UNIVERZITA KARLOVA V PRAZE

Právnická fakulta

Dominik Vítek

PRÁVO BÝT ZAPOMENUT JAKO SOUČÁST OCHRANY OSOBNOSTI

Disertační práce

Školitel: doc. JUDr. PhDr. David Elischer, Ph.D.

Studijní program: Teoretické právní vědy – Občanské právo

Datum vypracování práce (uzavření rukopisu): 6. dubna 2022

Čestné prohlášení

Prohlašuji, že jsem předkládanou disertační práci vypracoval samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 575.776 znaků včetně mezer.

V Praze dne 19. dubna 2022

…….

Dominik Vítek

Poděkování

Na tomto místě bych tímto rád poděkoval docentu Davidu Elischerovi za jeho odborné vedení a konzultace během přípravy mé disertační práce a rovněž za jeho přátelský a lidský přístup a pomoc.

OBSAH

Seznam zkratek

***eCommerce* směrnice**	Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
***ePrivacy* směrnice**	Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), ve znění pozdějších předpisů
ESLP	Evropský soud pro lidská práv
GDPR **obecné nařízení o ochraně osobních údajů**	nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Google Spain	Rozhodnutí Soudního dvora Evropské unie ze dne 13. května 2014 ve věci C-131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González
Listina EU	Listina základních práv Evropské unie (2012/C 326/02)
LZPS	Ústavní zákon č. 2/1993 Sb., usnesení předsednictva České národní rady ze dne 16.

	prosince 1992 o vyhlášení LISTINY ZÁKLADNÍCH PRÁV a SVOBOD jako součásti ústavního pořádku České republiky
občanský zákoník **o.z.**	Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
SDEU	Soudní dvůr Evropské unie
SEU	Smlouva o Evropské unii (2016/C 202/01)
SFEU	Smlouva o fungování Evropské unie (2016/C 202/01)
směrnice 2016/680	Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
směrnice 95/46/ES	směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
trestní zákoník **t.z.**	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
Úmluva	Úmluva o ochraně lidských práv a základních svobod (Evropská úmluva o lidských právech)
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981)

ÚOOÚ	Úřad pro ochranu osobních údajů
Ústava	Zákon č. 1/1993 Sb., Ústava České republiky
WP29	Article 29 Data Protection Working Party (Pracovní skupina zřízená podle čl. 29 směrnice 95/46/ES)
zákon o některých službách informační společnosti	Zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých souvisejících zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů
zákon o svobodném přístupu k informacím	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
zákon o ochraně elektronických komunikací **ZEK**	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
zákon č. 101/2000 **ZOOÚ**	Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
zákon o zpracování osobních údajů **ZZOÚ**	Zákon č. 110/2019 Sb., o zpracování osobních údajů

Úvod

Právo být zapomenut (z anglického „*right to be forgotten*“ nebo „*right to oblivion*“) je poměrně nový fenomén, který byl v této podobě zformulován v roce 2014 Soudním dvorem Evropské unie ve věci *Google Spain*. Španělský občan jménem Mario Costeja González, jehož nemovitosti byly koncem devadesátých let předmětem exekuce z důvodu dluhu na sociálním pojištění, se domáhal výmazu výsledků vyhledávání ve vyhledávači společnosti Google, neboť existence informace o této exekuci mu významně znesnadňovala další podnikatelskou činnost. Jelikož španělský soud dospěl k závěru, že se jedná o zpracování osobních údajů, které bylo v té době upraveno harmonizačním rámcem v podobě směrnice 95/46/ES, podal předběžnou otázku Soudnímu dvoru Evropské unie, který na základě testu proporcionality mezi právem na ochranu soukromí subjektu údajů a veřejným zájmem veřejnosti nalézt uvedenou informaci na základě vyhledávání jména poprvé formuloval podobu práva být zapomenut. SDEU zde dovodil, že v případě, kdy neexistuje převažující legitimní zájem veřejnosti na existenci určité informace, má subjekt údajů právo požadovat, aby jeho osobní údaje byly smazány. Po dalším vývoji došlo k zakotvení tohoto práva v obecném nařízení o ochraně osobních údajů (v laické i odborné veřejnosti hojně označovaném zkratkou GDPR z anglického *General Data Protection Regulation*) coby nového evropského předpisu na ochranu osobních údajů, který v podobě nařízení, tedy přímo aplikovatelného právního předpisu, nahradil předchozí směrnici 95/46/ES a v článku 17 toto právo legislativně zakotvil jakožto inherentní institut práva ochrany osobních údajů.

Právo být zapomenut má nicméně mnohem hlubší kořeny, vycházející z podstaty ochrany soukromí jednotlivce, které je garantováno jako základní lidské právo, a úlohy zapomínání v lidské mysli. Neméně je pak třeba toto právo chápat jako nezbytnou součást internetového světa, ve kterém se nezapomíná.[1] Právě oblast nových technologií je jedním z hlavních důvodů, proč právo být zapomenut

[1] PERRYER, Sophie. The internet never forgets, but people do. [online]. 13.11.2018. [cit. 2022-01-18]. https://www.theneweconomy.com/technology/the-internet-never-forgets-but-people-do

celospolečensky rezonuje a jednotlivci si, i v důsledku zprofanování rozsudku Google Spain, přijetí GDPR nebo kauz okolo sociálních sítí (jako např. Facebook ve věci Cambridge Analytica) začali uvědomovat dopady, které internet může mít pro jejich každodenní život – ať již soukromý, nebo profesní. Digitální stopa, kterou každý z nás zanechává, přitom nutně nesouvisí s aktivním zpřístupňováním obsahu na internetu a sociálních sítích, ale z velké části se často jedná o metadata a jiné střípky (často v podobě např. cookies, beacons či jiných „sledovacích" technologií), které sledují způsoby užívání různých služeb, náš pohyb, naše chování a na základě kterých lze např. vystavět náš osobnostní profil[2]. Jak totiž velmi trefně v roce 2017 shrnul americký časopis The Economist, „*the world's most valuable resource is no longer oil, but data"*[3], což si zjevně velmi dobře uvědomují (rovněž) technologičtí giganti, jejichž bohatství je založeno právě na sběru, zpracování a dalším zužitkování tzv. big data.

Spojitost technologií, které užíváme téměř každou minutu svého života (ať již se jedná o počítače, mobilní telefony, tak chytrá *(smart)* zařízení – hodinky, náramky, konvice, ledničky, osvětlení domácnosti – ale i kamerové systémy a další a další zařízení, u nichž si často ani neuvědomujeme, že mohou sbírat data) a dat, které produkují, je enormní. Ve svém důsledku může zásadním způsobem narušovat soukromí, a to ze strany soukromých společností, ale i ze strany státní moci. Všechny tyto důvody přinášejí zásadní posun v ochraně soukromí a osobnosti, jelikož míra, ve které jsou tyto základní atributy člověka vystaveny potenciálním zásahům, se s příchodem technologií exponenciálně navýšila. To byl také jeden z důvodů přijetí GDPR a nezbytnosti posílení oblasti ochrany osobních údajů, jak zákonodárce vymezil na samém počátku tohoto předpisu: *„Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné*

[2] Srov. např. DEYOUNG, Colin a Ian SPENCE. (2004). Profiling information technology users: En route to dynamic personalization. Computers in Human Behavior. 20. 55-65. 10.1016/S0747-5632(03)00045-1.

[3] The world's most valuable resource is no longer oil, but data. [online]. 6.5.2017 [cit. 2022-03-16]. Dostupné z https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Fyzické osoby stále častěji své osobní údaje zveřejňují, a to i v globálním měřítku. Technologie změnily ekonomiku i společenský život […].“[4]

Technologie navíc zásadním způsobem posunuly význam ochrany soukromí. Ta se z původní roviny ochrany jednotlivce vůči státu (která je samozřejmě stále velmi významným prvkem) přesouvá k ochraně jednotlivců vůči jiným osobám soukromého práva – zejména tedy *big data* společnostem či nadnárodním korporacím, které na zpracování (osobních) dat –souvisejícím „vytěžování soukromí“ – mají postavené celé své obchodní modely. Proto je nezbytné, aby jednotlivci měli dostatečné nástroje ochrany svého soukromí a aby tyto nástroje stát účinně vymáhal. Právě právo být zapomenut – zakotvené a vymahatelné (přinejmenším) prostřednictvím pravidel obecného nařízení o ochraně osobních údajů – takovým nástrojem může být, jelikož (ve spojení s dalšími instituty ochrany soukromí) každému jednotlivci (slovy GDPR – subjektu údajů) poskytuje kontrolu nad způsobem nakládání s jeho osobními daty zejména s ohledem na minulost jednotlivce a možnost regulovat objem historických informací, které jsou o každém jednotlivci dostupné, a tedy v tomto rozsahu kontrolu nad mírou zásahu do jeho soukromí.

Oblast zpracování osobních údajů, a ve výsledku i jakýchkoliv dat, je přitom stále poměrně novou (právní) disciplínou, u které se zákonodárce snaží vytvořit dostatečně široký a obecný právní rámec, který by stanovil alespoň základní, trvalá a co nejširším způsobem použitelná pravidla. Nicméně, jak dokazuje i neustále nová judikatura i nejvyšších soudních instancí, technologie tato pravidla neustále posouvají a právo za nimi (částečně) zaostává. Nejinak tomu je i u práva být zapomenut; ač rámcově zakotven v GDPR, tento právní instrument je stále na startovní čáře své aplikační praxe. Osobně se s těmito problémy setkávám rovněž ve své advokátní praxi, kde často narážíme na limity aplikovatelnosti tohoto práva a mnohé interpretační problémy (obvykle však z pohledu opačného – tedy nikoliv jednotlivce, ale právě správců/zpracovatelů v oblasti ochrany osobních údajů, společností zpracovávajících big data, poskytovatelů cloud

[4] Bod 6 úvodních ustanovení GDPR.

computingových technologií, telekomunikačních operátorů či poskytovatelů služeb v poměrně nové oblasti tzv. internetu věcí (*Internet of Things,* často také jen jako *IoT*).

Z tohoto důvodu jsem se rozhodl ve své disertační práci blíže rozebrat institut práva být zapomenut, které považuji za potenciálně velmi silný nástroj ochrany soukromí. Na toto téma v České republice neexistuje ucelená monografie a veškeré výstupy, které se mi podařilo v české i zahraniční doktríně identifikovat, jsou jen ve formě dílčích výstupů, obvykle komentářové literatury. Existující publikace se věnují buď ochraně osobnosti na obecné úrovni, či pak specifické aplikaci práva být zapomenut dle pravidel zakotvených v čl. 17 GDPR (coby komentářová literatura, jako jsou v českém prostředí např. komentář autorského kolektivu Pattynová, Suchánková, Černý a Růžička a kol, v němž byly publikovány části této práce, jak je popsáno níže, nebo ze zahraničních autorů, komentář autorů Paula Voigta a Axela von dem Bussche nebo komentář německého kolektivu zahrnující Sibylle Gierschmann, Katharinu Schlender, Rainer Stentzel a Winfried Veil). Neexistuje však komplexní publikace rozebírající soukromoprávní aspekty práva být zapomenut, což považuji za hlavní cíl a přidanou hodnotu této práce, která, kromě jiného, podrobně rozebírá ideová východiska zapomnění a soukromí v právu, jejich význam pro jednotlivce i celou společnost a podá tak ucelený pohled na aplikační praxi práva být zapomenut.

V rámci této práce jsem si položil několik výzkumných otázek:

- je právo být zapomenut složkou ochrany osobnosti?
- vztahuje se právo být zapomenut i na právnické osoby?
- jsou data věcí a je právní povaha dat významná z hlediska uplatnitelnosti práva být zapomenut?
- jaké jsou teritoriální dopady práva být zapomenut a do jaké míry jej lze uplatňovat mimo území České republiky, resp. Evropské unie?

Práce je koncipována koherentně tak, aby podala komplexní přehled o tomto právním institutu. Postupuje od obecných kapitol (rozbor ochrany soukromí, rozbor ochrany osobnosti, rozbor aplikovatelnosti práva na ochranu osobních

údajů) po konkrétní části úzce spojené s uplatňováním práva být zapomenut a jeho aplikační praxí. Ačkoliv bych považoval takový rozbor přinejmenším za zajímavý pro aplikační praxi, v práci se zaměřuji pouze na právní aspekty práva být zapomenut a vzhledem ke své nedostačující odbornosti v dalších oblastech si netroufám předestřít rozbor též z technologického (či snad ekonomického nebo obchodního) hlediska, ač v některých částech tyto aspekty alespoň okrajově zvažuji. Zejména rozbor z pohledu kybernetického bych považoval za velmi přínosný a hodný bližší pozornosti. Zároveň z odborných diskuzí s mnoha IT a kybernetickými odborníky rozumím, že problematika permanence dat a jejich výmazu z různých nosičů je rovněž velmi komplexní tématikou, která není černo-bílá a kterou se specialisté v této oblasti rovněž intenzivně zabývají.[5].

Cílem této práce však není, a z rozsahového hlediska ani být nemůže, detailní rozbor každého dílčího právního institutu nebo pojmu, který v práci zvažuji či se jej jinak dotýkám. Jejich podrobný rozbor by bezesporu vydal na samostatnou práci a vedl by k nežádoucímu rozmělnění problematiky práva být zapomenut.

Tímto způsobem např. u testu proporcionality (kapitola 1.4) nezkoumám jednotlivá východiska proporčního poměřování základních práv, ale zaměřuji se pouze na proporcionalitu mezi právem na ochranu soukromí a právem veřejnosti na přístup k informacím, u nichž jsem pracoval s předpokladem, že jsou hlavními dvěma právy, které mají vliv na právo být zapomenut. V této práci se tak více nezabývám úvahami nad střetem mezi právem na ochranu soukromí (resp. konkrétně práva být zapomenut) např. s právem na vlastnictví nebo právem na výkon podnikatelské činnosti.

Kapitola 1 vedle výše uvedeného kompilačně-deskriptivní metodou popisuje historický vývoj ochrany soukromí a pojmu soukromí jako takového, jeho právní úpravu v českém právním řádu a evropském právu. Části této kapitoly (konkrétně 1.1 a 1.3) byly již publikovány jako součást mého disertačního výzkumu v podobě komentářové literatury k obecnému nařízení o ochraně osobních údajů

[5] Příkladem toho mohou být poměrně komplexní pravidla pro likvidaci dat zakotvená na úrovni přílohy č. 4 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

a k českému zákonu o zpracování osobních údajů (v tomto úvodu budu o této publikaci pro zjednodušení referovat pouze jako o „komentáři“).[6]

V kapitole 2 (právo na ochranu osobnosti a soukromí v občanském právu) vycházím z předpokladu, že primární složkou osobnosti, která může být v souvislosti s právem být zapomenut ohrožena, je právo na soukromí člověka, a uzavírám, že samozřejmě může dojít i k dotčení jiných složek (zejména důstojnosti člověka nebo jeho podoby), ale jelikož je osobnost komplexním souborem jednotlivých dílčích částí osobnosti, blíže tyto aspekty nerozbírám. Tato kapitola rovněž zodpovídá otázku, zda je právo být zapomenut součástí ochrany osobnosti, ačkoliv samotná podstata a analýza samotného práva být zapomenut je ponechána na kapitoly pozdější (zejména 5 a 6), a zda může být z tohoto důvodu použitelné i pro právnické osoby.

V kapitole 3 (právo na ochranu osobních údajů) rovněž není cílem poskytnout komplexní rozbor oblasti ochrany osobních údajů, nýbrž pouze těch institutů, které považuji za nejvíce relevantní a při jejichž výkladu může docházet k rozporuplným závěrům ve vztahu k právu být zapomenut; z tohoto důvodu se v práci např. nezaměřuji na výklad pojmů správce a zpracovatel osobních údajů nebo pobočka (angl. establishment), u nichž, ač samozřejmě mají relevanci při interpretaci a aplikaci práva být zapomenut, nepovažuji za nezbytné je pro účely této práce blíže analyzovat. Cílem této práce tedy není podat komentářový výklad všech potenciálně dotčených institutů, ale pouze předestřít ty nejvíce relevantní anebo sporné. Velké části této kapitoly byly zároveň již publikovány jako součást

[6] Tento komentář byl vydán ve dvou vydáních:

Původně v roce 2018 jako komentář k GDPR: PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ a Jiří ČERNÝ. Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě. Praha: Leges, 2018, 487 stran ; 21 cm. ISBN 978-80-7502-288-2.

