS. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 289–303. ISSN 0267-3649. DOI: 10.1016/j.clsr.2017.08.006

MARCUS, Daniel J. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke Law Journal*, 2018, roč. 68, č. 3, s. 556–593. ISSN 0012-7086.

MARREIROS, Helia et al. "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization* [online]. 2017, roč. 140, s. 1–17. ISSN 0167-2681. DOI: 10.1016/j.jebo.2017.03.024

MAŘÁDEK, David. Pořízení zvukového záznamu soukromou osobou a obecné možnosti jeho použití jako důkazního prostředku v civilním soudním řízení. *Právní rozhledy*, 2015, roč. 23, č. 13–14, s. 481–486. ISSN 1210-6410.

MAŠTALKA, Jiří. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*, 2010, roč. 18, č. 10, s. 369–372. ISSN 1210-6410.

MATEJKA, Ján, Alžběta KRAUSOVÁ a Vojen GÜTTLER. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 17, s. 91–129. ISSN 1805-2797. DOI: 10.5817/RPT2018-1-5

MATYSOVÁ, Monika a František NONNEMANN. Možnost odmítnout uplatnění práva subjektu údajů dle GDPR. *Právní rozhledy*, 2018, roč. 26, č. 12, s. 424–433. ISSN 1210-6410.

MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4, s. 381. ISSN 1467-9930.

MCINTYRE, Joshua J. Balancing Expectations of Online Privacy: Why Internet Protocol (ip) Addresses Should Be Protected as Personally Identifiable Information. *DePaul Law Review*, 2011, roč. 60, č. 3, s. 895–936. ISSN 0011-7188.

MÍŠEK, Jakub. Právní kýč: Argumenty v zajetí koťátek a lidských práv. In: *Právní kýč*: *Argumenty v zajetí koťátek a lidských práv*. Brno: Masarykova univerzita, 2014, s. 58–72.

MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 3–74. ISSN 1805-2797.

MÍŠEK, Jakub. Konflikt technologického vývoje a práva na příkladu autorského práva. *Právník*, 2015, roč. 154, č. 10, s. 843–855. ISSN 0231-6625.

MÍŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie*, Česká advokátní komora, 2015, roč. 2015, č. 1–2, s. 30–34. ISSN 1210-6348.

MÍŠEK, Jakub. *Právní aspekty otevřených dat*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019, 172 s. Dostupné z: https://is.muni.cz/th/sqe7a/ [cit. 30. 6. 2020].

MITRAKAS, Andreas. Assessing liability arising from information security breaches in data privacy. *International Data Privacy Law* [online]. 2011, roč. 1, č. 2, s. 129–136. ISSN 2044-3994, 2044-4001. DOI: 10.1093/idpl/ipr001

MOLEK, Pavel. *Politická práva*. 1. vyd. Praha: Wolters Kluwer, 2014, 613 s. ISBN 978-80-7478-502-3.

MORÁVEK, Jakub. Nad rozhodováním Nejvyššího správního soudu ohledně pravomocí Úřadu pro ochranu osobních údajů. *Právní rozhledy*, 2011, roč. 19, č. 9, s. 305–309. ISSN 1210-6410.

MOURBY, Miranda et al. Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 2, s. 222–233. ISSN 0267-3649. DOI: 10.1016/j.clsr.2018.01.002

MULGAN, Richard. 'Accountability': An Ever-Expanding Concept? *Public Administration* [online]. 2000, roč. 78, č. 3, s. 555–573. ISSN 1467-9299. DOI: 10.1111/1467-9299.00218

MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů*. Edice S. Brno: Masarykova univerzita, 2013, 133 s., Acta Universitatis Brunensis Iuridica, 456. ISBN 978-80-210-6462-1.

NISSENBAUM, Helen Fay. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books, 2010, 288 s. ISBN 978-0-8047-5236-7.

NONNEMANN, František. Ochrana spotřebitele a ochrana osobních údajů. *Právní rozhledy*, 2010, roč. 18, č. 22, s. 807–810. ISSN 1210-6410.

NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Správní právo*, 2011, roč. 44, č. 14, s. 520–522. ISSN 0139-6005.

NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*, 2012, roč. 20, č. 13–14, s. 505–509. ISSN 1210-6410.

NONNEMANN, František. Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google. *Právní rozhledy*, 2014, roč. 22, č. 13–14, s. 479–486. ISSN 1210-6410.

NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*, 2015, roč. 23, č. 12, s. 425–431. ISSN 1210-6410.

NONNEMANN, František. IP adresa jako osobní údaj. *Právní rozhledy*, 2017, roč. 25, č. 3, s. 88–93. ISSN 1210-6410.

NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. *Právní rozhledy*, 2018, roč. 26, č. 5, s. 167–172. ISSN 1210-6410.

NORBERG, Patricia A., Daniel R. HORNE a David A. HORNE. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* [online]. 2007, roč. 41, č. 1, s. 100–126. ISSN 0022-0078. DOI: 10.1111/j.1745-6606.2006.00070.x

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-665-5.

NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 2009, roč. 57, č. 6, s. 1701–1777. ISSN 0041-5650.

PEARCE, Henry. Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law? *Information & Communications Technology Law* [online]. 2018, roč. 27, č. 2, s. 133–165. ISSN 1360-0834. DOI: 10.1080/13600834.2018.1458449

PEARCE, Henry. Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law. *European Data Protection Law Review*, 2018, č. 2, s. 190–208. ISSN 0928-9801.

PENNEY, Jonathon. Chilling effects and transatlantic privacy. *European Law Journal* [online]. 2019, roč. 25, č. 2, s. 122–139. ISSN 1468-0386. DOI: 10.1111/eulj.12315

PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal* [online]. 2016, roč. 31, č. 1, s. 117–182. ISSN 1086-3818. DOI: 10.15779/Z38SS13

POLČÁK, Radim. Aims, methods and achievements in European data protection. *International Review of Law, Computers & Technology* [online]. 2009, roč. 23, č. 3, s. 179–188. ISSN 1360-0869. DOI: 10.1080/13600860903262248

POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, 388 s. ISBN 978-80-87284-22-3.