A ve druhém vydání v roce 2019 v aktualizované podobě rovněž v doplnění s, v té době nově přijatým, českým zákonem o zpracování osobních údajů: PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4.

Pro jednoduchost veškeré pasáže, které byl již touto komentářovou formou vydány, odkazuji pouze na toto druhé aktualizované vydání.

mého disertačního výzkumu v podobě komentáře, kde byly součástí výkladu obecné působnosti tohoto předpisu (tedy komentář k čl. 1, 2 a 3 GDPR).

V kapitole 4 se zaměřuji na význam dat (a rozdíl mezi daty, osobními údaji a informacemi, se kterými jinak tato práce pracuje jako se synonymy), digitální stopu a právní povahu dat. Při zkoumání právní povahy dat, zejména tedy otázky, zda jsou data věcí, jsem identifikoval největší množství sporných bodů a značné množství otázek, které si soudní ani doktrinální praxe dosud nebyla schopna (jednoznačně) zodpovědět a jejichž detailní analýza významně převyšuje rozsah a cíle této práce. Touto otázkou je zejména otázka potenciálního vlastnictví dat případně možnosti omezení majetkových (subjektivních) práv k datům, které vyvstávají při přijetí hypotézy, že data jsou právní povahou věc. Vzhledem k tomu, že jsem při svém zkoumání dospěl k závěru, že tyto aspekty nemají přímý vliv na rozsah uplatnitelnosti práva být zapomenut (jelikož pracuji v práci s hypotézou, že se jedná o přirozené právo, které jé součástí osobnosti), nepodávám na tyto otázky vyčerpávající a konkrétní odpovědi. Součástí této kapitoly je rovněž samostatný rozbor možností dalšího zpracování zveřejněných osobních údajů, které může být velmi významné v internetovém prostředí a jehož možnosti mohou rovněž poměrně zásadním způsobem omezit kontrolu jednotlivců nad svými osobními údaji, a tedy zároveň jejich praktické možnosti uplatnění práva být zapomenut. Tento rozbor jsem rovněž publikoval jako spoluautor v rámci svého disertačního výzkumu.[7]

Kapitola 5 v detailu rozebírá filozofická východiska práva být zapomenut, jeho postupný vývoj – včetně rozboru rozsudku SDEU ve věci *Google Spain a* další vybranou judikaturu, která dopady práva být zapomenut blíže specifikovala (zejména tedy rozhodnutí ve věci Manni nebo CG a další). Vzhledem k tomu, že právo být zapomenut vychází z evropského práva, považuji za významný rozbor judikatury na úrovni členských států, která by měla být co nejvíce jednotná napříč celou Evropskou unií. Proto v této práci rovněž jako jeden z příkladů

[7] VÍTEK, Dominik a Jana PATTYNOVÁ. Využívání zveřejněných osobních údajů [online]. 14.6.2019 [cit. 2022-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/vyuzivani-zverejnenych-osobnich-udaju-109518.html.

rozebírám rozsudek německého Spolkového ústavního soudu z roku 2019 týkající se výmazů informací z online archivu německého televizního kanálu.

Kapitola 6 poskytuje detailní rozbor práva být zapomenut ve smyslu čl. 17 GDPR a rozebírá jeho jednotlivé složky a problematické body. Tato kapitola byla, až na mírné úpravy a aktualizaci pro účely této disertační práce, publikována jako součást komentáře k čl. 17 GDPR. Tuto kapitolu považuji za stěžejní část mé práce, jelikož analytickou metodou podrobně rozebírá institut práva být zapomenut z pohledu aktuálního právního rámce, s přihlédnutím ke všem jeho historickým i právně-filozofickým východiskům.

Kapitola 7 rozebírá možné důsledky, které může mít porušení práva být zapomenut ze strany povinných osob, přičemž hlavní důraz je kladen na náhradu újmy jako na jeden z hlavních možných důsledků. Rozbor dalších institutů, jako je případné bezdůvodné obohacení či nekalosoutěžních aspekty již není součástí této práce. Zároveň blíže neanalyzuji případné veřejnoprávní důsledky, včetně ukládání pokut podle obecného nařízení o ochraně osobních údajů či trestněprávní dopady, které by takové porušení mohlo přinášet.

V závěrečné kapitole této práce se zamýšlím nad potenciálními problémy aplikační praxe, zejména tedy uplatnitelnosti práva být zapomenut v prostředí internetu a *virálně* šířeného obsahu nebo v rámci systémů umělé inteligence.

Jak je uvedeno výše, části této práce byly v průběhu disertačního výzkumu již publikovány – většinově v podobě výše citovaného komentáře k obecnému nařízení a ochraně osobních údajů, na kterém jsem se podílel spolu s dalšími kolegy a ve kterém jsme se zaměřili na aplikační dopady ochrany osobních údajů na kybernetický a digitální svět. Zároveň uvádím, že tato komentářová literatura vycházela ze zdrojů, které jsou vždy v dané kapitole souhrnně citovány, avšak vzhledem k požadavkům nakladatelství nebyly citovány formou konkrétních citací pod čarou, jako tomu je ve zbylých částech této práce.

Konkrétně byly publikovány následující části této práce (které byly, s mírnými úpravami a aktualizacemi, do této práce převzaty):

Kapitola 1.1 (Historický vývoj úpravy soukromí), kapitola 1.2.2 (Ochrana osobních údajů), kapitola 1.3 (Právní úprava ochrany soukromí a osobních údajů),

kapitola 3.3 (Limity ochrany osobních údajů dle obecného nařízení o ochraně osobních údajů), kapitola 3.2.6 (Volný pohyb osobních údajů), kapitola 3.2.1 (Rozsah ochrany poskytované GDPR) byly publikovány jako součást komentáře k čl. 1 GDPR. Kapitola 1.3.2.3 (Český zákon o zpracování osobních údajů) byla publikována jako součást komentáře k čl. § 1 ZZOÚ. Kapitola 3.2.2 (Věcná působnost obecného nařízení o ochraně osobních údajů) byla publikována jako součást komentáře k čl. 2 GDPR. Kapitola 3.2.3 (Působnost zákona o zpracování osobních údajů) byla publikována jako součást komentáře k § 2 ZZOÚ. Kapitola 3.2.4 (Místní působnost obecného nařízení o ochraně osobních údajů) a kapitola 3.2.5 (Extrateritoriální působnost obecného nařízení o ochraně osobních údajů) byly publikována jako součást komentáře k čl. 3 GDPR. Kapitola 3.2.7 (Vliv GDPR mimo EU) byla publikována jako samostatný článek s názvem „Evropa jako světový standard pro bezpečnost (osobních) dat“, jak je citován v této kapitole. Kapitola 4.3 (Využívání zveřejněných osobních údajů) byla spolu ve spoluautorství s mou dlouholetou kolegyní Janou Pattynovou publikována jako samostatný článek „Využívání zveřejněných osobních údajů“, jak je citován v této kapitole. Kapitola 5.2.2 (Rozsudek SDEU ve věci Google Spain) a kapitola 6 (Právo být zapomenut z hlediska ochrany osobních údajů) byly publikovány jako součást komentáře k čl. 17 GDPR. Kapitola 7.3.1 (Nároky podle obecného nařízení o ochraně osobních údajů) byla publikována jako součást komentáře k čl. 79 GDPR. Kapitola 7.2.2 (Náhrada újmy podle obecného nařízení o ochraně osobních údajů) byla publikována jako součást komentáře k čl. 82 GDPR.

1 Právní rámec ochrany soukromí

1.1 Historický vývoj úpravy soukromí[8]

Jako samostatné téma a právní disciplína se ochrana soukromí (k vymezení pojmu soukromí pak viz kapitola 1.2 této práce) v evropské společnosti začala hojněji objevovat koncem 19. století, kdy byla spojována především s problematikou osobní cti a urážky na cti. Z teoretického hlediska pak tzv. *right to be let alone* (právo být ponechán o samotě, resp. sobě samému) v roce 1890 formulovali autoři Samuel D. Warren a Louis D. Brandeis[9], kteří doktrinálně navázali na dřívější „pojem" soudce Thomase Cooleyho z roku 1880 a formulaci *right to be alone* tak ve svém díle zpopularizovali. Warren a Brandeis považovali ochranu soukromí za přirozený vývoj a nevyhnutelný krok ve vývoji společnosti a právní ochrany. Tuto doktrínu vystavěli především na tehdejší rozhodovací praxi evropských soudů týkající se ochrany osobní cti a dobré pověsti, tedy na tehdy platné legislativě (tvořené spíše jednotlivými veřejnoprávními předpisy, nikoliv ucelenou právní úpravou).

V první polovině 20. století byla ochrana soukromí stále považována jen za okrajovou záležitost, která nezasluhuje širší pozornosti. Zatímco v Evropě se v této oblasti vyskytly alespoň náznaky pokroku, Spojené státy v ochraně soukromí nepokročily téměř vůbec. Poměrně paradoxně tak byla průlomová rozhodnutí v oblasti ochrany soukromí a osobních údajů přijata právě Nejvyšším soudem Spojených států amerických (U.S. Supreme Court). Ten v roce 1939 přijal hned dvě rozhodnutí ve věcech *Nardone* a *Weiss*, ve kterých na základě

[8] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

[9] WARREN, Samuel D. a BRANDEIS, Louis D. Right to privacy. Harv. L. Rev. 1890, 4, s. 193, dostupné online z https://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

federálního zákona o komunikacích z roku 1934 a výkladu čtvrtého dodatku americké ústavy (který obecně upravuje právo na ochranu svobody osobní a domovní) diskvalifikoval důkazy získané nezákonným odposlechem.[10] Soud se tak vůbec poprvé přiklonil k ochraně soukromé sféry jednotlivce, která by v souladu s liberálními myšlenkami zároveň měla sloužit k ochraně jednotlivce vůči zásahům státní moci. Zajímavá a významná je rovněž skutečnost, že rozhodnutí reagovala na využití moderních technologií při uplatňování státní moci.

Ochrana soukromé sféry jednotlivce vůči zásahům státní moci nabyla na významu po druhé světové válce, kdy nacistický režim díky přístupu k precizně vedeným matrikám, zaznamenávajícím kromě jiného také náboženské vyznání a původ jednotlivých občanů, měl usnadněnou práci s identifikací nepřátel režimu – a to jak na území samotného Německa, tak i v okupovaných územích, zejména pak v Nizozemí.[11] I ostatní autoritářské a totalitní režimy pouze potvrdily, že ochrana soukromé sféry jednotlivce je nezbytnou součástí moderní společnosti, a právo na soukromí se tak hojně objevovalo v nových ústavách posttotalitních zemí – např. Portugalsko (1976), Španělsko (1978), a později rovněž v ústavách většiny postsocialistických států střední a východní Evropy. V České republice je právo na soukromí chráněno podle čl. 7 a 10 LZPS.

Pokud se vrátíme zpět do poválečného období, nesmíme opomenout přijetí Všeobecné deklarace lidských práv v roce 1948 jako prvního mezinárodního dokumentu, který mj. zakotvil i právo na ochranu soukromého života. Ač Všeobecná deklarace lidských práv není mezinárodní smlouvou, stala se významným milníkem v oblasti ochrany soukromí a na tento předpis postupně navázaly mezinárodní dohody včetně Mezinárodního paktu o občanských a politických právech v roce 1966, který zcela převzal znění čl. 12 Všeobecné deklarace upravujícího právo na ochranu soukromí.

[10] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

[11] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

Na regionální – evropské – úrovni byla v roce 1950 Radou Evropy přijata Úmluva o ochraně lidských práv a základních svobod (Úmluva). Úmluva upravuje právo na respektování soukromého a rodinného života v článku 8 a díky ustanovení Evropského soudu pro lidská práva a jeho bohaté judikatuře (vykládající právě toto ustanovení) dodnes slouží jako významný nástroj pro nastavování pravidel ochrany soukromí v rámci Evropy.

Na článek 8 Úmluvy pak navázala specificky zaměřená Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů, kterou přijala rovněž Rada Evropy dne 28. ledna 1981. 28. leden od té doby slavíme jako Evropský den ochrany osobních údajů.

V roce 2003 byl k této Úmluvě č. 108 přijat Dodatkový protokol, který doplnil požadavky na zřízení nezávislého dozorového orgánu (jednoho či více) každým ze smluvních států a podřízení jeho rozhodnutí soudnímu přezkumu. Protokol se rovněž zabývá přeshraničním přenosem osobních údajů k příjemcům, kteří se nenacházejí v jurisdikci vázané Úmluvou 108. Příjemce v takovém případě musí zabezpečit dostatečnou úroveň ochrany zamýšleného přenosu dat. Česká republika Úmluvu 108 ratifikovala v roce 2001.

Když byla přijata směrnice 95/46/ES z roku 1995, zakotvila v evropském právu obdobné principy jako Úmluva 108. Vzhledem k tomu, že všechny členské státy EU (s výjimkou Itálie, která ratifikační proces dokončila až v roce 1997) byly zároveň smluvními stranami Úmluvy 108, nepředstavovalo přijetí nové směrnice zásadní novinku a nepřineslo drastické změny, které by výrazně měnily dosavadní režim ochrany osobních údajů.

1.2 Vymezení pojmu soukromí

1.2.1 Ochrana soukromí

1.2.1.1 Pojem a funkce soukromí

Právo být zapomenut je institutem nedílně spojovaným s ochranou osobních údajů, a v širším pojetí tedy s ochranou soukromí a osobnosti člověka.

Pojem „soukromí“ není v českém ani evropském právní řádu nijak vymezen; stejně tak s ním nepracují ani mezinárodní dohody. Jakékoliv rigidní legislativní

vymezení pojmu soukromí by mohlo být při aplikaci práva nežádoucí a mohlo by vést k nežádoucímu zužování tohoto pojmu, a tedy oslabení jeho ochrany.[12] Soukromí je, přinejmenším na území Evropské unie, chráněno jako základní lidské právo a jakékoliv jeho zužování je přípustné jen v mezích, které připouští Listina EU, LZPS či další lidskoprávní předpisy. Jak uvádí Judith Jarvis Thomson, *„nejspíš tou nejpozoruhodnější věcí na právu na soukromí je to, že nikdo nemá zřejmou představu o tom, co to vlastně je.“*[13] Podle Evropského soudu pro lidská práva pak není vyčerpávající definice soukromí možná, ale ani nutná[14]. Koncept soukromí (práva na soukromí) je natolik specifický, že je téměř nemožné jej podrobně vymezit a definovat, neboť v sobě zahrnuje nemalé množství aspektů týkajících se psychické a fyzické integrity jednotlivce a jeho soukromého života v interakci společenských vztahů.[15]

Pojetí pojmu „soukromí“ se významně liší a vyvíjí v čase (k historickému vývoji pojetí soukromí pak viz kapitola 1.1 této práce). Soukromí, jakožto základní lidské právo, je pak rovněž nezbytné vyvažovat a proporcionálně poměřovat vůči dalším právům – zejména pak právem na informace (srov. zejména kapitolu 1.4 této práce), nicméně v úvahu přicházejí i další práva, jako např. právo na vlastnictví či výkon podnikatelské činnosti, které mohou být zásadní zejména v souvislosti s vlastnictvím dat (srov. kapitolu 4.2 této práce).

Soukromí lze vnímat jako multidimenzionální fenomén skládající se z mnoha jednotlivých vrstev[16]. To potvrdil rovněž Ústavní soud, když konstatoval, že *„[právo na soukromí] se uplatňuje ve více sférách. Jedná se o soukromou sféru, sféru společenskou, občanskou a profesionální, přičemž poslední tři lze označit za sociální sféru. V první sféře jde vlastně o ochranu soukromí, v jehož*

[12] K tomu rovněž viz. MATEJKA, Ján. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. Praha: CZ.NIC, 2013, 256 s. ; 25 cm. ISBN 978-80-904248-7-6.

[13] THOMSON, JUDITH JARVIS. The Right to Privacy. Philosophy & public affairs [online]. Princeton, N.J: Princeton University Press, 1975, 4(4), 295-314 [cit. 2022-03-14]. ISSN 0048-3915, s. 295.

[14] Srov. Rozsudek ESLP ze dne 16. 12. 1992, stížnost č. 13710/88 (Niemietz proti Německu) [online]. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-57887.

[15] Rozsudek ESLP ze dne 4. prosince 2018 ve věci 30562/04 - Marper proti Spojenému království.

[16] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 328.

rámci se nepochybně uplatňuje i právo na čest. Zásadně je však věcí každého, co a v jakém rozsahu z této sféry uvolní jako informaci pro okolní svět. Jinými slovy, v tomto segmentu zpravidla platí naprosté informační sebeurčení. Sféra sociální, občanská a profesionální reflektují sociální povahu základních práv, resp. odrážejí fakt, že jednotlivec žije ve společenství a vstupuje s ostatními jeho členy do komunikace, přičemž skrze své chování, ba dokonce skrze své samotné bytí ovlivňuje ostatní členy společenství. V této druhé sféře již neplatí naprosté informační sebeurčení, jinými slovy do této sféry lze za určitých podmínek vstupovat, neboť se v ní mohou vyskytovat fakta, která mohou být předmětem oprávněného veřejného zájmu. Sociální sféry tak mohou být narušeny proporcionálními zásahy veřejné moci za účelem ochrany zájmů společenství. Vnější okraj sociální sféry jednotlivce tvoří tzv. veřejná sféra. Jedná se o ten segment lidského života, který může vnímat nebo brát na vědomí každý."[17]

1.2.1.2 Doktrinální přístupy k pojmu soukromí

Detailní vymezení pojmu soukromí a jeho obsahu není předmětem této práce. V každém případě však platí, že v odborné literatuře nalezneme celou řadu různých (historických) přístupů, přičemž k těm nejvýznamnějším lze řadit zejména následující:

- výše zmíněné historické pojetí soukromí jako *right to let alone*, tj. **soukromí jako ponechání sobě samému**, které reprezentují zejména Samuel Warren a Lousie Brandeise v jejich původní práci *„The Right to Privacy"*. Jejich práce z roku 1790 byla na svou dobu velmi pokroková a zaměřovala se na pokrok informačních a komunikačních technologií[18] a na integritu osobnosti člověka a její nedotknutelnost.

[17] Nález Ústavního soudu ze dne 17. července 2007, sp. zn. IV. ÚS 23/05.

[18] *„Vynálezy a obchodní metody poslední doby ukazují na potřebu učinit další krok v ochraně člověka, v zajištění toho, co soudce Cooley nazývá právem ‚být ponechán sám sobě'. […] Intenzita a komplexita moderního života, vyplývající z civilizačních pokroků, činí z možnosti uchýlit se do ústraní před světem nezbytnost; člověk se pod vlivem kulturního vývoje stal citlivějším vůči publicitě, pročež se samota a soukromí staly důležitějšími, než kdy dříve; moderní vynálezy však člověka prostřednictvím zásahů do soukromí vystavují mentálnímu utrpení v míře vyšší, než jaké by s sebou neslo fyzické poranění. […] Tyto úvahy nás vedou k závěru, že ochrana před neoprávněnou publikací, která je poskytována myšlenkám, názorům a citům vyjeveným prostřednictvím písemností či uměleckých děl, je pouhým projevem obecnějšího*

- **redukcionistické pojetí soukromí**, které soukromí jako takové nepovažuje za hlavní zájem a vychází z premisy, že soukromí lze vždy redukovat na skupinu jiných fundamentálních zájmů. Hlavní představitelkou tohoto pojetí je pak zejména Judith Jarvis Thomson[19], podle které je soukromí štěpitelné na jednotlivé různorodé zájmy v tom smyslu, že každý zásah do soukromí lze vyložit jako zásah do některého z fundamentálnějších práv jednotlivce, přičemž právo na soukromí jako takové nemusí být dotčeno.[20]
- **pojetí soukromí jako omezení přístupu k jednotlivci** vychází z principů *right to let alone*, které dále specifikuje[21]. Základní premisou tohoto přístupu je rozpoznání různých vrstev ochrany soukromí, které determinují možnosti přístupu k jednotlivci (a tedy do jeho soukromé sféry).[22] Podle hlavní představitelky tohoto názorového směru Ruth Gavison je dokonalým modelem soukromí naprostá nedostupnost jednotlivce ostatním lidem.[23] Z toho pak vychází rovněž tři hlavní složky soukromí: (i) utajení,

---

práva jednotlivce být ponechán sám sobě.“ in WARREN, Samuel D. a BRANDEIS, Louis D. Right to privacy. Harv. L. Rev. 1890, 4, s. 193, s. 205 dostupné online z https://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

[19] MOORE, Adam. Defining Privacy. Journal of Social Philosophy. 2008, 39(3), 411–428. ISSN 00472786, 14679833. s. 413 ; DECEW, Judith. Privacy. In: Edward N. ZALTA, ed. The Stanford Encyclopedia of Philosophy [online]. Spring 2018. B.m.: Metaphysics Research Lab, Stanford University, 2018, dostupné z: https://plato.stanford.edu/archives/spr2018/entries/privacy/.

[20] *„Nelze říci, že mé právo nebýt pozorována vyplývá z mého práva na soukromí; nelze říci, že mé právo nebýt mučena za účelem získání mých soukromých informací vyplývá z mého právo na soukromí; spíše by se chtělo říci, že právo na soukromí naopak vyplývá z těchto práv. […] Někdo vás mučí, aby z vás dostal soukromé informace? Pak zasáhl do vašeho práva nebýt mučen za účelem vyjevení soukromých informací, a toto právo vám přísluší, poněvadž máte právo na zachování fyzické integrity – a díky tomuto právu je jednání mučitele zásahem. Někdo užije rentgenového zařízení s cílem sledovat vás skrze stěny vašeho domu? Zasáhl do vašeho práva nebýt pozorován, které vám náleží, proto máte právo na vlastní osobu analogickou vlastnickému právu – a právě díky tomuto právu je jednání pozorovatele zásahem.“* in THOMSON, Judith Jarvis. The Right to Privacy. Philosophy & Public Affairs. 1975, 4(4), 295–314. ISSN 0048-3915. s. 312-313.

[21] SOLOVE, Daniel J. Conceptualizing Privacy. California law review [online]. Berkeley: School of Law, University of California, Berkeley, 2002, 90(4), 1087-1155 [cit. 2022-03-14]. ISSN 0008-1221. Dostupné z: doi:10.2307/3481326.

[22] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 35.

[23] GAVISON, Ruth. Privacy and the Limits of Law. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1980, 89(3), 421-471 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/795891.

(ii) anonymita a (iii) izolace; tyto složky jsou zcela nezávislé, neboť ztráta soukromí může být důsledkem zásahu do kterékoliv z nich.[24]

- **pojetí soukromí jako kontroly nad soukromými informacemi** je představováno zejména Alanem Westinem, podle kterého soukromí představuje *„nárok jednotlivců, skupin či organizací rozhodovat podle vlastního uvažování kdy, jakým způsobem a v jakém rozsahu budou jejich soukromé informace sdělovány ostatním".*[25] Tento přístup je významný v kontextu moderních technologií, jak dokládá rovněž český Ústavní soud[26] a je rovněž významným základem pro klastrové pojetí soukromí.
- **klastrová pojetí soukromí** je, zdá se, dnes nejkomplexnějším a nejvýstižnějším myšlenkovým směrem pro vymezení soukromí. Podle tohoto přístupu platí, že soukromí je určitým zastřešujícím souborem různých aspektů; na rozdíl od redukcionistického přístupu se však nemusí vždy jednat o samostatně chráněné zájmy, které by pojem soukromí štěpily. Za hlavní představitelku lze pak považovat Judith W. DeCew, která rozlišuje tři aspekty soukromí: (i) informační aspekt soukromí (*informational privacy)* umožňující kontrolu nad soukromými informacemi jednotlivce[27], (ii) přístupností aspekt soukromí (*accessibility privacy)* vycházející z fyzického přístupu k jednotlivci v určité prostorové dimenzi[28] a (iii) výrazový aspekt soukromí *(expressive privacy)* pokrývající především sebepojetí jednotlivce a jeho osobnosti

[24] GAVISON, Ruth. Privacy and the Limits of Law. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1980, 89(3), 421-471 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/795891.

[25] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 35.

[26] *„[…] právo na soukromí garantuje rovněž právo jednotlivce rozhodnou podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům".* Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10 (Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu).

[27] BORKOWSKI, S.C. Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching business ethics (Dordrecht) [online]. Dordrecht: Kluwer Academic Publishers, 1999, 3(4), 402-406 [cit. 2022-03-14]. ISSN 1382-6891. Dostupné z: doi:10.1023/A:1009843728384.

[28] BORKOWSKI, S.C. Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching business ethics (Dordrecht) [online]. Dordrecht: Kluwer Academic Publishers, 1999, 3(4), 402-406 [cit. 2022-03-14]. ISSN 1382-6891. Dostupné z: doi:10.1023/A:1009843728384.

prostřednictvím jeho projevu či jednání[29]. Výhodou tohoto pojetí soukromí je především schopnost dívat se na soukromí komplexně v mnoha různých kontextech. Klastrové vymezení soukromí je tak v zásadě základem doktrinálního[30] i ústavodárného[31] pojetí ochrany soukromí, jak jej známe v dnešní (české/evropské) společnosti. Toto pojetí rovněž do značné míry přebírá (zejména v podobě informačního sebeurčení, jak je popsáno dále, rovněž Evropský soud pro lidská práva i český Ústavní soud).

Na výše uvedené školy navázal rovněž např. Alan Westin, který stanovil tři úrovně vymezující soukromí: (i) politická, (ii) socio-kulturní a (iii) osobní.[32] Jednotlivec hraje ústřední roli ve všech těchto úrovních a soukromí lze tedy chápat jako určité vymezení okruhu daného jednotlivce, který určuje limity mezi ním samotným a okolním světem. Ač v zásadě kazuisticky, přesto podrobně a v dnešním vnímání přesně – na základě jednotlivých definičních prvků a vrstev – vymezuje soukromí Daniel Solove: (i) právo být ponechán o samotě, (ii) omezený přístup k osobě, (iii) tajemství, (iv) kontrola nad soukromými informacemi, (v) osobností a (vi) intimitou.[33]

1.2.1.3 Ochrana a význam soukromí v informační společnosti

Pro účely práva být zapomenut spojovaným zejména s moderními technologiemi, a tedy pro účely této práce, je významný zejména pohled na ochranu soukromí v moderní společnosti. Ačkoliv veškeré výše popsané doktrinální přístupy mají neodmyslitelně své místo pro definici soukromí v moderní informační společnosti,

[29] BORKOWSKI, S.C. Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching business ethics (Dordrecht) [online]. Dordrecht: Kluwer Academic Publishers, 1999, 3(4), 402-406 [cit. 2022-03-14]. ISSN 1382-6891. Dostupné z: doi:10.1023/A:1009843728384.

[30] FILIP, Jan. Úvodní poznámky k problematice práva na soukromí. In: Vojtěch ŠIMÍČEK, ed. Právo na soukromí. Brno: Masarykova univerzita, 2011, s. 9–19. ISBN 978-80-210-6449-3. ; WAGNEROVÁ, Eliška. Čl. 10 - Právo na soukromí v širším smyslu. In: Eliška WAGNEROVÁ, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL, ed. Listina základních práv a svobod - Komentář. Praha: Wolters Kluwer ČR, 2012, s. 277–300. ISBN 978-80-7357-750-6.

[31] Srov. zakotvení obecné záruky nedotknutelnosti soukromí osoby v čl. 7 odst. 1 LZPS doplněné zárukami jednotlivých aspektů soukromí (především čl. 10, čl. 12, čl. 13, čl. 15 odst. 1 LZPS).

[32] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 35.

[33] SOLOVE, Daniel J. a Taxonomy of Privacy. University of Pennsylvania law review [online]. Philadelphia: University of Pennsylvania Law School, 2006, 154(3), 477-564 [cit. 2022-03-14]. ISSN 0041-9907. Dostupné z: doi:10.2307/40041279.

je zjevné, že rozvoj technologií přináší zásadní výzvy a klade tak na vymezení soukromí zásadní akcent. Soukromí tak nelze vnímat jen jako jednoduchou, v prostoru vymezenou veličinu, nýbrž jako soubor různých vrstev a prvků, které jako celek vymezují jednotlivce a součást jeho osobnosti.

Přitom z výše popsaného vývoje je zjevné, že právě technologické změny a jejich vliv na soukromí, resp. možnosti zásahů do něj, jsou převážně tím, co historicky motivuje evoluci právní ochrany soukromí. Ačkoliv samozřejmě existují technologie, které rovněž berou v potaz zájem na ochrany soukromí[34], aktuální technologický vývoj neodmyslitelně směřuje k rozšiřování možností pro sdílení a uchovávání informací,[35] což zároveň zvyšuje možnosti a rizika zásahů do soukromí jednotlivců. Podle Kokeše pak prudký rozvoj informačních technologií (internet, elektronické komunikace, sociální sítě) vyvolal diskuzi nad potřebou rekonceptualizace práva na soukromí jednotlivců a přenesení jeho právní ochrany do tzv. kyberprostoru.[36] Moderní technologie rovněž významně posouvají rozsah ochrany soukromí, která se přesouvá od původní ochrany jednotlivce vůči státu[37] (ač ten je samozřejmě i nadále relevantní, a to zejména s přihlédnutím k možnostem státu nasazovat moderní technologie) do každodenního života – tím je tedy pak zejména využívání mobilních telefonů, internetu, ale i dalších nových technologií, jako jsou virtuální realita či např. umělá inteligence. Tyto technologie často vedou k nekontrolovanému (a často i nekontrolovatelnému) sběru dat[38], provázanosti informací, vyhledávání a jiných možností v analogovém světě často nepředstavitelných, které mohou zásadním způsobem narušit soukromí člověka.

---

[34] AUSLOOS, Jef. The 'Right to be Forgotten' – Worth remembering? Computer Law & Security Review. 2012, 28(2), 143–152. ISSN 0267-3649. s. 149.

[35] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5; CONLEY, Chris. The Right to Delete. AAAI Spring Symposium: Intelligent Information Privacy Management. 2010, 53–58. s. 53.

[36] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 329.

[37] Obdobně rovněž DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 555.

[38] Obdobně rovněž DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 555.

Z tohoto důvodu je nezbytné zkoumat funkce soukromí a to, jakou roli soukromí hraje v každodenním životě jednotlivce, a možnosti jeho ochrany.

Například podle Alana Westina existují čtyři základní funkce soukromí: (i) emocionální oddych, (ii) sebehodnocení, (iii) osobní autonomie a (iv) omezenost a důvěrnost komunikace.[39] Zatímco minimálně první dvě funkce jsou významným aspektem ochrany lidské osobnosti každého individua a jeho existence v lidské společnosti, včetně sociálního postavení a rozvoje jeho individuality, pro účely ochrany soukromí v moderní společnosti, tedy v souvislosti s právem být zapomenut, pak významně souvisí především čtvrtá funkce – omezenost a důvěrnost komunikace ve spojení s osobní autonomií jednotlivce.

Podle Westina se mezilidské vztahy vytvářejí v určitých kruzích, v jejichž středu stojí jádro a ochrana lidské osobnosti.[40] Ochrana tohoto jádra je významným předpokladem pro rozvoj nezávislé osobnosti a individuality jednotlivce, který bude schopen si utvářet vlastní názory – mimo okruh (široké) veřejnosti, či dokonce i okruh jeho nejbližších osob – resp. vždy v souladu s jeho soukromým rozhodnutím. Názory i postoje by měl být každý jednotlivec schopen si utvářet i měnit bez toho, aby byly předmětem kritiky jeho (širokého i blízkého) okolí a aniž by byl jednotlivec v případě, že své názory změní, označován za pokrytce.[41]

Veškeré názory a postoje by měl mít každý jednotlivec možnost projevovat pouze v takovém okruhu lidí, ve kterém se rozhodne. Záleží na něm, zda jde o soukromou korespondenci, vyjádření pro okruh přátel, nebo naopak zcela veřejný projev. Podle Westina existují dva fundamentální principy důvěrnosti komunikace: (i) možnost sdílení intimních záležitostí s blízkými osobami, s nimiž se jednotlivec na základě důvěrného vztahu rozhodl tyto záležitosti sdílet[42];

[39] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 35.