POLČÁK, Radim. Structure and Proportionality of Fundamental Rights in PSI Re-use. *Masaryk University Journal of Law and Technology*, 2013, roč. 6, č. 3, s. 381–400. ISSN 1802-5951.

POLČÁK, Radim. Getting European Data Protection Off the Ground. *International Data Privacy Law* [online]. 2014 [cit. 30. 6. 2020]. ISSN 2044-3994. DOI: 10.1093/idpl/ipu019

POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13, s. 67–91. ISSN 1804-5383.

POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, 640 s. ISBN 978-80-7598-045-8.

POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 86–98. ISSN 0231-6625.

POLČÁK, Radim a Dan Jerker B. SVANTESSON. *Information sovereignty: data privacy, sovereign powers and the rule of law*. Cheltenham, UK: Edward Elgar Publishing, 2017, 268 s. ISBN 978-1-78643-921-5.

POSNER, Richard A. *Economic analysis of law*. 3. vyd. Boston: Little, Brown, 1986, 666 s. ISBN 978-0-316-71438-9.

POSNER, Richard A. *Law, pragmatism, and democracy*. Cambridge, Mass: Harvard University Press, 2003, 398 s. ISBN 978-0-674-01081-9.

POST, Robert C. Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere. *Duke Law Journal*, 2017, roč. 67, č. 5, s. 981–1072. ISSN 0012-7086.

POUND, Roscoe. A Survey of Social Interests. *Harvard Law Review* [online]. 1943, roč. 57, č. 1, s. 1. ISSN 0017-811X. DOI: 10.2307/1334970

PROKEŠ, Josef. IP adresa v ochraně osobních údajů. *Data Security Management*, 2014, roč. 2014, č. 4, s. 31–33. ISSN 1211-8737.

PURTOVA, Nadezhda. Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review* [online]. 2009, roč. 25, č. 6, s. 507–521. ISSN 0267-3649. DOI: 10.1016/j.clsr.2009.09.004

PURTOVA, Nadezhda. Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights. *Netherlands Quarterly of Human Rights*, 2010, roč. 28, č. 2, s. 179–198.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* [online]. 2018, roč. 10, č. 1, s. 40–81. ISSN 1757-9961. DOI: 10.1080/17579961.2018.1452176

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 502–526. ISSN 1867-299X, 2190-8249. DOI: 10.1017/err.2018.47

RACHELS, James. Why Privacy is Important. *Philosophy & Public Affairs*, 1975, roč. 4, č. 4, s. 323–333. ISSN 0048-3915.

RAUHOFER, Judith. Privacy Is Dead, Get over It: Information Privacy and the Dream of a Risk-Free Society. *Information & Communications Technology Law,* 2008, č. 3, s. 185–198.

RECIO, Miguel. Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability Reports: Practitioner's Corner. *European Data Protection Law Review (EDPL)*, 2017, roč. 3, č. 1, s. 114–118. ISSN 2364-2831.

REDING, Viviane. The upcoming data protection reform for the European Union. *International Data Privacy Law; Oxford* [online]. 2011, roč. 1, č. 1, s. 3–5. ISSN 2044-3994. DOI: 10.1093/idpl/ipq007

REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 1976, roč. 6, č. 1, s. 26–44. ISSN 0048-3915.

REIMAN, Jeffrey H. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer and High-Technology Law Journal*, 1995, roč. 27, č. 1, s. 27–44. ISSN 2334-1610.

ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies* [online]. 2014, roč. 11, č. 1, s. 74–104. ISSN 1740-1461. DOI: 10.1111/jels.12035

ROTHSTEIN, Henry, Olivier BORRAZ a Michael HUBER. Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe. *Regulation & Governance* [online]. 2013, roč. 7, č. 2, s. 215–235. ISSN 1748-5983. DOI: 10.1111/j.1748-5991.2012.01153.x

ROTHSTEIN, Henry, Michael HUBER a George GASKELL. A theory of risk colonization: The spiralling regulatory logics of societal and institutional risk. *Economy & Society* [online]. 2006, roč. 35, č. 1, s. 91–112. ISSN 0308-5147. DOI: 10.1080/03085140500465865

SAFAROV, Igbal, Albert MEIJER a Stephan GRIMMELIKHUIJSEN. Utilization of open government data: A systematic literature review of types, conditions, effects and users. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2017, roč. 22, č. 1, s. 1–24. ISSN 1570-1255. DOI: 10.3233/IP-160012

SAMARATI, Pierangela a Latanya SWEENEY. *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression*. 1998.

SANDERS, Sherry D. Privacy Is Dead: The Birth of Social Media Background Checks. *Southern University Law Review*, 2011, č. 2, s. 243–264.

SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology* [online]. 2016, roč. 24, č. 1, s. 72–98. ISSN 0967-0769, 1464-3693. DOI: 10.1093/ijlit/eav017

SHANNON, Claude Elwood a Warren WEAVER. *The mathematical theory of communication*. [online]. Urbana: University of Illinois Press, 1949, 131 s. [cit. 27. 7. 2019]. Dostupné z: http://public.eblib.com/choice/publicfullrecord.aspx?p=4792736

SCHAIBLE, Johann et al. Linking Study Descriptions to the Linked Open Data Cloud. *IASSIST Quarterly*, 2014, roč. 38/39, č. 4/1, s. 38–46. ISSN 0739-1137.

SCHATZ, Daniel a Rabih BASHROUSH. The impact of repeated data breach events on organisations' market value. *Information & Computer Security* [online]. 2016, roč. 24, č. 1, s. 73–92. ISSN 2056-4961. DOI: 10.1108/ICS-03-2014-0020

SCHWARTZ, Paul M. a Daniel J. SOLOVE. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 2011, roč. 86, č. 6, s. 1814–1894.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada, 2006, 296 s. ISBN 978-80-247-1667-1.

SMITS, Jan M. *The mind and method of the legal academic*. Cheltenham, UK: Edward Elgar, 2012, 180 s. ISBN 978-0-85793-654-7.

SOKOL, Pavol, Jakub MÍŠEK a Martin HUSÁK. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, 2017, roč. 2017, č. 1, s. 1–9. ISSN 1687-4161.