[40] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 36.

[41] SOLOVE, Daniel J. The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure. Duke law journal [online]. Duke University School of Law, 2003, 53(3), 967-1065 [cit. 2022-03-14]. ISSN 0012-7086.

[42] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 41.

(ii) možnost každého jednotlivce vytvářet si a udržovat hranice mentálního odstupu v mezilidských situacích – ať už se jedná o intimní vztahy jednotlivce, vztahy s přáteli nebo formální vztahy při vystupování na veřejnosti.[43]

Např. Charles Fried pak zdůrazňuje funkci soukromí založenou na kontrole nad soukromými informacemi, resp. považuje soukromí (a veškeré projevy jednotlivce) za určitý „morální kapitál“, s nímž jednotlivci nakládají a „obchodují“ (směňují). Tato směna pak tvoří základ jakýchkoliv mezilidských vztahů.[44] Zásadní význam podle Frieda hraje především kvalita, resp. povaha, sdílených informací, spolu s jejich množstvím.[45]

Z výše představených funkcí soukromí je zjevné, že každý má mít výhradní kontrolu nad tím, v jakém rozsahu, kde a jak bude sdílet projevy své osobní povahy, své názory a postoje. Tato kontrola nad vlastním soukromím, ochrana osobní autonomie i důvěrnosti a omezenosti komunikace jsou přitom zcela zásadní pro budování digitální existence jednotlivce v informační společnosti.

Pokud má jednotlivec právo určit rozsah a povahu sdílení informací o sobě sama, má tedy plnou kontrolu nad svým soukromím. a toto platí rovněž v digitálním světě, ve kterém má jednotlivec možnost kontrolovat rozsah svých aktivit. Přitom platí, že zejména v digitálním světě, resp. kyberprostoru lze koncept soukromí považovat za jeden z nejvíce se dynamicky rozvíjejících konceptů, ať již z hlediska judikaturního, tak i z hlediska právně teoretického (právně filozofického), byť vývojem nutně nemusí procházet koncept soukromí jako celek, nýbrž toliko jeden z jeho aspektů (dimenzí).[46]

[43] WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 42.

[44] FRIED, Charles. Privacy. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1968, 77(3), 475-493 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/794941.

[45] FRIED, Charles. Privacy. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1968, 77(3), 475-493 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/794941.

[46] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 329.

Soukromí v moderní době tak podléhá novým trendům, které „internetizace“ přináší.[47] Nové výzvy, které kyberprostor zasahující do všech aspektů lidského života přináší, jsou významné. Podle Kokeše totiž koncept soukromí do značné míry podléhá aktuálním (zejména politicky a kulturně podmíněným) představám společnosti o jeho obsahu, a i míře poskytované ochrany, přičemž tyto představy jsou začasté vyvolány např. potřebou reagovat na nějaký nový fenomén (typickým příkladem jsou tedy sociální sítě).[48] Rovněž podle Wagnerové technický a ekonomický pokrok přináší velký, dříve nemyslitelný a ohrožující potenciál.[49]

Právo na informační sebeurčení se rovněž postupně začalo blíže projevovat v rozhodovací praxi ESLP i Ústavního soudu, jak je blíže popsáno v kapitole 1.3.2.1.4 níže. V zásadě se pak jedná o možnosti jednotlivce kontrolovat vlastní soukromí, projevy osobní povahy a jejich další šíření a též možnost kontrolovat šíření jakýchkoliv informací a dat nesoucích osobnostní prvky, a to především, nikoliv však výlučně, v oblasti nových technologií.

1.2.2 Ochrana osobních údajů[50]

V rámci ochrany soukromí a vymezení institutu práva být zapomenut je rovněž nezbytné vnímat jeho podmnožinu – ochranu osobních údajů. Oblast ochrany

[47] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 330.

[48] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 329.

[49] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 279.

[50] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

WARREN, Samuel D. a BRANDEIS, Louis D. Right to privacy. Harv. L. Rev. 1890, 4, s. 193, dostupné online z https://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

osobních údajů je fenoménem často spojovaným s rozvojem technologií, zejména využíváním big data, umělé inteligence a dalších nových technologií.[51] To se rovněž odráží v komplexní právní úpravě této oblasti, která se z původní, velmi marginální právní oblasti stala samostatnou a svébytnou právní disciplínou.[52]

Oblast ochrany osobních údajů je přitom specifickou oblastí na přelomu soukromého a veřejného práva[53], kde přesahy do oblasti veřejného práva jsou dané zejména kontrolou této oblasti ze strany dozorových orgánů a možnosti uplatňování veřejnoprávních sankcí – ať už z hlediska správního práva[54], nebo práva trestního[55]. Ochrana osobních údajů v poslední dekádě celosvětově prodělala značný rozmach, o čemž svědčí rovněž přijetí komplexního právního předpisu na úrovni Evropské unie – obecného nařízení o ochraně osobních údajů, které je v českém (právním i laickém) prostředí často označované jako GDPR z anglického *General Data Protection Regulation*. Vzhledem k tomu, že se jedná o nařízení (tj. přímo aplikovatelný právní předpis Evropské unie), zajišťuje vysokou míru unifikace aplikace práva napříč všemi členskými státy EU. Dosavadní roztříštěnost aplikace pravidel napříč členskými státy byl přitom jeden z hlavních důvodů, který vedl evropského zákonodárce k tomu, aby nový právní rámec ochrany osobních údajů byl přijat jako nařízení, a ne jako směrnice, jako tomu bylo do přijetí GDPR, které tedy nahradilo dosavadní směrnici 95/46/ES.

Bod 6 úvodních ustanovení obecného nařízení o ochraně osobních údajů jako důvody přijetí nařízení uvádí rychlý rozvoj technologií a globalizaci a související významný nárůst rozsahu shromažďování a sdílení osobních údajů, jakož i možnosti využívat osobní údaje v nebývalém rozsahu, které technologie

[51] K tomu např. USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

[52] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 350.

[53] K tomu např. KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0, s. 2.

[54] K tomu tedy zejména ochrana poskytovaná obecným nařízením o ochraně osobních údajů ve spojení s českým zákonem o zpracování osobních údajů.

[55] Tedy ochrana dle trestního zákoníku, zejména pak § 180 (neoprávněné nakládání s osobními údaji), § 182 (porušení tajemství dopravovaných zpráv), § 183 (porušení tajemství listin a jiných dokumentů uchovávaných v soukromí)

dávají soukromým společnostem a orgánům veřejné moci.[56] Ambicí obecného nařízení o ochraně osobních údajů je tak nejen upravit současný stav zpracovávání osobních údajů, ale vytvořit právní rámec pro rozvoj digitální ekonomiky do budoucna tak, aby poskytovala fyzickým osobám kontrolu nad jejich údaji a v konečném důsledku podporovala důvěru založenou na vymahatelnosti práva v oblasti digitální ekonomiky. GDPR je v současné době jednou z nejkomplexnějších právních úprav ochrany soukromí na světě a je pravděpodobné, že ovlivní tuto oblast práva v řadě zemí.

V oblasti technologií a ochrany soukromí v informační společnosti a elektronických komunikacích je významná úprava obsažená v tzv. *ePrivacy* směrnici, která harmonizovala ochranu osobních údajů při používání telekomunikačních služeb, internetu a jiných nových technologií. Zároveň se předpokládá, že tato směrnice bude nahrazena novým nařízením na ochranu osobních údajů v el. komunikacích (tzv. *ePrivacy Regulation*)[57], které bude doplňovat a specifikovat ochranu poskytovanou tímto nařízením (ačkoliv původní předpoklady byly, že *ePrivacy Regulation* nabude účinnosti spolu s GDPR, tj. 25. května 2018, v době uzávěrky tohoto textu nebylo stále známé konečné znění tohoto nového nařízení, ani datum, kdy by mělo dojít k jeho konečnému přijetí. Na přijetí tohoto nařízení nepanuje napříč EU politický konsensus a stále dochází k odsouvání jeho schválení.

[56] *„Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Fyzické osoby stále častěji své osobní údaje zveřejňují, a to i v globálním měřítku. Technologie změnily ekonomiku i společenský život a měly by dále usnadňovat volný pohyb osobních údajů v rámci Unie a předávání do třetích zemí a mezinárodním organizacím a zároveň zajistit vysokou úroveň ochrany osobních údajů.“* bod 6 úvodních ustanovení GDPR.

[57] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU a RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), dostupný z https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017PC0010&from=EN.

1.3 Právní úprava ochrany soukromí a osobních údajů

1.3.1 Právo Evropské unie

1.3.1.1 Primární právo Evropské unie[58]

Na úrovni Evropské unie je právo na soukromí a ochranu osobních údajů chráněno na úrovni primárního i sekundárního práva.

Článek 6 odst. 3 Smlouvy o Evropské unii (SEU) výslovně zakotvuje ochranu všech základních práv, která jsou zaručena Úmluvou o ochraně lidských práv a základních svobod vydanou Radou Evropy v roce 1950 a která vyplývají z ústavních tradic společných členským státům a tvoří obecné zásady práva Unie. Tím se evropské primární právo výslovně přihlásilo k aplikaci všech základních práv a svobod zajištěných v Úmluvě, včetně práva na ochranu soukromí ve smyslu čl. 8 Úmluvy.

Z hlediska evropského primárního práva je hlavním předpisem poskytujícím ochranu osobních údajů Listina EU. Ta v článku 7 deklaruje, že každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace. Zároveň podle článku 8 Listiny EU má každý právo na ochranu osobních údajů, které se ho týkají, přičemž tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem (členského státu). Listina EU rovněž každému přiznává právo na přístup k údajům, které o něm byly shromážděny, a právo na jejich opravu. Listina EU tak výslovně zakotvuje ochranu osobních údajů jako základní lidské právo a jde tak nad rámec obecné ochrany soukromí,

[58] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

kterou poskytují ostatní předpisy týkající se ochrany osobních údajů. Listina EU výslovně neomezuje svou věcnou působnost a z podstaty evropského předpisu tak chrání primárně občany EU. Podle stávajících výkladů však chrání i občany třetích států (obdobně jako dnes GDPR). Listina EU rovněž výslovně neomezuje svou působnost jen na fyzické osoby. Toto aplikační omezení pouze na fyzické osoby je v souvislosti s ochranou soukromí dovozováno na základě běžného chápání pojmu „soukromí“, které nezahrnuje soukromí právnických osob.

Článek 6 odst. 1 SEU dále stanoví, že EU uznává práva, svobody a zásady obsažené v Listině základních práv EU (Listina EU) ze dne 7. prosince 2010, která byla původně vyhlášená jako součást Smlouvy o Ústavě pro Evropu. Díky přijetí Lisabonské smlouvy se tak Listina EU v zásadě stala součástí primárního práva EU.

Dále článek 16 Smlouvy o fungování Evropské unie (SFEU) stanoví, že každý má právo na ochranu osobních údajů, které se jej týkají. Čl. 16 odst. 2 SFEU pak zplnomocňuje Evropský parlament a Radu k tomu, aby přijaly pravidla o zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie.

1.3.1.2 Sekundární právo Evropské unie[59]

S ochranou soukromí a ochranou osobních údajů souvisí celá řada právních norem, a to v oblasti sekundárního práva EU i v národní úpravě členských států.

V oblasti práva Evropské unie se jedná především o obecné nařízení o ochraně osobních údajů, rozsah, jehož působnosti je blíže rozebrán v kapitole 3 níže. Dále

[59] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

se pro oblast technologií jedná o úpravu obsaženou v tzv. *ePrivacy* směrnici, která je v relevantních oblastech implementovaná především v zákoně o elektronických komunikacích[60] a v zákoně o některých službách informační společnosti[61] a která má být do budoucna nahrazena novým nařízením na ochranu osobních údajů v el. komunikacích (tzv. *ePrivacy Regulation*). Rovněž nelze opomenout např. nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018, které upravuje zpracování osobních údajů orgány, institucemi a jinými subjekty Unie a volný pohyb těchto údajů, a veškeré další legislativní iniciativy Evropské unie v oblasti nových technologií a nakládání s daty, jakou jsou např. připravovaný tzv. Data Act[62] nebo Data Governance Act[63].

1.3.1.3 Význam výkladových stanovisek – evropského soft-law[64]

Pro výklad právních předpisů v oblasti ochrany osobních údajů (zejména tedy obecného nařízení o ochraně osobních údajů) jsou pak velmi zásadní výkladová stanoviska přijímaná Evropským sborem pro ochranu osobních údajů (tzv. *European Data Protection Board*), který byl ustanoven článkem 68 GDPR a který tak navázal na předcházející činnost poradní komise zřízené podle čl. 29 směrnice 95/46/ES. Tato výkladová stanoviska jsou zásadní pro sjednocující aplikaci pravidel ochrany osobních údajů, a to i s přihlédnutím k rychlému vývoji nových technologií, které zpravidla s osobními údaji nakládají a na které zákonodárce nemůže dostatečně pružně reagovat. Ačkoliv jsou tak tato výkladová stanoviska nezávazná, jednotlivé dozorové úřady v členských státech (které jsou

[60] Srov. především § 87 an. zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[61] Srov. zejména § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

[62] Data Act: Commission proposes measures for a fair and innovative data economy. [online]. 23.2.2022. [cit. 2022-04-05]. Dostupné z https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[63] Návrh nařízení Evropského parlamentu a Rady o evropské správě dat. [online]. 25.11.2020. [cit. 2022-04-05]. Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.

[64] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 30 - 37.

zároveň v Evropském sboru pro ochranu osobních údajů zastoupeny a mohou se tak podílet na jejich tvorbě) obvykle postupují v souladu s těmito stanovisky a pravidla obecného nařízení o ochraně osobních údajů a souvisejících předpisů tedy aplikují podle těchto stanovisek. To je samozřejmě významný signál pro recipienty právních norem a právní jistotu v této oblasti. Pro rozsah této práce lze namátkou zmínit např. Pokyny č. 5/2019 ke kritériím práva být zapomenut v případech vyhledávačů podle nařízení GDPR[65].

V souvislosti s právní úpravou ochrany osobních údajů v oblasti nových technologií nelze opomenout Pravidla ochrany soukromí a přeshraničních toků osobních údajů vydaná v roce 1980 OECD. Ta vůbec jako první definovala dnes běžně používané pojmy „osobní údaj", „správce" či „subjekt údajů" a taktéž zakotvila základní zásady a principy ochrany osobních údajů, na kterých právní úprava stojí dodnes a které nalezneme i v čl. 5 GDPR. Tento dokument OECD však nebyl právně závazný a jednalo se jen o doporučení (guidelines) pro členské státy OECD. Smyslem těchto Pravidel bylo vytvořit rovnováhu mezi ochranou soukromí fyzických osob a volným obchodem, aby nedocházelo k vytváření bariér omezujících volný pohyb dat přes národní hranice. Pravidla nijak nerozlišovala mezi soukromým a veřejným sektorem ani mezi automatizovaným a neautomatizovaným zpracováním osobních údajů. Chráněny měly být takové údaje, jejichž zpracování by mohlo představovat nebezpečí pro soukromí a svobody jednotlivce.

1.3.2 Český právní řád

1.3.2.1 Ústavněprávní ochrana soukromí a osobnosti

1.3.2.1.1 Koncepce ochrany osobnosti a soukromí v ústavněprávním pořádku

Na úrovni ústavního práva zakotvuje ochranu soukromí Listina základních práv a svobod České republiky (LZPS). Součástí českého právního řádu jsou rovněž

[65] Pokyny č. 5/2019 ke kritériím práva být zapomenut v případech vyhledávačů podle nařízení GDPR (část 1), verze 2.0, přijato dne 7. července 2020, v českém znění dostupné z https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_cs.pdf.

lidskoprávní mezinárodní smlouvy[66] (díky tzv. generální inkorporaci dle čl. 10 Ústavy), které se tak stávají součástí ústavního pořádku[67] a mají aplikační přednost před zákonem.[68] Specifické postavení má v tomto ohledu Listina EU, na kterou lze hledět buď jako na součást práva EU, kdy by však netvořila součást českého ústavního pořádku, nebo jako na mezinárodní smlouvu o lidských právech, kdy se rovněž stane na základě čl. 10 Ústavy, součástí ústavněprávního pořádku.[69] Toto rozlišení nicméně není pro další aplikaci a výklad v této práci nijak zásadní.

Soukromí a osobnost jsou tak na ústavní úrovni chráněny v několika rovinách: Článek 7 LZPS zaručuje nedotknutelnost osoby a jejího soukromí, čl. 10 LZPS zakotvuje ochranu soukromého a rodinného života a článek 13 LZPS dále chrání listovní tajemství (včetně zpráv předávaných telefonem a jinými technologiemi). Tím se navzájem doplňují (a překrývají) s ochranou poskytovanou podle čl. 7 a 8 Listiny EU a podle čl. 8 Úmluvy.

Ačkoliv jednotlivé lidskoprávní smlouvy anebo LZPS poskytují lidským právům ochranu v různé systematice, na samostatnou interpretaci ochrany soukromí zásadní vliv nemají[70], jelikož, jak zdůrazňuje např. Ústavní soud *„onu ‚roztříštěnost' právní úpravy aspektů soukromé sféry jednotlivce nelze přeceňovat a v Listině uvedený výčet toho, co je třeba podřadit pod ‚deštník' práva na*

[66] K tomu viz kapitola 2.2.1 níže.

[67] K tomu např. BARTOŇ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 7.

[68] K tomu např. BARTOŇ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 6.

[69] K tomu např. BARTOŇ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 9.

[70] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 332.

soukromí či na soukromý život, nelze považovat za vyčerpávající a konečný."[71] Tato práva jsou pak rozvinuta na úrovni občanského zákoníku (§ 81 a násl. o.z.).[72]

1.3.2.1.2 Nedotknutelnost osoby ve smyslu čl. 7 LZPS

Článek 7 odst. 1 LZPS[73] zaručuje nedotknutelnost osoby a jejího soukromí. Spojení tělesné a duševní integrity člověka s právem na soukromí přitom není zcela standardním pojením lidskoprávní ochrany a nemá jednoznačnou oporu v jiných lidskoprávních dokumentech.[74] Spojitost těchto dvou práv je nicméně velmi úzká, což se projevuje rovněž v rozhodovací praxi nejvyšších, ústavních i mezinárodních soudů[75], které při absenci explicitních ustanovení o respektování tělesné a duševní integrity člověka poskytují těmto hodnotám ochranu právě prostřednictvím práva na soukromí.[76]

Pro výklad spojení integrity člověka a nedotknutelnosti soukromí pak existují dva hlavní přístupy[77]: (i) pojem soukromí nemá v systematice integrity a nedotknutelnosti jednotlivce svůj samostatný význam[78], nebo (ii) méně se vyskytující přístup[79], podle kterého je nedotknutelnost jednotlivce ve smyslu čl. 7 LZPS i garancí ochrany soukromí, jehož jednotlivé aspekty (jako ochrana

[71] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

[72] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 289.

[73] Článek 7 odst. 1 LZPS: *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."*

[74] LANGÁŠEK, T. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 186.

[75] Srov. např. ESLP při výkladu čl. 8 Úmluvy v rozsudku ze dne 8. listopadu 2011 ve věci 18968/07 - Glass proti Spojenému království.

[76] LANGÁŠEK, T. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 187.

[77] NECHVÁTALOVÁ, L. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 225.

[78] K tomu např. nález Ústavního soudu ze dne 8. června 2010, sp. zn. Pl. ÚS 3/09, nebo nález Ústavního soudu ze dne 27. února 2019, sp. zn. IV ÚS 774/18.

[79] NECHVÁTALOVÁ, L. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 226.

soukromého života, osobních údajů, domovní svobody, tajemství telefonem sdělovaných zpráv apod.) jsou pak zároveň chráněny v následujících článcích Listiny.[80]

Pavlíček rovněž uzavírá, že článek 7 poskytuje ochranu pouze fyzickým osobám[81], pro ochranu právnických osob pak slouží právě článek 10 LZPS.[82]

1.3.2.1.3 Ochrana osobnosti a soukromí dle čl. 10 LZPS

Článek 10 odst. 1 LZPS zakotvuje nedotknutelnost lidské důstojnosti, osobní cti, dobré pověsti a jména, což dále doplňuje odst. 2, který poskytuje ochranu před neoprávněným zasahováním do soukromého života. Článek 10 odst. 3 LZPS pak poskytuje ochranu tzv. právu na informační sebeurčení (blíže rozebrané v následující kapitole).

Článek 10 odst. 1 se věnuje osobní soukromé sféře[83], která je charakterizována zejména tzv. osobnostními právy – tj. především právo na lidskou důstojnost, osobní čest, dobrou pověst a jméno[84]. Toto vymezení nutně nemusí odpovídat tradičnímu civilistickému pojetí[85], což výslovně popírá pojetí ochrany osobních práv v občanském zákoníku.[86] Na prvním místě této klauzule je zdůrazňována lidská důstojnost sloužící jako východisko veškerých základních práv[87], což je rovněž v souladu s čl. 1 Listinou EU, který stanoví, že *„Lidská důstojnost je*

[80] K tomu např. nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

[81] K tomu rovněž např. usnesení Ústavního soudu ze dne 26. dubna 2016, sp. zn. I. ÚS 971/16.

[82] PAVLÍČEK, Václav, Ján GRONSKÝ, Jiří HŘEBEJK, et al. Ústavní právo a státověda. II. díl, Ústavní právo České republiky. 3. vydání. Praha: Leges, 2020, 1160 s. ISBN 978-80-7502-468-8, s. 524.

[83] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 282.

[84] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 282.

[85] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 282.

[86] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 337.

[87] PAVLÍČEK, Václav, Ján GRONSKÝ, Jiří HŘEBEJK, et al. Ústavní právo a státověda. II. díl, Ústavní právo České republiky. 3. vydání. Praha: Leges, 2020, 1160 s. ISBN 978-80-7502-468-8, s. 528.

nedotknutelná“. Úprava v čl. 10 odst. 1 spolu s garancí autonomie vůle jednotlivce (čl. 2 odst. 3 LZPS) slouží jako generální klauzule zajišťující bezmezerovitou ochranu svobody jednotlivce.[88]

Podle Kokeše je úprava čl. 10 odst. 2 LZPS (tj. právo na soukromý a rodinný život) – nejvíce se překrývající s s ochranou poskytovanou podle čl. 8 Úmluvy – nejzřetelnější ukázkou roztříštěného charakteru práva na soukromí poskytované v LZPS. Nicméně se významně překrývají a v doktrinální i rozhodovací praxi jsou používány a chráněny *promiscue (right to privacy, right to private social life).*[89] Tento překryv zároveň vychází z mnohovrstevnatosti pojmu a funkce soukromí[90], kde tedy právo na soukromí je více spojováno s individuální svobodou a identitou jednotlivce, zatímco ochrana skrze právo na soukromý život cílí více na garanci soukromí jednotlivce sloužící k seberealizaci v rámci společenských vztahů (v interakci s okolím, včetně veřejné moci); toto rozlišení je ovšem primárně teoretické a pro ochranu všech aspektů práva na soukromí, resp. soukromého života by nemělo hrát zásadní význam.[91] Wagnerová pak zároveň vnímá zásadní překryv s právem na informační sebeurčení (které je však primárně upravené na úrovni čl. 10 odst. 3 LZPS, jak je popsáno dále) a jakožto součást ochrany soukromého a rodinného života pak vnímá rovněž právo autonomního rozhodování a osobní integritě.[92]

1.3.2.1.4 Právo na informační sebeurčení

Pro účely práva být zapomenut a této práce je pak velmi významné právo na informační sebeurčení (obecně rovněž vymezené v kapitole 1.2.1.3), které je chráněno podle čl. 10 odst. 3 LZPS, coby jeden z aspektů (dimenzí) práva

[88] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 336.

[89] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 345.

[90] K tomu srov. zejména kapitolu 1.2.1.1 výše.

[91] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 345.

[92] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 284.

na soukromí), resp. práva na ochranu soukromého života[93]. Jedná se tedy v zásadě o možnost kontroly jednotlivce nad vlastním soukromím, projevy osobní povahy a jejich dalšího šíření a kontrolu nad šířením jakýchkoliv informací a dat nesoucích osobnostní prvky, a to především, nikoliv však výlučně, v oblasti nových technologií.

Toto právo dává jednotlivcům možnost rozhodnout podle vlastního uvážení zda mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům, popřípadě v jakém rozsahu, jakým způsobem a za jakých okolností.[94] Toto právo na informační sebeurčení současně patří k těm aspektům (sférám) práva na soukromí, které nejvíce čelí dopadům současného dynamického technologického vývoje ve společnosti.[95] Solove v této souvislosti rovněž představuje koncept tzv. digitální osoby (angl. *digital person*): *„na internetu je v současné době, právě díky elektronizaci a internetizaci běžných společenských procesů a činností, o každém z nás, jakožto digitálních jedincích, veden tzv. digitální spis, v němž jsou ve formě 0 a 1 uchovávána a zahrnuta veškerá námi poskytnutá data a datové soubory s informacemi o nás a našem soukromí, které jsou na internetu (s naším souhlasem a vědomím či bez nich) zpřístupněny a které jsou pomocí internetových vyhledávačů i snadno dohledatelné. Souhrny takto nasbíraných dat jsou způsobilé zmapovat ‚lidskoprávní genom' jednotlivce, který zahrnuje informace nejintimnější, profesní, obchodní, účast na veřejném životě, společenské aktivity, prostě celý lidský profil."*[96]

Wagnerová pak v souvislosti s právem na informační sebeurčení zdůrazňuje, že se neomezuje jen na vybranou soukromou sféru, ale naopak konzumuje i právo

[93] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 347.

[94] K tomu srov. např Nález Ústavního soudu ze dne 17. července 2007, sp. zn. IV. ÚS 23/05., nález Ústaního soudu ze dne 1. prosince 2008, sp. zn. I. ÚS 705/06, nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, nález Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11, či nález Ústavního soudu ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17.

[95] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 348.

[96] Solove, D. J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004, s. 2.

na ochranu před sledováním, hlídáním a pronásledováním především ze strany veřejné moci i veřejném prostoru či veřejně přístupných místech.[97] To může být relevantní zejména v oblasti sledování veřejného prostoru kamerovými systémy[98] nebo na internetu[99].

Ochranu informačního aspektu soukromí, resp. právo na informační sebeurčení, potvrdil rovněž Evropský soud pro lidský práva[100] jako součást čl. 8 Úmluvy, když, kromě jiného, stanovil, že „*koncept soukromého života zahrnuje též soukromé informace, o nichž jednotlivci mohou legitimně předpokládat, že nebudou bez jejich souhlasu zveřejněny*“[101]. Právo na informační sebeurčení pak explicitně ESLP vyjádřil např. v rozsudku Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku.[102]

[97] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 284.

[98] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 284.

[99] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 348.

[100] Srov. např. rozsudek ESLP ze dne 4. května 2000 ve věci č. 28341/95 - Rotaru proti Rumunsku nebo rozsudek ESLP ze dne 4. prosince 2008 ve věci 30562/04 - S. a Marper proti Spojenému království.

[101] Rozsudek ESLP ze dne 12. října 2010, ve věci 184/06 - Saaristo a ostatní proti Finsku.

[102] „*Ochrana osobních údajů je nepostradatelná pro možnost jednotlivce využívat svého práva na respekt k soukromí a rodinnému životu, jak jej garantuje článek 8 Úmluvy. Národní právo musí poskytovat dostatečné záruky před užíváním osobních údajů v rozporu s tímto článkem. Článek 8 Úmluvy tedy explicitně zahrnuje právo na určitou formu informačního sebeurčení, čímž jednotlivcům umožňuje spoléhat se na právo na soukromí v souvislosti s jejich osobními údaji […].*“ in rozsudek ESLP ze dne 27. června 2017 ve věci č. 931/13 - Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku.

1.3.2.2 Zákonná ochrana soukromí[103]

Ochrana soukromí a osobnosti je v českém právním řádu upravena napříč různými předpisy i právními odvětvími.

Soukromoprávní ochranu podoby a soukromí jednotlivce upravuje především občanský zákoník – jako ochranu osobnostních práv ve smyslu § 81 a násl. o. z. (k tomu viz kapitola 2 této práce) či náhradu újmy vzniklé zásahem do soukromí podle § 2956 o. z., zákaz dotěrného obtěžování jako úpravu nekalé soutěže (srov. § 2989 o. z.).

Soukromí je chráněné rovněž trestním právem, kde Hlava II, díl 2 trestního zákoníku vymezuje trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství (§ 180 a násl.). Specifická skutková podstata trestného činu neoprávněného nakládání s osobními údaji dle § 180 tr. zákoníku chrání osobní údaje shromážděné v souvislosti s výkonem veřejné moci a chráněné státem uloženou nebo uznanou povinností mlčenlivosti. Všech těchto trestných činů se navíc může dopustit i právnická osoba (ve smyslu zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim), nikoliv však stát či samosprávný celek.

Dalšími předpisy upravujícími ochranu soukromí jsou např. zákoník práce, občanský zákoník, zákon o el. komunikacích, zákon o některých službách informační společnosti, tiskový zákon, zákon o svobodném přístupu k informacím aj. V případě, že národní předpisy jakýmkoliv způsobem upravují otázky nakládání s osobními údaji, jejich výklad a aplikace by měly vždy probíhat v souladu s nařízením a ZZOÚ. Občanský zákoník, ZZOÚ a obecné nařízení

---

[103] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 30 – 37 a dále na s. 499 - 505.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHELANOVÁ, M. Účinky unijního práva ve světle judikatury Soudního dvora. 2011. Dostupné z https://www.mvcr.cz/clanek/ucinky-unijniho-prava-ve-svetle-judikaturysoudniho-dvora.aspx.

o ochraně osobních údajů tak vytvářejí obecný právní rámec pro ochranu soukromí a osobních údajů.

Subsidiárně se uplatní vůči speciálním zákonům, nicméně oblast ochrany soukromí a osobních údajů zcela nevyčerpávají, tato oblast je upravena dalším množstvím zákonů; těmi jsou zejména[104]:

Pro oblast **občanského práva hmotného a procesního** (zákon č. 89/2012 Sb., občanský zákoník, zákon č. 99/1963 Sb., občanský soudní řád, zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)). Pro **oblast pracovního práva** (zákon č. 262/2006 Sb., zákoník práce, zákon č. 435/2004 Sb., o zaměstnanosti, zákon č. 234/2014 Sb., o státní službě). Pro oblast právní úpravy **informační společnosti** (zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce). Pro úpravy **svobody sdružování** (zákon č. 424/1991 Sb., o sdružování v politických stranách a v politických hnutích, zákon č. 3/2002 Sb., o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů (zákon o církvích a náboženských společnostech)). Pro oblast **trestního práva** (zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), zákon č. 40/2009 Sb., trestní zákoník, zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosu z trestné činnosti a financování terorismu, zákon č. 269/1994 Sb., o Rejstříku trestů, zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů). Pro oblast **práva správního** (zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, zákon č. 251/2016

[104] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s 3 - 6.