SOLOVE, Daniel J. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review* [online]. 2001, roč. 53, č. 6, s. 1393–1462. ISSN 0038-9765. DOI: 10.2307/1229546

SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review* [online]. 2002, roč. 90, č. 4, s. 1087–1155. ISSN 0008-1221. DOI: 10.2307/3481326

SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review* [online]. 2006, roč. 154, č. 3, s. 477–564. ISSN 0041-9907. DOI: 10.2307/40041279

SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review*, 2007, roč. 44, s. 745–772.

SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2012, roč. 126, č. 7, s. 1880–1903. ISSN 0017-811X.

SOLOVE, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven Conn.: Yale University Press, 2013, 256 s. ISBN 978-0-300-17233-1.

SPITZNER, Lance. *Honeypots: tracking hackers*. Boston: Addison-Wesley, 2003, 452 s. ISBN 978-0-321-10895-1.

SPITZNER, Lance. The Honeynet Project: trapping the hackers. *IEEE Security & Privacy* [online]. 2003, č. 2, s. 15–23. ISSN 1540-7993. DOI: 10.1109/MSECP.2003.1193207

STENNING, Ashley. Gone But Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impacts of Data Breaches. *San Diego International Law Journal*, 2016, roč. 18, č. 1, s. 129–160. ISSN 1539-7904.

SVANTESSON, Dan Jerker B. A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4, s. 278–286. ISSN 2044-3994, 2044-4001. DOI: 10.1093/idpl/ipt027

SVANTESSON, Dan Jerker B. Article 4(1)(a) 'establishment of the controller in EU data privacy law – time to rein in this expanding concept? *International Data Privacy Law*, 2016, roč. 6, č. 3, s. 210–1. ISSN 2044-3994.

SVANTESSON, Dan Jerker B. Enter the quagmire – the complicated relationship between data protection law and consumer protection law. *Computer Law & Security Review* [online]. 2018, roč. 34, č. 1, s. 25–36. ISSN 0267-3649. DOI: 10.1016/j.clsr.2017.08.003

SVANTESSON, Dan Jerker B. a Dariusz KLOZA (eds.). *Trans-Atlantic data privacy relations as a challenge for democracy*. Cambridge; Antwerp;Portland: Intersentia, 2017, 567 s. ISBN 978-1-78068-434-5.

SWEENEY, L. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems* [online]. 2002, roč. 10, č. 5, s. 557–570. ISSN 0218-4885. DOI: 10.1142/S0218488502001648

ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, 212 s., Ediční řada Sborníky, sv. 50. ISBN 978-80-210-5449-3.

TELEC, Ivo. Držba informací. *Právní rozhledy*, 2014, roč. 22, č. 4, s. 115–120. ISSN 1210-6410.

TENE, Omer a Jules POLONETSKY. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 2012, roč. 11.

THOMSON, Judith Jarvis. The Right to Privacy. *Philosophy & Public Affairs*, 1975, roč. 4, č. 4, s. 295–314. ISSN 0048-3915.

TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken a Anna-Maria TALIHÄRM (eds.). *International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010, s. 24–39. ISBN 978-9949-9040-4-4. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/LP_Proceedings_2010.pdf

TIMAN, Tjerk, Bryce Clayton NEWELL a Bert-Jaap KOOPS (eds.). *Privacy in public space: conceptual and regulatory challenges*. Cheltenham, UK: Edward Elgar Publishing, 2017, 315 s. Elgar law, technology and society series. ISBN 978-1-78643-539-2.

TZANOU, Maria. Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection. *Croatian Yearbook of European Law & Policy*, 2010, roč. 6, s. 54–74. ISSN 1845-5662.

TZANOU, Maria. Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures. *Journal of Internet Law*, 2013, roč. 17, č. 3, s. 21–34. ISSN 1094-2904.

SLOOT, Bart van der. Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of Big Data. *Utrecht Journal of International and European Law*, 2015, roč. 31, č. 80, s. 25–50. ISSN 0927-460X.

VAN HAL, Timothy J. Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection Note. *Vanderbilt Journal of Entertainment and Technology Law*, 2013, roč. 15, č. 3, s. 713–752. ISSN 1536-3872.

VERSACI, Guiseppe. Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, 2018, roč. 14, č. 4, s. 374–392. ISSN 1614-9920.

VOIGT, Paul a Axel von dem BUSSCHE. *The EU general data protection regulation (GDPR)*. New York, NY: Springer Berlin Heidelberg, 2017, 383 s. ISBN 978-3-319-57958-0.

VOSS, W. Gregory. After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy in at Time of Change. *Business Lawyer*, 2015, roč. 71, č. 1, s. 281–292.

WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012, 931 s. ISBN 978-80-7357-750-6.

WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5, s. 193–220.

WEITZNER, Daniel J. et al. Information Accountability. *Communications of the ACM* [online]. 2008, roč. 51, č. 6, s. 82–87. ISSN 0001-0782. DOI: 10.1145/1349026.1349043

WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967, 487 s.

WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích*. Praha: Státní nakladatelství technické literatury, 1960, 148 s., Teoretická knižnice inženýra.

WINN, Michael et al. Constructing cost-effective and targetable industrial control system honeypots for production networks. *International Journal of Critical Infrastructure Protection* [online]. 2015, roč. 10, s. 47–58. ISSN 1874-5482. DOI: 10.1016/j.ijcip.2015.04.002

WONG, Rebecca. Data protection: The future of privacy. *Computer Law & Security Review* [online]. 2011, roč. 27, č. 1, s. 53–57. ISSN 0267-3649. DOI: 10.1016/j.clsr.2010.11.004

WRIGHT, David. The state of the art in privacy impact assessment. *Computer Law & Security Review* [online]. 2012, roč. 28, č. 1, s. 54–61. ISSN 0267-3649. DOI: 10.1016/j.clsr.2011.11.007

WRIGHT, David a Paul de HERT (eds.). *Privacy impact assessment*. Dordrecht; New York: Springer, 2012, 523 s., Law, governance and technology series, volume 6. ISBN 978-94-007-2542-3.

YORDANOV, Atanas. Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review*, 2017, roč. 3, č. 4, s. 486. ISSN 2364-2831.