Sb., o některých přestupcích, zákon č. 500/2004 Sb., správní řád, zákon č. 150/2002 Sb., soudní řád správní). V oblasti **veřejnoprávní kontroly** (zákon č. 159/2006 Sb., o střetu zájmů nebo zákon č. 255/2012 Sb., o kontrole (kontrolní řád)). V rámci právní úpravy **veřejnoprávních databází** (zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)), zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů, zákon č. 111/2009 Sb., o základních registrech, zákon č. 158/1999 Sb., o sčítání lidu, domů a bytů v roce 2001, zákon č. 296/2009 Sb., o sčítání lidu, domů a bytů v roce 2011). V rámci úpravy **svobodného přístupu k informacím** (zákon č. 106/1999 Sb., o svobodném přístupu k informacím nebo zákon č. 123/1998 Sb., o právu na informace o životním prostředí). V rámci úpravy **finanční trhu a dohledu** nad ním (zákon č. 21/1992 Sb., o bankách, zákon č. 6/1993 Sb., o České národní bance, zákon č. 37/2004 Sb., o pojistné smlouvě a o změně souvisejících zákonů (zákon o pojistné smlouvě), zákon č. 277/2009 Sb., o pojišťovnictví). V oblasti **daní, účetnictví a poplatků** (zákon č. 586/1992 Sb., o daních z příjmů, zákon č. 235/2004 Sb., o dani z přidané hodnoty, zákon č. 563/1991 Sb., o účetnictví, zákon č. 280/2009 Sb., daňový řád, zákon č. 565/1990 Sb., o místních poplatcích, zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), zákon č. 634/2004 Sb., o správních poplatcích, zákon č. 17/2012 Sb., o Celní správě České republiky). V oblasti **zdravotní a sociální** (zákon č. 187/2006 Sb., o nemocenském pojištění, zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), zákon č. 373/2011 Sb., o specifických zdravotních službách, zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí).

V **oblasti bezpečnostní** (zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon č. 553/1991 Sb., o obecní policii, zákon č. 153/1994 Sb., o zpravodajských službách České republiky, zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, zákon č. 222/1999 Sb., o zajišťování obrany České republiky, zákon č. 289/2005 Sb., o Vojenském zpravodajství, zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii)).

Neméně důležitá je pak rovněž ochrana poskytovaná při využívání technologií **cloud computingu** ze strany orgánů veřejné správy, která je upravena zejména v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů a jeho prováděcí vyhlášce – tzv. cloudové vyhlášce č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, vyhláška č. 433/2020 Sb.

1.3.2.3 Český zákon o zpracování osobních údajů[105]

Zákon o zpracování osobních údajů formálně nahradil dosavadní zákon č. 101/2000, který v českém právním řádu transponoval směrnici 95/46/ES a který se uplatnil i po přechodnou dobu za účinnosti nařízení. Přijetím ZZOÚ tak došlo k odstranění přechodné souběžnosti nařízení a ZOOÚ a zároveň k odstranění výkladových a kompetenčních nejasností, kterými se zabýval i Nejvyšší správní soud.[106]

Zákon o zpracování osobních údajů lze zároveň chápat jako prováděcí předpis k obecnému nařízení o ochraně osobních údajů. Nedochází tak k nedovolené

[105] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 556 - 561.

[106] Rozsudek Nejvyššího správního soudu ze dne 9. 8. 2018, sp. zn. 9 Azs 49/2018 – 50, který vyjasnil, že ZOOÚ se použije po přechodnou dobu od nabytí účinnosti nařízení do přijetí adaptačního zákona.

implementaci a transpozici evropského nařízení, což by bylo v rozporu s judikaturou Soudního dvora Evropské unie. Rovněž důvodová zpráva tohoto zákona předpokládá, že v budoucnu bude dalším zapracovaným příslušným předpisem i nařízení týkající se ochrany údajů v elektronických komunikacích (tj. tzv. nařízení *ePrivacy Regulation*, které má rovněž doplňovat úpravu GDPR), které jsou dnes v relevantních oblastech v zákoně o elektronických komunikacích[107] a v zákoně o informačních službách informační společnosti[108], jež implementují tzv. *ePrivacy* směrnici.

Zákon o zpracování osobních údajů, stejně jako obecné nařízení o ochraně osobních údajů, chrání právo na soukromí ve formě ochrany osobních údajů (rovněž se zaměřuje na ochranu soukromí jako jeden z prvků ochrany osobnosti chráněné jako jedno ze základních lidských práv).

Obecně pak platí, že pokud by některá ustanovení ZZOÚ byla v rozporu s nařízením, na základě aplikační přednosti převáží pravidla stanovená nařízením (k tomu srov. komentář k čl. 1 odst. 2 GDPR). To však neplatí pro implementaci směrnice 2016/680 (Hlava III ZZOÚ), zde se uplatní pouze pravidla pro výklad směrnic.

Směrnice nejsou obecně přímo účinným právním předpisem a nelze se jich přímo dovolávat. Judikatura Soudního dvora nicméně za určitých podmínek stanovila i přímý účinek směrnic, který nastává zejména v případě, kdy členský stát v transpoziční lhůtě vůbec směrnice netransponuje (tj. po marném uplynutí transpoziční lhůty); v případě směrnice 2016/680 tak bylo možné zvažovat její přímou aplikaci zejména v mezidobí od 6. května 2018, kdy měla být nejpozději transponována, do nabytí účinnosti ZZOÚ. Přímý účinek směrnice nastává rovněž v případě, že členský stát danou směrnici transponuje či implementuje nesprávně a pravidla stanovená ve směrnici jsou sama o sobě jasná, přesná a bezpodmínečná, tedy k naplnění účelu směrnice není nutný další prováděcí

[107] Srov. především § 87 an. zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[108] Srov. zejména § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

předpis (k tomu zejména rozsudek ve věci Marshall[109]). Přímý účinek směrnice je obvykle vertikální, tj. jednotlivec se může dovolávat svých práv vyplývajících ze směrnice proti příslušnému členskému státu, který směrnici netransponoval či ji transponoval nesprávně. Soudní dvůr historicky dovodil i horizontální přímý účinek směrnic.[110]

Pro výklad hlavy III ZZOÚ rovněž přichází v úvahu tzv. nepřímý účinek směrnice. Pokud tak budou některá ustanovení hlavy III ZZOÚ nejasná či mohou nabízet dvojí různý výklad, soudy jsou povinny vykládat tyto vnitrostátní normy eurokonformně, tj. ve světle znění a účelu směrnice 2016/680 a jí poskytovaných práv, a to takovým způsobem, aby byl vždy upřednostněn z možných výkladů vnitrostátního práva takový, který nejlépe umožní zajistit efektivitu unijního práva.

Zákon o zpracování osobních údajů nejen provádí nařízení do českého právního řádu, ale zároveň implementuje směrnici 2016/680 upravující zpracování osobních údajů v rámci policejní a justiční spolupráce v trestních věcech. Ta nahradila dosavadní úpravu, která byla zakotvena v rámcovém rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech (které se v českém právní řádu promítlo především v rámci zákonů o Policii České republiky, o Vojenské policii, o Celní správě České republiky nebo v rámci trestního řádu – srov. zejména zákon č. 150/2011 Sb.). ZZOÚ tak slouží jako komplexní předpis v oblasti ochrany osobních údajů, který vedle nařízení dopadá na veškeré zpracovatelské operace na území České republiky. Nejedná se však zdaleka o jediné předpisy, které se dotýkají zpracování osobních údajů a práva na soukromí obecně. Úprava se (kazuisticky) promítá do dílčích právních předpisů, které upravují konkrétní oblasti; jejich demonstrativní výčet je k dispozici v předchozí kapitole.

[109] Rozsudek SDEU ze dne 26. února 1986 ve věci 152/84, M. H. Marshall v. Southampton and South-West.

[110] Rozsudek SDEU ze dne 26. února 1986 ve věci 152/84, M. H. Marshall v. Southampton and South-West.

1.4 Kolize práva na ochranu soukromí s ostatními lidskými právy

1.4.1 Proporcionalita výkladu základních lidských práv

Právo na ochranu soukromí (a osobních údajů) je nezbytné vykládat v kontextu ostatních základních práv, která jsou garantována Listinou EU. Jak vyplývá z článku 52 odst. 1 Listiny EU[111], každé základní právo musí být vykládáno proporcionálně vůči ostatním právům. Podle článku 54 Listiny EU pak platí, že žádné právo a jeho ochrana nemůžou být zneužity na úkor ostatních práv, které Listina EU chrání. [112]

Při omezení jakéhokoliv základního práva – v tomto případě práva na soukromí, resp. tedy osobnostních práv – je určujícím princip proporcionality, na jehož základě je zkoumána přiměřenost učiněných omezení (zásahů).[113] Test proporcionality pak probíhá na základě tří dílčích příkazů: (i) vhodnost (způsobilost) prostředku pro dosažení určitého účelu (cíle), (ii) potřebnost (nutnost) použití právě a jenom vybraného prostředku, (iii) proporcionalita (v užším slova smyslu) neboli přiměřenost vybraného prostředku v relaci k dotčenému právnímu statku – základnímu právu.[114]

Právo na ochranu soukromí (resp. obecně osobnostní práva) je v judikatuře Ústavního soudu i ESLP (ale i obecných) nejčastěji řešeno v kolizi s právem

[111] Podle článku 52 odst. 1 Listiny EU platí, že *„každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.“*

[112] Podle článku 54 Listiny EU platí, že „*žádné ustanovení této listiny nesmí být vykládáno tak, jako by dávalo jakékoli právo vyvíjet činnost nebo dopustit se činu zaměřeného na zmaření kteréhokoli z práv a svobod uznaných v této listině nebo na jejich omezení ve větším rozsahu, než tato listina stanoví.“*

[113] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 125.

[114] BARTOŇ in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 26 a 27.

na svobodu projevu[115] a právem na informace, které jsou chráněny dle čl. 11 Listiny EU[116] a stejně tak v českém právním řádu dle čl. 17[117] Listiny.[118]

Tato práce vychází rovněž z obdobné premisy, kdy se právo být zapomenut vymezuje primárně jako součást ochrany soukromí (ergo rovněž součástí ochrany osobnosti) a poměřuje ji s právem (společnosti) na přístup k informacím, resp. tedy s právem na svobodu projevu. Nicméně se domnívám, že se zdaleka nejedná o jediné hodnoty, se kterými může soukromí, resp. tedy jeho dílčí složka v podobě práva být zapomenut, konfrontováno. Zejména v oblasti nových technologií nakládajícími s významným množství dat (vč. osobních údajů), čímž přenášejí význam ochrany soukromí do každodenního života každého jednotlivce, a to i v komerční sféře a potenciální monetizaci soukromí[119] přichází v souvislosti s ochranou osobnosti a uplatňováním práva být zapomenut v úvahu rovněž další hodnoty, které dosud stály v zásadě mimo rámec ochrany soukromí – potenciálně by bylo možné rovněž zvažovat vlastnické právo ve smyslu čl. 11 LZPS (popř. čl. 17 Listiny EU a čl. 1 dodatkového protokolu Úmluvy) či právo na svobodu podnikání ve smyslu čl. 26 LZPS (popř. čl. 16 Listiny EU).

Na tomto místě je rovněž nezbytné připomenout, že i obecné nařízení o ochraně osobních údajů, coby evropské nařízení, je závazné i pro samotné členské státy a jejich zákonodárce.[120] V případě, kdy národní zákonodárci přijímají jakoukoliv úpravu související se zpracováním osobních údajů, měli by respektovat nařízení

---

[115] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 126.

[116] Podle článku 11 Listiny EU platí, že *„každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice.“*

[117] Podle čl. 17 odst. 1 LZPS platí, že *„svoboda projevu a právo na informace jsou zaručeny.“*

[118] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 343.

[119] Srov. např. NONNEMANN, František. Osobní údaje jako platidlo?. Právní rozhledy, 2020, č. 5, s. 174-180 nebo Elvy, Stacy-Ann. “PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY.” Columbia Law Review, vol. 117, no. 6, Columbia Law Review Association, Inc., 2017, pp. 1369–459, http://www.jstor.org/stable/44392955.

[120] Srov. např. CRAIG, Paul P. a G. (Gráinne) DE BÚRCA. EU law: text, cases, and materials. 5th ed. Oxford: Oxford University Press, 2011, clvii, 1155 s. ; 25 cm. ISBN 978-0-19-957699-9, s. 112.

a jeho principy a zásady. Ve vztahu k podnikajícím fyzickým osobám a/nebo členům statutárních orgánů právnických osob, kde často existuje veřejný zájem na zveřejnění údajů těchto osob, by měl zákonodárce postupovat uvážlivě a veškeré takové zpracování – vyplývající z veřejného společenského zájmu a následně inkorporované do zákona – podrobovat testu proporcionality, případně rozumnosti.[121]

1.4.2 Kolize jednotlivých práv ve vybrané rozhodovací praxi

1.4.2.1 Zhodnocení stávajícího stavu a aplikace vůči právu být zapomenut

Výsledky judikatury při aplikaci testu proporcionality jsou značně rozkolísané a neposkytují jednoznačnou rozhodovací linii.[122] V kapitole níže uvádím několik vybraných příkladů judikatury ESLP, Soudního dvora Evropské unie i českých soudů zaměřující na otázku proporcionality ochrany soukromí – zejména tedy v porovnání oproti právu na svobodu projevu a právu na přístup k informacím. Velká část níže popsaných případů se přitom týká zejména zveřejňování informací ze strany (bulvárního) tisku, resp. tedy postupem času obecně zveřejňování informací a údajů v online prostředí. Soudy se tak musely vždy vypořádat s otázkou postavení konkrétní osoby, jejího případného veřejného postavení či výkonu veřejné funkce, a tedy do jaké míry musí snášet míru zásahu do svého soukromí, resp. do jaké míry má veřejnost právo na to, aby byla o životě těchto osob informována a měla přístup k takovým informacím.

Jakékoliv hodnocení aplikace testu proporcionality v těchto případech je přitom zásadní i pro aplikaci práva být zapomenut coby integrální součásti ochrany osobnosti (srov. kapitolu 2). Aplikace práva být zapomenut – ať už podle pravidel implementovaných v obecném nařízení o ochraně osobních údajů (tedy zejména v čl. 17, k tomu srov. kapitolu 6 této práce), nebo podle obecných pravidel ochrany osobnosti (k tomu viz kapitola 2) – nebude vždy černobílá a obvykle bude muset reflektovat skutkové okolnosti daného případu, jako je např. uplynutí

[121] K tomu srov. nález Ústavního soudu ze dne 12. 12. 2017, Pl. ÚS 26/16.

[122] WAGNEROVÁ, E. in WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 283.

účelu zpracování osobních údajů, možnosti míry zásahu do soukromí, uplynutí dostatečného času k tomu, aby relevance zveřejněných informací byla zanedbatelná a jiné. Ač je přitom právo být zapomenut relativně nový právní instrument, tyto standardní principy a proporcionalita zásahu bude vyplývat ze standardních pravidel, dlouhodobě postupně formovaných výkladovou praxí.

1.4.2.2 Rozhodovací praxe Evropského soudu pro lidská práva

V případu *Von Hannover I*[123] se Evropský soud pro lidská práva musel vypořádat s otázkou, zda publikace fotografií zachycujících stěžovatelku ve veřejném prostoru při běžných každodenních činnostech soukromého života porušuje její právo na ochranu soukromí, jestliže stěžovatelka nevykonává žádnou veřejnou funkci a veřejně známou osobou je pouze pro svoji příslušnost k vládnoucímu rodu. Zejména pak v případě, že účelem těchto fotografií je pouze pobavení společnosti, a nikoliv její informování o záležitostech veřejného zájmu. Stěžovatelkou byla Caroline von Hannover, nejstarší dcera monackého knížete Rainiera III. a později také hannoverská princezna, která jakožto příslušnice monackého vládnoucího rodu zastávala reprezentativní funkce na různých charitativních a kulturních akcích; nikdy však nezastávala žádnou veřejnou funkci ani pozici ve veřejné instituci. ESLP zde dospěl k závěru, že pouze na základě toho, že je veřejně známou osobou a pohybuje se ve veřejném prostoru, nelze veřejnosti přiznávat legitimní zájem znát všechny detaily o jejím soukromém životě. Fotografie zachycující stěžovatelku při výkonu každodenních aktivit v jejím soukromém životě nijak nepřispívají do veřejné debaty, přestože je stěžovatelka veřejně známou osobností. Stejně tak soud zvážil význam ochrany soukromí jednotlivců z pohledu rozvoje osobnosti a zdůraznil, že i veřejně známé osobě musí být dopřána ochrana jejího soukromí v rozsahu, jaký může legitimně očekávat.

Princezna Caroline von Hannover byla stěžovatelkou před ESLP rovněž v případě *Von Hannover II*[124], ve kterém spolu se svým manželem, princem Ernstem

[123] Rozsudek ESLP ze dne 24. června 2004 ve věci 59320/00 - Von Hannover proti Německu.

[124] Rozsudek ESLP ze dne 7. února 2012 ve věci 40660/08 a 60641/08 – Von Hannover proti Německu.

Augustem von Hannover, bránili proti zveřejňování fotografií z jejich soukromého života v časopise Frau im Spiegel a Frau Aktuell. Tři zveřejněné fotografie se týkaly různých okamžiků ze soukromého života princezny a prince – jedna zachovala stěžovatelku a jejího otce během jejich lyžařské dovolené ve sv. Moritzu, na druhé byli stěžovatelé zachyceni při procházce ve sv. Moritzu, na třetí pak byli stěžovatelé zachyceni během jízdy lanovkou v Zürs am Arlberg v průběhu jejich dovolené. ESLP v tomto případě zdůraznil, že při poměřování práva na ochranu osobnosti a práva na svobodu projevu je nutné postupovat velice opatrně[125]. Soud definoval základní kritéria, která je třeba aplikovat: (i) zda a jakým způsobem fotografie nebo článek zveřejněné v tisku přispívají veřejné debatě o věcech ve veřejném zájmu; (ii) kritérium známosti dotčené osoby a to, co je předmětem reportáže nebo článku; (iii) předešlé chování dotčené osoby ve vztahu k publikaci fotografií a článků; a (iv) okolnosti, za kterých byla fotografie pořízena – zejména, zda byl s pořízením a publikací fotografie vysloven souhlas, nebo zda byly pořízeny bez jejího vědomí (či dokonce za použití různých nepoctivých prostředků). Na základě těchto kritérií v daném případě ESLP neshledal zásadní zásah do soukromí stěžovatelů.

Rovněž v případu *Axel Springer proti Německu*[126] se ESLP zabýval narušením soukromí veřejně známé osoby (televizního herce), který byl zatčen na mnichovském pivním festivalu pro držení kokainu. Stěžovatelem bylo v tomto případě vydavatelství novin Axel Springer AG, které zveřejnilo na titulní straně detailní informace pojednávající o celém incidentu a později rovněž článek o trestním řízení v dané věci. Oba články obsahovaly detailní informace, včetně fotografií z místa činu. ESLP v tomto případě aplikoval šestistupňový test, jehož cílem bylo zvážit všechna nezbytná kritéria mezi právem na ochranu soukromí a právem na svobodu projevu stěžovatele: (i) míra, do jaké projev přispívá k debatě o veřejném zájmu, (ii) status osoby, (iii) předchozí chování osoby, (iv) metoda získání informací a jejich pravdivost, resp. důvěryhodnost

[125] *„require an examination of the fair balance that has to be struck between the applicants' right to respect for their private life and the right of the publishing company to freedom of expression…"*

[126] Rozsudek ESLP ze dne 7. února 2012 ve věci 39954/08 - Axel Springer proti Německu.

(angl. *veracity*), (v) obsah, forma a následky projevu, a (vi) závažnost sankce, která může být za projev uložena. V tomto případě ESLP dospěl k závěru, že svoboda projevu převažuje nad ochranou soukromí v demokratické společnosti.

Míra možnosti zásahů do soukromí se netýká jen veřejně známých osob, ale v rozhodovací praxi ESLP se objevuje rovněž v souvislosti se sledováním zaměstnanců při výkonu jejich práce a používání pracovních prostředků.

V případu *Copland proti Velké Británii*[127] z roku 2007 se ESLP zabýval otázkou, zda bylo monitorování pracovních pomůcek (pracovního telefonu, emailu a internetového přístupu žalobkyně) předmětem monitorování zaměstnavatelem za účelem kontroly, zda nejsou zneužívány pro osobní účely. Žalobkyní byla osobní asistentka ředitele vysoké školy Carmarthenshire. Soud zde připomněl, že pracovní telefonní hovory jsou chráněny ochranou soukromí a korespondence podle článku 8 Úmluvy, stejně jako informace z monitorování osob odvozené. ESLP uzavřel, že ačkoliv obdobné sledování pracovních prostředků může být v některých případech "nezbytné v demokratické společnosti" za účelem dosažení legitimního cíle, v daném případě nebyl zásah proporcionální, jelikož neexistoval dostatečně odůvodněný zájem zaměstnavatele na sledování soukromých aktivit zaměstnance.

Obdobnou situací se ESLP zabýval v případě *Bărbulescu*[128], kde posuzoval, zda zaměstnavatel mohl ukončit pracovní poměr se svým zaměstnancem, u kterého zjistil, že v pracovní době využívá svůj pracovní počítač na soukromou komunikaci s rodinnými příslušníky (prostřednictvím pracovního účtu na komunikačním nástroji Yahoo Messenger). Podle stěžovatele takové sledování komunikace s rodinnými příslušníky zasahovalo do jeho soukromí ve smyslu čl. 8 Úmluvy. Ačkoliv ESLP nejdříve v rozhodnutí z r. 2016[129] shrnul, že stěžovateli nebyla způsobena škoda, a proto je zásah do soukromí v pořádku, velký senát ESLP následně shledal tento zásah do soukromí nepřiměřený, protože nesplňoval

[127] Rozsudek ESLP ze dne 3. dubna 2007 ve věci 62617/00 - Copland proti Velké Británii.

[128] Rozsudek ESLP ze dne 5. září 2017 ve věci 61496/08 - Bărbulescu v. Romania.

[129] Rozsudek ESLP ze dne 12. ledna 2016 ve stejné věci 61496/08 - Bărbulescu v. Romania.

základní principy nezbytnosti, specifikace účelu, transparentnosti, legitimnosti a proporcionality, které vyžadují zejména předpisy na ochranu osobních údajů. ESLP kromě jiného považoval za zásadní zejména nedostatečné informování zaměstnance o tomto způsobu sledování jeho komunikace, který navíc měl nejzávažnější možné konsekvence – ukončení pracovního poměru.

1.4.2.3 Rozhodovací praxe Soudního dvora Evropské unie

Vývoj judikatury Soudního dvora Evropské unie postupně přinesl rozlišení několika typů základních práv. Obecné ochraně osobnosti se Soudní dvůr věnoval například již v rozsudku ve věci *Stauder*[130], ve kterém SDEU dospěl k závěru, že svoboda projevu zaručená v čl. 10 Úmluvy náleží k obecným právním zásadám, jejichž respektování Soudní dvůr Evropské unie zajišťuje. K ochraně svobody projevu se Soudní dvůr Evropské unie vyjadřoval např. ve svém rozsudku v případu *VBBB proti Komis*i, kde dospěl k závěru, že svoboda vyjadřovat se zaručuje i v rozhlase a v oblasti televizního vysílání.[131] Rozsah ochrany svobody projevu rozebíral Soudní dvůr Evropské unie např. ve svém rozhodnutí ve věci *The Society for the Protection of Unborn Children Ireland Ltd*[132], přičemž např. podle rozhodnutí ve věci *Elliniki Radiophonia Tiléorassi AE*[133] platí, že svoboda projevu je ve vztahu ke svobodě sdělovacích prostředků a požadavku pluralisticky strukturované podstaty rozhlasového vysílání, kvalifikována jako obecná právní zásada. Podle rozhodnutí Soudního dvora Evropské unie věci *Hauer*[134], které významně ovlivnila německá rozhodovací praxe, omezení lidských práv nikdy nesmí zasahovat do podstaty lidských práv;

[130] Rozsudek Soudního dvora Evropské unie ze dne 12. listopadu 1969, Erich Stauder proti Stadt Ulm - Sozialamt, C-29/69.

[131] Rozsudek Soudního dvora Evropské unie ze dne 17. ledna 1984, VBVB proti Komisi Evropských společenství, Spojené věci 43/82 a 63/82.

[132] Rozsudek Soudního dvora Evropské unie ze dne 4. října 1991, The Society for the Protection of Unborn Children Ireland Ltd, C-159/90.

[133] Rozsudek Soudního dvora Evropské unie ze dne 18. června 1991, Elliniki Radiophonia Tiléorassi AE, C-260/89.

[134] Rozsudek Soudního dvora Evropské unie ze dne 13. prosince 1979 ve věci C-44/79 Hauer.

jakákoliv omezení musí být přiměřená a vhodná k ochraně chráněného institutu a současně v rozumném poměru k zamýšlenému cíli.[135]

Otázkou proporcionality ochrany soukromí a možnostmi státu vyžadovat si od soukromých osob informace se Soudní dvůr zabýval např. ve věci *Österreichischer Rundfunk*[136], ve kterém zvažoval, zda ochrana osobních údajů (ve smyslu směrnice 95/46/ES) brání vnitrostátní právní úpravě, která ukládá státnímu orgánu dohledu povinnost shromažďovat a sdělovat pro účely zveřejnění údaje ohledně jmen a příjmů osob zaměstnaných subjekty, které podléhají tomuto dohledu, převyšují-li tyto příjmy určitý strop. SDEU v tomto případě kromě výkladu samotné směrnice rovněž aplikoval principy čl. 8 Úmluvy. SDEU zvažoval, zda je tento zásah nezbytný k dosažení sledovaného legitimního cíle v demokratické společnosti. Zároveň poměřoval zájem na zajištění optimálního používání veřejných prostředků se závažností zásahu do práv dotčených osob, přičemž zdůraznil, že je třeba přezkoumat, zda je s ohledem na legitimní cíl přiměřené zveřejňovat jména dotčených osob. Pro konkrétní aplikaci daných principů však ponechal na národních soudech, které Soudnímu dvoru tyto předběžné otázky položily – aby ověřily, zda je uvedené zveřejňování k dosažení legitimního cíle nutné a přiměřené a zda nebylo možné uváděného legitimního cíle možno dosáhnout poskytnutím předmětných méně invazními prostředky.

V případě *Promusicae*[137] se SDEU zabýval otázkou, zda uvedené autorskoprávní směrnice (konkrétně směrnice 2001/29 a směrnice 2004/48) ve spojení s tzv. *eCommerce* směrnicí (2000/31) a ve spojení s čl. 17 a 47 Listiny EU ukládají členským státům, aby za účelem zajištění účinné ochrany autorského práva stanovily povinnost sdělit osobní údaje v rámci občanskoprávního řízení. Soudní dvůr při výkladu těchto norem zdůraznil, že členské státy při implementaci

[135] K tomu rovněž srov. např. TICHÝ, Luboš, Rainer ARNOLD, Jiří ZEMÁNEK, Richard KRÁL a Tomáš DUMBROVSKÝ. Evropské právo. 5. přeprac. vyd. Praha: C.H. Beck, 2014, xlii, 756 s. ISBN 978-80-7400-546-6.

[136] Rozsudek Soudního dvora Evropské unie ze dne 20. května 2003 ve věci C-465/00 Österreichischer Rundfunk.

[137] Rozsudek Soudního dvora Evropské unie ze dne 29. ledna 2008 ve věci C-275/06 Promusicae.

předmětných směrnic musí zajistit spravedlivou rovnováhu mezi jednotlivými základními právy, v tomto případě právem na ochranu soukromí a ochrannou vlastnického práva. Jakýkoliv výklad těchto pravidel pak musí být eurokonformní a nesmí být rozporu se základními právy nebo obecnými zásadami komunitárního práva, jako je například zásada přiměřenosti. SDEU zároveň odkázal na svou předchozí rozhodovací praxi, zejména rozhodnutí ve věci *Lindqvist*[138].

Právě v rozhodnutí ve věci *Lindqvist* se SDEU zabýval střetem práva na ochranu soukromí a svobodu projevu, kdy paní Bodil Lindqvist, katechetka ve farnosti Alseda ve Švédsku, zveřejnila bez souhlasu svých kolegů jejich osobní informace na internetových stránkách farnosti. SDEU zvažoval možný rozpor mezi obecnými pravidly o zpracování osobních údajů (dle směrnice 95/46/ES) dopadajícími na předmětný případ a obecnými zásadami svobody projevu ve smyslu čl. 10 Úmluvy. Soudní dvůr zde konstatoval, že ustanovení směrnice a z nich vyplývající omezení jsou dostatečně široká a apriori tak nejsou v rozporu s právem s obecnou zásadou svobody projevu; je přitom na jednotlivých členských státech dané požadavky proporcionálně aplikovat na konkrétní skutkový stav.

Pro vymezení možností zásahů do soukromí a proporcionality s dalšími chráněnými zájmy (zde pak zejména s bezpečnostní a obecnými povinnostmi ukládanými státem k uchovávání některých osobních údajů) jsou pak rovněž zcela zásadní nálezy SDEU (a související rozhodnutí Ústavního soudu) v otázkách *data retention*. Ty jsou samostatně popsány v kapitole 4.1.2.

1.4.2.4 Rozhodovací praxe českých soudů

Ústavní soud se ve své rozhodovací praxi musel často vypořádat s otázkou vystupování veřejných osob a míře kritiky, kterou musejí snést. Nejinak tomu bylo např. v případě Zeman v. Brezina, ve kterém se Miloš Zeman, toho času (r. 1999) ve funkci premiéra České republiky, dopustil několika slovních útoků vůči novináři Ivanu Brezinovi (o „korupci novinářů"), které mohly vést k zásadnímu narušení jeho žurnalistické kredibility. Ústavní soud se v tomto

[138] Rozhodnutí Soudního dvora Evropské unie ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist.

případě tedy zabýval otázkou svobody projevu M. Zemana (ve smyslu čl. 17 LZPS) oproti ochraně dobré pověsti a cti I. Breziny (ve smyslu čl. 10 LZPS). V zásadě se tak jednalo o poměrně nestandardní situaci, kdy veřejně známá osoba (M. Zeman) zasahovala do práv novináře. Ústavní soud zde došel k závěru, že osoby veřejně činné jsou povinny (nad rámec toho, že standardně musejí snést větší míru kritiky) opatrněji uveřejňovat informace, zejména v případech, pokud je prezentují jako fakt. Zároveň je vždy nezbytné vzít v úvahu sílu projevu kritizujícího a kritizovaného.

V nálezu I. ÚS 517/10[139] se Ústavní soud zabýval otázkou poskytování informací o členství soudců v KSČ, kdy stěžovatel na základě zákona o svobodném přístupu k informacím žádal od Vrchního soudu v Olomouci poskytnutí informací o tom, kteří jeho soudci byli před listopadem 1989 členy Komunistické strany Československa. Ústavní soud si kladl otázku, zda se předmětný údaj týká výlučně soukromí subjektu údajů, nebo je součástí veřejné sféry (tj. zda je na jeho poskytnutí veřejný zájem). ÚS zde dospěl k závěru, že profesionální sféra soudců náleží do sféry veřejné, přičemž její součástí jsou veškeré aspekty osobnosti soudce, které mohou mít objektivní souvislost s výkonem jeho funkce. Soud se zároveň vypořádal otázkou, zda se tato informace kvalifikuje jako citlivý osobní údaj (dnes tedy zvláštní kategorie osobních údajů) a zda jako takový jeho ochrana převáží nad právem na informace, a to s přihlédnutím k tomu, zda k jakémukoliv zásahu do práva na informace došlo na základě zákona, zda sleduje legitimní cíl a zda je nezbytný v demokratické společnosti. Ústavní soud zhodnotil, že v daném případě právo na informace převážilo nad právem na ochranu soukromí, a to zejména protože údaj o členství v KSČ (i) je způsobilý přispět k diskusi v demokratické společnosti týkající se veřejného zájmu, (ii) umožní jednotlivci vytvořit si názor na nezávislost a nestrannost soudců a může sloužit jako prostředek jeho ochrany při soudním řízení a (iii) umožní jednotlivci utvořit si názor, zda toto členství může souviset s rozhodováním soudců, pokud jde o hodnotové zaměření soudů i metodologii výkladu práva. Podle Ústavního soudu by naopak neposkytnutí předmětných údajů mohlo vést

[139] Nález Ústavního soudu ze dne 15. listopadu 2010, sp. zn. I. ÚS 517/10.

ke snížení autority soudní moci a ohrozit samotnou existenci justice, která musí být personálně a profesionálně nezpochybnitelná.