ZANFIR, Gabriela. The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law; Oxford* [online]. 2012, roč. 2, č. 3, s. 149–162. ISSN 2044-3994. DOI: 10.1093/idpl/ips009

ZANFIR, Gabriela. Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European Data Protection Law*. Dordrecht: Springer Netherlands, 2015, s. 227–249. ISBN 978-94-017-9384-1.

ZARKER, Kenneth A. a Robert L. KERR. Pollution prevention through performance-based initiatives and regulation in the United States. *Journal of Cleaner Production* [online]. 2008, roč. 16, č. 6, s. 673–685, Advancing Pollution Prevention and Cleaner Production: USA's Contribution. ISSN 0959-6526. DOI: 10.1016/j.jclepro.2007.02.018

ZARSKY, Tal. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Science Technology and Human Values* [online]. 2016, roč. 41, č. 1, s. 118–132. ISSN 1552-8251. DOI: 10.1177/0162243915605575

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 2015, roč. 30, č. 1, s. 75–89. ISSN 0268-3962.

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. 1. vyd. New York: PublicAffairs, 2019, 691 s. ISBN 978-1-61039-569-4.

Kapitoly knih

ALBERS, Marion. Realizing the Complexity of Data Protection. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 213–235.

ALHADEFF, Joseph, Brendan Van ALSENOY a Jos DUMORTIER. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 49–82.

BUTIN, Denis, Marcos CHICOTE a Daniel Le MÉTAYER. Strong Accountability: Beyond Vague Promises. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 343–369.

BENNET, Colin J. Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 33–48.

BROWNSWORD, Roger. Consent in Data Protection Law. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 83–110.

CAVOUKIAN, Ann. Privacy by Design: Leadership, Methods, and Results. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 175–202.

COGLIANESE, Cory a Evan MENDELSON. Meta-Regulation and Self-Regulation. In: BALDWIN, Robert, Martin CAVE a Martin LODGE (eds.). *The Oxford handbook of regulation*. Oxford: Oxford University Press, 2012, s. 146–168.

DE TERWANGE, Cécile. The Right to be Forgotten and Informational Autonomy in the Digital Environment. In: GHEZZI, Alessia, Ângela Guimarães PEREIRA a Lucia VESNIĆ-ALUJEVIĆ (eds.). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. Houndmills: Palgrave Macmillan UK, 2014, s. 82–101.

FINN, Rachel L., David WRIGHT a Michael FRIEDWALD. Seven Types of Privacy. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht: Springer Netherlands, 2013, s. 3–32.

FOLDOVÁ, Vanda. § 5 odst. 2 písm. c). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 140–142, Beckova edice komentované zákony.

GELLERT, Raphaël a Serge GUTWIRTH. Beyond Accountability, the Return to Privacy? In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 261–283.

GRATT, Lawrence B. Risk Analysis or Risk Assessment; A Proposal for Consistent Definitions. In: COVELLO, Vincent T. et al. (eds.). *Uncertainty in risk assessment, risk management, and decision making*. New York; London: Plenum Press, 1987, s. 241–250. ISBN 978-0-306-42557-8.

HERBST, Tobias. Art. 5. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 210–233.

HARTUNG, Jürgen. Art. 30. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 628–643.

HERT, Paul de a Serge GUTWIRTH. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: CLAES, Erik, Antony DUFF a Serge GUTWIRTH (eds.). *Privacy and the criminal law*. Antwerp: Intersentia, 2006, s. 61–104.

HERT, Paul de a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 3–44.

HERT, Paul de. Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law. In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 193–232.

HOECKE, Mark Van. Legal Doctrine: Which Method(s) for What Kind of Discipline? In: HOECKE, Mark van (ed.). Methodologies of legal research: which kind of method for what kind of discipline? Oxford, Portland: Hart, 2011, s. 1–18. European Academy of Legal Theory monograph series.

HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. 1. vyd. New York, NY: Oxford University Press, 2017, s. 123–173, The collected courses of the Academy of European Law.

KORENHOF, Paulan et al. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reforming European data protection law*. Dordrecht: Springer, 2015, s. 171–201.

KOŠČÍK, Michal. Výzkumná data ve světle absolutních majetkových práv. In: KOŠČÍK, Michal et al. *Výzkumná data a výzkumné databáze. Právní rámec zpracování a sdílení vědeckých poznatků*. Praha: Wolters Kluwer ČR, 2018, s. 25–31.

KRATOCHVÍL, Jan. Kapitola XVIII [čl. 8 EÚLP]. In: KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C. H. Beck, 2012, s. 863–962.

KUČEROVÁ, Alena. § 1. In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Beckova edice komentované zákony. Praha: C. H. Beck, 2012, s. 1–4.

KUČEROVÁ, Alena. § 5 odst. 2 písm. a). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 133–138, Beckova edice komentované zákony.

LANGÁŠEK, Tomáš. Čl. 7. In: WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012.

LYNSKEY, Orla. From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. In: GUTWIRTH, Serge et al. (eds.). *European Data Protection: Coming of Age*. Dordrecht, Springer Netherlands, 2013, s. 59–84.

MÉTAYER, Daniel Le. a Julien Le CLAINCHE. From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles. In: GUTWIRTH, Serge et al. (eds.). *European data protection: in good health?* New York: Springer, 2012, s. 315–329.

MÍŠEK, Jakub. Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing). In: SVANTESSON, Dan Jerker B. a Dariusz KLOZA (eds.). *Trans-Atlantic data privacy relations as a challenge for democracy*. Cambridge, Antwerp, Portland: Intersentia, 2017, s. 331–346.

MÍŠEK, Jakub. Data veřejného sektoru. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 347–390.

NARAYANAN, Arvind, Joanna HUEY a Edward W. FELTEN. A Precautionary Approach to Big Data Privacy. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, s. 357–485.

NARDELL QC, Gordon. Levelling up: Data Privacy and the European Court of Human Rights. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Data protection in a profiled world*. Dordrecht; New York: Springer, 2010, s. 43–52.

NOVÁKOVÁ, Ludmila. § 5, Odst. 1, písm. a). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 102–108, Beckova edice komentované zákony.

PEREIRAA, Ângela Guimarães, Lucia VESNIĆ-ALUJEVIĆA a Alessia GHEZZIA. The Ethics of Forgetting and Remembering in the Digital World through the Eye of the Media. In: GHEZZI, Alessia, Ângela Guimarães PEREIRA a Lucia VESNIĆ-ALUJEVIĆ (eds.). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. Houndmills: Palgrave Macmillan UK, 2014, s. 9–27.

POLČÁK, Radim. Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 1–28.

POSPÍŠIL, Daniel. § 5 odst. 2 d) a e). In: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů: komentář*. Beckova edice komentované zákony. Praha: C. H. Beck, 2012, s. 141–148.

PURTOVA, Nadezhda. Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence. In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Computers, privacy and data protection: an element of choice*. Dordrecht; New York: Springer, 2011, s. 39–64.

QUELLE, Claudia. The 'Risk Revolution' in EU Data Protection Law: We can't Have Our Cake and Eat it, Too. In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 33–62.

RAAB, Charles. The Meaning of 'Accountability' in the Information Privacy Context- In: GUAGNIN, Daniel et al. (eds.). *Managing privacy through accountability*. Houndmills, Basingstoke: Palgrave Macmillan, 2012, s. 15–47.

ROOSENDAAL, Arnold. We Are All Connected to Facebook… by Facebook! In: GUTWIRTH, Serge et al. (eds.). *European data protection: in good health?* New York: Springer, 2012, s. 3–19.

ROUVROY, Antoinette a Yves POULLET. The Right to Informational Self-Determination and the Value of Self-Development. In: GUTWIRTH, Serge et al. (eds.). *Reinventing data protection?* Dordrecht: Springer, 2009, s. 45–76.

SOBEK, Tomáš. Svoboda a soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, s. 37–48, Ediční řada Sborníky, sv. 50.

SLOOT, Bart van der. Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Data protection on the move*. Dordrecht: Springer, 2016, s. 411–436.

SLOOT, Bart van der. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: LEENES, Ronald et al. (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer, 2017, s. 3–31.

SNYDER BENNEAR, Lori. Evaluating Management-Based Regulation: A Valuable Tool in the Regulatory Toolbox?. In: COGLIANESE, Cary a Jennifer NASH (eds.). *Leveraging the private sector: management-based strategies for improving environmental performance*. Washington, DC: RFF PRess, 2006, s. 51–86.

TŮMA, Pavel. § 86 [Právo člověka na soukromí]. In: LAVICKÝ, Petr (ed.). *Občanský zákoník: komentář*. 1. vyd. Praha: C. H. Beck, 2014, s. 509–523.

WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní Politologický Ústav, 2011, s. 49–62, Ediční řada Sborníky, sv. 50.

WAGNEROVÁ, Eliška. Čl. 10. In: WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012. Dostupné z: ASPI [Právní informační systém].

WEICHERT, Thilo. Art. 9. In: KÜHLING, Jürgen et al. *Datenschutz-Grundverordnung/BDSG: Kommentar*. 2. vyd. München: C. H. Beck, 2018, s. 319–358.

ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge, Ronald LEENES a Paul de HERT (eds.). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Dordrecht: Springer, 2014, s. 237–257.

Další online zdroje

AHS, James M. European Commission Announces New U.S.-EU Safe Harbor Agreement. *HuschBlackwell.com* [online]. [cit. 30. 6. 2020]. Dostupné z: https://www.huschblackwell.com/newsandinsights/Alert-European-Commission-Announces-New-US-EU-Safe-Harbor-Agreement-02-02-2016

BERNERS-LEE, Tim. *5*Open Data* [online]. [cit. 30. 6. 2020]. Dostupné z: http://5stardata.info

JOHNSON, Bobbie. Privacy no longer a social norm, says Facebook founder. *The Guardian* [online]. 2010 [cit. 30. 6. 2020]. Dostupné z: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

KAMÍNEK, Petr. Návod jak na GDPR. *Google sites* [online]. 2018 [cit. 25. 6. 2019]. Dostupné z: https://sites.google.com/site/jaknagdpr/home

KUNEVA, Meglena. Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling. *Europa.eu* [online]. [cit. 30. 6. 2020]. Dostupné z: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Liability. *The Law Dictionary* [online]. [cit. 30. 6. 2020]. Dostupné z: https://thelawdictionary.org/liability/

PROUST, Olivier. EU-U.S. Privacy Shield comes into force. *Privacy, Security and Information Law* [online]. 2016 [cit. 30. 6. 2020]. Dostupné z: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-comes-into-force/

Publications. *The Information Accountability Foundation* [online]. [cit. 30. 6. 2020]. Dostupné z: http://informationaccountability.org/publications/

WIKIPEDIA. Streisand effect. *Wikipedia.org* [online]. [cit. 30. 6. 2020]. Dostupné z: https://en.wikipedia.org/wiki/Streisand_effect

Mapa exekucí [online]. [cit. 30. 6. 2019]. Dostupné z: http://mapaexekuci.cz/

Doporučení, stanoviska a další dokumenty

Adequacy decisions. *Evropská komise* [online]. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Asia-Pacific Economic Cooperation (APEC). *Apec.org* [online]. APEC Privacy Framework, 2005, 36 s. [cit. 30. 6. 2020]. Dostupné z: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

Data Protection Accountability: The Essential Elements A Document for Discussion. *The Centre for Information Policy Leadership, Hunton & Williams LLP* [online]. 2009, 21 s. [cit. 30. 6. 2020]. Dostupné z: https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf

Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. *Evropská komise* [online]. Press Release Database, 2012 [cit. 25. 6. 2019]. Dostupné z: http://europa.eu/rapid/press-release_IP-12-46_en.htm

ČSN ISO/IEC 29134, Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí.

Data transfers to the US and Safe Harbor – interim guidance. *Information commissioner's office* [online]. 2016 [cit. 30. 6. 2020]. Dostupné z: https://ico.org.uk/media/1560653/data-transfers-to-the-us-and-safe-harbor-interim-guidance.pdf

Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník. Zvláštní část, § 178. Dostupné z: Beck-online [Právní informační systém]. [cit. 30. 6. 2020].

EUROSTAT. Statistics on small and medium-sized enterprises. *Europa.eu* [online]. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises#General_overview

EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů. In: *EurLex* [online]. KOM(2007) 87, 2007, 10 s. [cit. 30. 6. 2020]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:CS:PDF

EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Komplexní přístup k ochraně osobních údajů v Evropské unii. In: *EurLex* [online]. KOM(2010) 609, 19 s. [cit. 30. 6. 2020]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:CS:PDF

First fine imposed by the President of the Personal Data Protection Office. *Evropský sbor pro ochranu osobních údajů* [online]. 2019 [cit. 30. 6. 2020]. Dostupné z: https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_cs

First report on the implementation of the Data Protection Directive (95/46/EC). *Evropská komise* [online]. 2003, 27 s.[cit. 30. 6. 2020]. Dostupné z: http://ec.europa.eu/transparency/regdoc/rep/1/2003/EN/1-2003-265-EN-F1-1.Pdf

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. *Evropský sbor pro ochranu osobních údajů* [online]. 2019, 29 s. [cit. 30. 6. 2020]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

Guidelines 3/2019 on processing of personal data through video devices. *Evropský sbor pro ochranu osobních údajů* [online]. 2019, 29 s. [cit. 31. 7. 2019]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

Handbook on Security of Personal Data Processing. *ENISA* [online]. 2017, 68 s. [cit. 30. 6. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport

International Conference of Data Protection and Privacy Commissioners (5. 11. 2009). International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution [online]. 2009, 36 s. [cit. 30. 6. 2020]. Dostupné z: https://dig.watch/sites/default/files/2009_M1.pdf

Legislativní pravidla vlády, ve znění pozdějších usnesením vlády. *Vláda České republiky* [online]. [cit. 30. 6. 2020]. Dostupné z: https://www.vlada.cz/cz/ppov/lrv/dokumenty/legislativni-pravidla-vlady-91209/#_ftn1

Nepravdy o wi-fi v souvislosti s GDPR. *Úřad pro ochranu osobních údajů* [online]. 2018, [cit. 25. 6. 2019]. Dostupné z: https://www.uoou.cz/nepravdy%-2Do%2Dwi%2Dfi%2Dv%2Dsouvislosti%2Ds%2Dgdpr/d-28774)

Obecné zásady pro hodnocení dopadů regulace (RIA). *Vláda České republiky*. [online]. 2016, 34. s. [cit. 25. 6. 2019]. Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/metodiky/OZ_RIA_-novela_2016_uplne-zneni-FINAL.pdf

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Organizace pro hospodářskou spolupráci a rozvoj* [online]. [cit. 30. 6. 2020]. Dostupné z: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Opinion on the Communication from the Commissionto the European Parliament and the Council on the follow-up of the Work Programme for betterimplementation of the Data Protection Directive (2007/C 255/01). *Evropský inspektor ochrany osobních údajů* [online]. [cit. 30. 6. 2020]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/07-07-25_dir95-46_en.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 4/2007 k pojmu osobní údaj. *Evropská komise* [online]. 20. 6. 2007, 26 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 1/2008 k otázkám ochrany údajů v souvislosti s vyhledávači. *Evropská komise* [online]. 4. 4. 2008, 29 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko „The Future of Privacy". *Evropská komise* [online]. 1. 12. 2009, č. 02356/09/EN, WP 168, 28 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel". *Evropská komise* [online]. 16. 2. 2010, 34 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 3/2010 k zásadě odpovědnosti. *Evropská komise* [online]. 13. 7. 2010, 19 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení. *Evropská komise* [online]. 16. 5. 2011, 20 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 15/2011 k definici souhlasu. *Evropská komise* [online]. 13. 7. 2011, 38 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 3/2013 o limitaci účelem. *Evropská komise* [online]. 2. 10. 2013, 70 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. *Evropská komise* [online]. 9. 4. 2014, 71 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Stanovisko č. 5/2014 k technikám anonymizace. *Evropská komise* [online]. 10. 4. 2014, 39 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement on the role of a risk-based approach in data protection legal frameworks. *Evropská komise* [online]. 30. 5. 2014, č. 14/EN, WP 218, 4 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Statement of the Article 29 Working Party. *Evropská komise* [online]. 16. 10. 2015 [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny týkající se pověřenců pro ochranu osobních údajů. *Evropská komise* [online]. 13. 12. 2016, v revidovaném znění 5. 4. 2017, č. WP243rev.01, 29 s. [cit. 30. 6. 2020]. Dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679. *Evropská komise* [online]. 3. 10. 2017, č. WP253, 17 s. [cit. 30. 6. 2020]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679. *Evropská komise* [online]. 4. 4. 2017, v revidovaném znění ze dne 4. 10. 2017, č. WP248rev.01. 24 s. [cit. 30. 6. 2020]. Dostupné z: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

PRACOVNÍ SKUPINA ZŘÍZENÁ DLE ČLÁNKU 29. Pokyny pro souhlas podle nařízení 2016/679. *Evropská komise* [online]. 28. 11. 2017, v revidovaném znění ze dne 10. 4. 2018, č. WP259rev.01, 32 s. [cit. 30. 6. 2020]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

Privacy Impact Assessment (PIA). *CNIL* [online]. 2018, 109 s. [cit. 30. 6. 2020]. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

RADA EVROPY. Modernisation of the Data Protection "Convention 108". *Council of Europe* [online]. [cit. 30. 6. 2020]. Dostupné z: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

Report of the Special Rapporteur on the right to Privacy. *Office of the High Commissioner for Human Rights* [online]. 19. 10. 2017, 26 s. [cit. 30. 6. 2020]. Dostupné z: http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

Stanovisko 4/2017. *Evropský inspektor ochrany osobních údajů* [online]. 14. 3. 2017, 26 s. [cit. 30. 6. 2020]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf

ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Návrh zákona o hromadném řízení (703/19). *ODOK* [online]. [cit. 30. 6. 2020]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBA9EXSST

Citované předpisy

Mezinárodní smlouvy

Vyhláška MZV č. 120/1976 Sb. ze dne 10. 5. 1976 o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb. m. s., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

Sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Evropské předpisy

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Charta základních práv a svobod Evropské unie (dokument č. 2000/C 364/1).

Listina základních práv a svobod Evropské unie (Dokument č. 2010/C 83/02).

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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).

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 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.

Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. 7. 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (oznámeno pod číslem C(2016) 4176).

Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. 10. 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.

Směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. 5. 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

České předpisy

Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.

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

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, ve znění pozdějších předpisů.

Zákon č. 110/2019 Sb., o zpracování osobních údajů.

Zahraniční předpisy

Personal Information Protection and Electronic Documents Act (PIPEDA, Kanada). *Justice Laws Website* [online]. 2000 [cit. 30. 6. 2020]. Dostupné z: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Citovaná rozhodnutí

Evropský soud pro lidská práva

Rozsudek Evropského soudu pro lidská práva ze dne 2. 8. 1984 ve věci *Malone vs. Spojené království*, stížnost č. 8691/79. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 26. 3. 1987 ve věci *Leander vs. Švédsko*, stížnost č. 9248/81. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 7. 7. 1989 ve věci *Gaskin vs. Spojené království*, stížnost č. 10454/83. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 25. 3. 1992 ve věci *B. vs. Francie*, stížnost č. 13343/87. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 28. 10. 1994 ve věci *Murray vs. Spojené království*, stížnost č. 14310/88. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 28. 9. 1999 ve věci *Öztürk vs. Turecko*, stížnost č. 22479/93. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 4. 5. 2000 ve věci *Rotaru vs. Rumunsko*, stížnost č. 28341/95. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 25. 9. 2001 ve věci *P. G. a J. H. vs. Spojené království*, stížnost č. 44787/98. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 29. 4. 2002 ve věci *Pretty vs. Spojené království*, stížnost č. 2346/02. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 28. 1. 2003 ve věci *Peck vs. Spojené království*, stížnost č. 44647/98. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 13. 2. 2003 ve věci *Odièvre vs. Francie*, stížnost č. 42326/98. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 24. 6. 2004 ve věci *Von Hannover vs. Německo*, stížnost č. 59320/00. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 10. 4. 2007 ve věci *Evans vs. Spojené království*, stížnost č. 6339/05. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 1. 7. 2008 ve věci *Liberty a další vs. Spojené království*, stížnost č. 58243/00. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2008 ve věci *S. a Marper vs. Spojené království*, stížnosti č. 30562/04 a 30566/04. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci *Von Hannover vs. Německo (No. 2)*, stížnosti č. 40660/08 a 60641/08. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci Axel *Springer vs. Německo*, stížnost č. 39954/08. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 18. 12. 2012 ve věci *Ahmet Yildirim vs. Turecko*, stížnost č. 3111/10. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2015 ve věci *Roman Zakarov vs. Rusko*, stížnost č. 47143/06. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 27. 6. 2017 ve věci *Satakunnan Markkinapörssi Oy a Satamedia Oy vs. Finsko*, stížnost č. 931/13. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 24. 4. 2018 ve věci *Benedik vs. Slovinsko*, stížnost č. 62357/14. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Rozsudek Evropského soudu pro lidská práva ze dne 28. 6. 2018, ve věcech *M.L. a W.W. vs. Německo*, stížnosti č. 60798/10 a 65599/10. Dostupné z: http://hudoc.echr.coe.int [cit. 30. 6. 2018].

Evropský soudní dvůr a Soudní dvůr Evropské unie

Rozsudek Evropského soudního dvora ze dne 20. 5. 2003 ve věci *Österreichischer Rundfunk a další*, C-465/00. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Evropského soudního dvora ze dne 6. 11. 2003 ve věci *Bodil Lindqvist*, C-101/01. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Evropského soudního dvora ze dne 29. 1. 2008 ve věci Promusicae, C-275/06. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Evropského soudního dvora ze dne 16. 12. 2008 ve věci *Satakunnan Markkinapörssi a Satamedia*, C-73/07. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Evropského soudního dvora ze dne 7. 5. 2009 ve věci *Rijkeboer*, C-553/07. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Evropského soudního dvora ze dne 9. 11. 2010 ve věcech *Volker und Markus Schecke* a *Eifert*, C-92/09 a 93/09. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 24. 11. 2011 ve věci Scarlet Ex*tended,* C-70/10. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 24. 11. 2011 ve věci *ASNEF*, C-468/10. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 30. 5. 2013 ve věci *Worten*, C-342/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 7. 11. 2013 ve věci *IPI*, C-473/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 13. 2. 2014 ve věci *Svensson a další*, C-466/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 8. 4. 2014 ve věci *Komise vs. Maďarsko*, C-288/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014 ve věci *Google Spain*, C-131/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 17. 7. 2014 ve věci *YS a další*, C-141/12. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 21. 10. 2014 ve věci *BestWater International*, C-348/13. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci *Ryneš*, C-212/13. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 16. 6. 2015 ve věci *Coty Germany,* C-580/13. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci *Bara a další*, C-201/14. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2015 ve věci *Weltimmo*, C-230/14. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2015 ve věci *Schrems*, C-362/14. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 8. 9. 2016 ve věci *GS Media*, C-160/15. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 19. 10. 2016 ve věci *Breyer,* C-582/14. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 27. 9. 2017 ve věci *Puškár,* C-73/16. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 20. 12. 2017 ve věci *Nowak,* C-434/16. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 25. 1. 2018 ve věci *Schrems*, C-498/16. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 10. 7. 2018 ve věci *Jehovan todistajat,* C-25/17. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 14. 2. 2019 ve věci *Buivids*, C-345/17. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 29. 7. 2019 ve věci *Fashion ID*, C-40/17. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 24. 9. 2019 ve věci *GC a další*, C-136/17. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 1. 10. 2019 ve věci *Planet49*, C-673/17. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 9. 7. 2020 ve věci *Land Hessen*, C-272/19. Dostupné z: http://curia.europa.eu [cit. 20. 7. 2020].

Rozsudek Soudního dvora Evropské unie ze dne 16. 7. 2020 ve věci *Schrems II*, C-311/18. Dostupné z: http://curia.europa.eu [cit. 20. 7. 2020].

Usnesení Soudního dvora Evropské unie ze dne 19. 6. 2014 ve věci *Pharmacontinente - Saúde e Higiene a další*, C-683/13. Dostupné z: http://curia.europa.eu [cit. 30. 6. 2020].

Ústavní soud

Nález Ústavního soudu ze dne 12. 1. 1994, sp. zn. Pl.ÚS 4/94, č. N 46/2 SbNU 557, č. 214/1994 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 21. 3. 2002, sp. zn. III.ÚS 256/01, N 37/25 SbNU 287. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl.ÚS 3/02, č. N 105/24 SbNU 177, č. 405/2002 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 28. 1. 2004, sp. zn. Pl.ÚS 41/02, č. N 10/32 SbNU 61, č. 98/2004 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 9. 3. 2004, sp. zn. Pl.ÚS 38/02, č. N 36/32 SbNU 345, č. 299/2004 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I.ÚS 453/03, č. N 209/39 SbNU 215. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 17. 7. 2007, sp. zn. IV.ÚS 23/05, č. N 111/46 SbNU 41. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 1. 12. 2008, sp. zn. I.ÚS 705/06, č. N 207/51 SbNU 577. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 21. 4. 2009, sp. zn. II.ÚS 703/06. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 2. 11. 2009, sp. zn. II.ÚS 2048/09, č. N 232/55 SbNU 181. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 7. 4. 2010, sp. zn. I.ÚS 22/10, č. N 77/57 SbNU 43. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 18. 8. 2009, sp. zn. I.ÚS 557/09, č. N 188/54 SbNU 325. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 15. 11. 2010, sp. zn. I.ÚS 517/10, č. N 223/59 SbNU 217. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625, 94/2011 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl.ÚS 24/11, č. N 217/63 SbNU 483, 43/2012 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 27. 11. 2012, sp. zn. Pl.ÚS 1/12, č. N 195/67 SbNU 333. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 9. 12. 2014, sp. zn. II.ÚS 1774/14, č. N 221/75 SbNU 485. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 12. 12. 2017, sp. zn. Pl.ÚS 26/16. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl.ÚS 45/17, č. 161/2019 Sb. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Usnesení Ústavního soudu ze dne 5. 9. 2017 sp. zn III.ÚS 3565/16. Dostupné z: http://nalus.usoud.cz [cit. 30. 6. 2020].

Nejvyšší soud

Rozsudek Nejvyššího soudu ze dne 16. 9. 2015, sp. zn. 30 Cdo 3629/2014, č. 55/2016 Sb.NS. Dostupné z: http://nsoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího soudu ze dne 17. 12. 2015, sp. zn. 21 Cdo 367/2015, č. 45/2017 Sb.NS. Dostupné z: http://nsoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího soudu ze dne 26. 2. 2019, sp. zn. 30 Cdo 2233/2017. Dostupné z: http://nsoud.cz [cit. 30. 6. 2020].

Nejvyšší správní soud

Rozsudek Nejvyššího správního soudu ze dne 12. 2. 2009, č. j. 9 As 34/2008-68, č. 1844/2009 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 29. 7. 2009, č. j. 1 As 98/2008-148, č. 1944/2009 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 4. 9. 2012, č. j. 1 As 93/2009-273, č. 2732/2013 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 28. 6. 2013, č. j. 5 As 1/2011-156. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 13. 8. 2014, č. j. 1 As 78/2014-41, č. 3127/2014 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012-133, č. 3222/2015 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 8. 6. 2016 č. j. 3 As 118/2015-34. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 20. 9. 2017, č. j. 2 As 140/2017-57. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Rozsudek Nejvyššího správního soudu ze dne 19. 4. 2018, č. j. 2 As 107/2017-72. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Usnesení Nejvyššího správního soudu ze dne 6. 2. 2004, č. j. Konf 15/2003-24, č. 189/2004 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Usnesení Nejvyššího správního soudu ze dne 10. 3. 2004, č. j. Konf 11/2003-12, č. 426/2005 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Usnesení Nejvyššího správního soudu ze dne 24. 2. 2010, č. j. Konf 56/2009-7, č. 2274/2011 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Usnesení Nejvyššího správního soudu ze dne 17. 10. 2011, č. j. Konf 11/2011-6, č. 2500/2012 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Usnesení Nejvyššího správního soudu ze dne 14. 8. 2014, č. j. 1 As 78/2014-41, č. 3127/2014 Sb.NSS. Dostupné z: http://nssoud.cz [cit. 30. 6. 2020].

Zahraniční soudy

Rozhodnutí německého Spolkového ústavního soudu ze dne 15. 12. 1983, sp. zn. BvR 209/83, BVerfGE 65. Dostupné z: http://openjur.de [cit. 30. 6. 2020].

Rozhodnutí Royal Courts of Justice, Strand, London zde dne 8. 10. 2018, sp. zn. [2018] EWHC 2599 (QB). Dostupné z: http://judiciary.uk [cit. 30. 6. 2020].

Rozhodnutí ÚOOÚ

Rozhodnutí předsedkyně ÚOOU ze dne 6. 6. 2019, č. j. UOOU-03469/18-19. Dostupné z: http://uoou.cz [cit. 30. 6. 2020].

Rozhodnutí předsedkyně ÚOOU ze dne 5. 12. 2019, č. j. Č. j. UOOU-09383/18-17. Dostupné z: http://uoou.cz [cit. 30. 6. 2020].

MODERNÍ REGULATORNÍ METODY OCHRANY OSOBNÍCH ÚDAJŮ

JUDr. MgA. Jakub Míšek, Ph.D.

Vydala Masarykova univerzita
Žerotínovo nám. 617/9, 601 77 Brno
v roce 2020

Spisy Právnické fakulty Masarykovy univerzity
Edice Scientia, sv. č. 694

Tisk: Point CZ, s.r.o., Milady Horákové 890/20, 602 00 Brno
1. vydání, 2020

ISBN 978-80-210-9736-0
ISBN 978-80-210-9737-7 (online ; pdf)
www.law.muni.cz

ISBN 978-80-210-9737-7

MUNI PRESS

MUNI LAW