Otázkou možností přístupu k informacím se v nedávné době zabýval rovněž Nejvyšší správní soud např. v rozsudku ve věci 5 As 440/2019[140], kde se zabýval otázkou zpřístupnění informací o platu a odměnách vedoucích jednotlivých odborů, poradců hejtmana, náměstků a radních Ústeckého kraje a ředitele uvedeného krajského úřadu, přičemž požadoval mimo jiné zdůvodnění případných mimořádných odměn. S odkazem na judikaturu Ústavního soudu[141] i ESLP[142] Nejvyšší správní soud uzavřel, že „všechna základní práva jsou rovnocenná" a že neexistuje důvod, proč by právo na informace mělo bez dalšího převážit nad právem na ochranu soukromí, resp. osobních údajů. Podle NSS pak platí, že právo na informace ve veřejném zájmu tedy rovněž není absolutní – pokud jeho výkon zasahuje do práva na ochranu soukromého života, je třeba mezi těmito právy zajistit spravedlivou rovnováhu. V daném případě NSS usoudil, že poskytnutí informací není zásahem do soukromí, jelikož je nezbytné zvážit rovněž postavení žadatele o informace, který podal žádost o informace z pozice novináře, zjevně tedy plnil roli *„společenského hlídacího psa"*.

Ve věci negativního registru dlužníků (spotřebitelů)[143] se Ústavní soud zabýval otázkou ústavní konformity vedení tohoto registru dlužníků a zpracování jejich osobních údajů bez jejich souhlasu, a to na základě zákonné úpravy v zákoně č. 634/1992 Sb., o ochraně spotřebitele. Ústavní soud dospěl k závěru, že dochází k zásahu do samé podstaty práva na ochranu soukromí jednotlivce, jelikož toto zpracování osobních údajů bylo velmi úzce účelově vymezeno – pouze pro posouzení úvěruschopnosti spotřebitele, přičemž údaje byly přístupné jen velmi úzce vymezené skupině osob. Z tohoto důvodu považoval Ústavní soud

[140] Rozhodnutí Nejvyššího správního soudu ze dne 5. března 2021, sp. zn. 5 As 440/2019.

[141] Zejména nález Ústavního soud se ze dne 17. října 2017, sp. zn. IV. ÚS 1378/16, ve kterém se Ústavní soud zabýval ústavností poskytnutí informací o platech vedoucích zaměstnanců statutárního města Zlín a uzavřel, že *„je nepochybné, že při jakémkoliv zveřejňování osobních dat je vždy třeba zvažovat i právo na ochranu soukromí dotčených osob. Takovému postupu znění § 8b zákona o svobodném přístupu k informacím nikterak nebrání."*

[142] Rozsudek ESLP ze dne 8. listopadu 2016 ve věci věci 18030/11 - Magyar Helsinki Bizottság.

[143] Nález Ústavního soudu ze dne 3. listopadu 2020, sp. zn. Pl. ÚS 10/17.

zásah do soukromí za přiměřený, jelikož tento přístup navíc podléhá soudní ochraně.

Pro vymezení možností zásahů do soukromí jsou pak rovněž zcela zásadní nálezy Ústavního soudu (a související rozhodnutí SDEU) v otázkách data retention. Ty jsou samostatně popsány v kapitole 4.1.2.

Jako ukázkový případ aplikace testu proporcionality pro možnosti zásahu do soukromí ještě považuji za velmi významné rozhodnutí Nejvyššího soudu ve věci užívání záznamů o sledování osob a věcí v jiné trestní věci[144]. Nejvyšší soud zvažoval možnosti použití záznamů o sledování osob a věcí v jiné trestní věci, než v které bylo sledování povoleno. Nejvyšší soud zde zvažoval vyváženost mezi závažností konkrétního zásahu do soukromí a závažností „jiné" trestné činnosti, která vyšla najevo při sledování a která má být v jiné trestní věci prokazována pořízenými záznamy o sledování.[145] Soud pak uzavřel, že právo na soukromí na jedné straně a veřejný zájem na objasnění trestné činnosti na straně druhé je vždy nezbytné vyvažovat v každém konkrétním případě.

Z rozhodovací činnosti nižších soudů si dovolím zmínit rozhodnutí Krajského soudu v Brně o předběžném opatření z roku 2015[146], ve kterém se žalobce v zásadě domáhal svého práva být zapomenut – vydavatel zpravodajského deníku v tisku i na internetu zveřejnil článek ze soudního řízení, ve kterém zveřejnil celá jména žalobců a jejich fotografie; tento článek byl dostupný na internetu až do roku 2015, kdy si jej všimli žalobci domáhali se odstranění prostřednictvím předběžného opatření. Prvoinstanční soud vydání tohoto předběžného opatření nepřiznal, jelikož podle jeho názoru s časovým odstupem osmi let není dána naléhavá potřeba (nezbytná k vydání předběžného opatření). Krajský soud (coby

[144] Usnesení Nejvyššího soudu ze dne 1. září 2020, sp. zn. 7 Tdo 865/2020, a usnesení Nejvyššího soudu ze dne 25. srpna 2020, sp. zn. 8 Tdo 647/2020.

[145] *„Pokud by v rámci sledování osoby podezřelé ze zvlášť závažné trestné činnosti (například zločinu vraždy) byly pořízeny v jejím bydlišti zvukové a obrazové záznamy, z nichž by vyšlo najevo spáchání nesouvisejícího bagatelního trestného činu (například vyhýbání se plnění vyživovací povinnosti), pak by byl z hlediska proporcionality zřejmě problematický závěr o procesní použitelnosti těchto záznamů jako důkazu v řízení o onom bagatelním trestném činu."* in usnesení Nejvyššího soudu ze dne 1. září 2020, sp. zn. 7 Tdo 865/2020, a usnesení Nejvyššího soudu ze dne 25. srpna 2020, sp. zn. 8 Tdo 647/2020.

[146] Usnesení Krajského soudu v Brně ze dne 7. října 201, sp. zn. 70 Co 228/2015 – 38.

soud odvolací) uvedl, že vliv faktoru času v rámci ochrany práva na soukromí s kolizí práva na svobodu projevu a právem na informace může být velmi relevantní; podle soudu tak zveřejnění nebo další zpřístupňování údajů, které byly původně zveřejněny oprávněně, může představovat neoprávněný zásah osobnostních práv.

1.5 Závěr

Právní ochrana soukromí se začala v právní nauce poprvé objevovat ke konci 19. století, když Samuel D. Waren a Louis D. Brandeis formulovali *right to be alone.* Širší pozornosti se ochraně soukromí začalo dostávat ve 30. letech, když Nejvyšší soud USA v roce 1939 přijal svá první rozhodnutí v této oblasti. Vůbec poprvé se tak přiklonil k liberálním myšlenkám spočívajícím v ochraně jednotlivce vůči zásahům státní moci. Význam ochrany soukromí a jednotlivce vůči státu se ukázal jako nezbytný zejména po zkušenostech s totalitářskými režimy – fašistickými i komunistickými – které se snažily zneužívat informace o soukromí svých občanů ve svůj prospěch a k posílení vlastní moci.

Zásadní význam v právním vymezení soukromí přinesla Všeobecná deklarace lidských práv a svobod z roku 1948, která, ač jako nezávazný dokument, zakotvovala v čl. 12 rovněž právo na ochranu soukromého života. Na tu postupně navazovaly konkrétní mezinárodní smlouvy – zejména tedy Mezinárodní pakt o občanských a politických právech z roku 1966, který téměř doslovně převzal znění čl. 12 Všeobecné deklarace lidských práv a svobod. Na evropské úrovni byl nejzásadnější dokument přijat šestnáct let později, když Rada Evropy v r. 1950 přijala svou Úmluvu o ochraně lidských práv a svobod (v této práci jen jako Úmluva), která v čl. 8 upravuje právo na respektování soukromého a rodinného života, které pak ve své četné judikatuře rozebírá Evropský soud pro lidská práva. Na Úmluvu pro oblast automatizovaného zpracování osobních údajů v r. 1981 navázala tzv. Úmluva č. 108, která navíc byla doplněna Dodatkovým protokolem v r. 2003 upravujícím zřízení nezávislých dozorových orgánů a volné přenosy osobních údajů napříč signatářskými státy.

Významný posun v oblasti právní ochrany soukromí a její podmnožiny ochrany osobních údajů přineslo právo Evropské unie, a to především přijetím směrnice

95/46/ES v roce 1995. Ta dala konkrétní rysy celé oblasti zpracování a ochrany osobních údajů, jak je známe dnes a jak byla za posledních bezmála třicet let dále formována Soudním dvorem Evropské unie i členskými státy při implementaci a další aplikaci těchto pravidel. Ochrana soukromí a osobních údajů je přitom v EU chráněna i na úrovni primárního práva. Evropská unie se přihlásila k aplikaci Úmluvy, když podle čl. 6 odst. 3 SEU zaručuje ochranu všech základních práv dle Úmluvy. Přijetím Lisabonské smlouvy se navíc součástí primárního práva stala i Listina EU, jejíž článek 7 zaručuje ochranu soukromého a rodinného života, obydlí a komunikace, a článek 8 pak zaručuje ochranu osobních údajů, které musejí být vždy zpracovávány korektně, k přesně stanoveným účelům a na základě souhlasu či jiného oprávněného důvodu předvídaného právním předpisem. Tato úprava primárního práva je dále detailně upravena v podobě obecného nařízení o ochraně osobních údajů, které bylo přijato v roce 2016 a je aplikovatelné od 25. května 2018. Právní ochrana poskytovaná soukromí je tak několikavrstvá a překrývající se mezi mezinárodními, evropskými i ryze českými předpisy kombinujícími nejobecnější prvky ochrany nedotknutelnosti osoby (zejména čl. 7 LZPS) a specifické soukromí (čl. 8 Úmluvy, čl. 7 Listiny EU a čl. 10 LZPS) až po velmi úzce vymezenou ochranu osobních údajů (čl. 8 Listiny 8, částečně doplněný čl. 10 odst. 3 LZPS).

Pojem soukromí přitom není v českém ani evropském právní řádu nijak vymezen a blíže jej nedefinují ani jednotlivé mezinárodní dohody. Absence konkrétního vymezení soukromí však není na škodu, naopak pomáhá jeho ochraně. Pojem soukromí (a práva na soukromí) v sobě totiž zahrnuje nemalé množství aspektů týkajících se psychické a fyzické integrity jednotlivce a jeho soukromého života a uplatňuje se napříč jednotlivými vrstvami života jednotlivce – soukromou, společenskou, občanskou a profesionální, přičemž do každé z nich lze v určitém (diferenciovaném) rozsahu za určitých okolností zasahovat. Bližší definice soukromí by tak mohla vést k nežádoucímu zužování tohoto pojmu a omezování jeho ochrany.

Vnímání soukromí se rovněž významně vyvíjí v čase, především pak v souvislosti s rozvojem nových technologií. Pravděpodobně největší rozvoj vnímání soukromí a potřeby jeho ochrany přinesl v posledních dvou dekádách rozvoj internetu

a kyberprostoru, ve kterém může docházet k zásahům do soukromí na každodenní bázi, a to často bez většího uvědomění ze strany jednotlivců. Jednotlivé školy došly ve vnímání pojmu soukromí od jednoduchého pojetí *right to be alone* (ponechání sebe samému), přes redukcionistické pojetí (soukromí jako množina fundamentálních zájmů), omezení přístupu k jednotlivci (dokonalé soukromí by v tomto pohledu bylo vnímané jako absolutní nepřístupnost jednotlivce vůči jeho okolí), kontrolu nad soukromými informacemi až po klastrové pojetí soukromí (v zásadě kombinující jednotlivé přístupy stavějící soukromí na třech základních elementech: informační aspekt (*informational privacy*), přístupnost v prostorové dimenzi (*accesssibility privacy*) a výrazový aspekt (*expressive privacy*)). K těm lze, např. v podání Daniela Solova, přičíst obecnou kontrolu nad vlastními tajemstvími, soukromými informacemi, osobností i intimitou. To všechno vede k pojetí soukromí ve třech základních vrstvách, jak je vymezil Alan Westin – politické, socio-kulturní a osobní.

Judikatura evropských i českých nejvyšších soudů se pak standardně musí vypořádávat se střetem soukromí a dalšími lidskými právy, kde vždy záleží na konkrétní situaci a složce a vrstvě soukromí, která může být dotčena. Jak demonstroval např. ESLP v případu *Van Hannover I* nebo později ve *Van Hannover II*, vždy je třeba posuzovat konkrétní situaci, ve které dochází k zásahům do soukromí; přestože se může jednat o veřejně známou osobu, zásah do její čistě soukromé sféry nemusí být ničím opodstatněný, zejména pokud nevykonává žádnou veřejnou funkci a veřejnost tak nemá žádný převažující zájem na přístup k informacím o takové osobě. Právo na soukromí tak nejčastěji přichází do střetu s právem na přístup k informacím a svobodou projevu. Ačkoliv to neznamená, že soukromí nemůže konkurovat i jiným právům (jako je např. právo na vlastnictví nebo právo na výkon podnikatelské činnosti), tyto nebyly blíže předmětem zkoumání této práce. Pro střet mezi právem na ochranu soukromí a právem na svobodu projevu ESLP (konkrétně v případu *Axel Springer AG*) postupem času přinesl šestistupňový test: (i) míra, do jaké projev přispívá k debatě o veřejném zájmu, (ii) status osoby, (iii) předchozí chování osoby, (iv) metoda získání informací a jejich pravdivost, resp. důvěryhodnost (angl. *veracity*), (v) obsah, forma a následky projevu, a (vi) závažnost sankce, která může být

za projev uložena. Aplikace testu proporcionality (při využití obdobného šestistupňového testu) byla rovněž demonstrována v další aplikační praxi evropských i českých soudů.

Za nejvýznamnější pro účely aplikace práva být zapomenut považuji vymezení práva na informační sebeurčení, které dává jednotlivcům možnost rozhodnout podle vlastního uvážení zda, popřípadě v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jejich soukromí zpřístupněny jiným subjektům. To rovněž potvrdil a blíže specifikoval ESLP (např. v případu *Rotaru*), stejně jako Ústavní soud v několik případech, ve kterých se zabýval možnostmi narušení soukromí moderními sledovacími technologiemi (zejména tedy ve věcech *Data Retention I* a *Data Retention II*, které jsou blíže analyzovány v kapitole 4.1.2).

2 Právo na ochranu osobnosti a soukromí v občanském právu

2.1 Vymezení pojmu osobnost

2.1.1 Pojem osobnost

Osobnost (resp. tedy „osobnost člověka“) v právním slova smyslu se vykládá jako jedinečné spojení biologických, psychologických a společenských aspektů, či spíš hodnot lidské osobnosti.[147] Tato úprava vychází z přirozenoprávního právně-filosofického pojetí, jak je rovněž reflektováno v § 81 o. z., podle nějž je to člověk, který je východiskem pro soukromé právo.[148] Pro přirozená práva je pak typické, že jsou zásadně spjata s člověkem od jeho narození po celou dobu života; přirozená osobnostní práva naopak nejsou ta, která člověk nabývá až v průběhu života.[149]

Nicméně neexistuje jednotná definice osobnosti, jelikož osobnost se projevuje jako dynamický systém, jehož rysy se mění podle věku, přičemž hlavní stálosti dosahuje v dospělosti (v závislosti na vývoji vlastností, charakterových rysů, schopností, temperamentu, postojů, potřeb a zájmů, vzdělání, náboženského a kulturního zaměření aj.).[150]

Jedná se tak o předmět vrozených osobnostních práv člověka stojících oproti kategorii předmětů práv majetkových. Osobnost člověka jako předmět soukromých práv tak zahrnuje vše, čím se člověk projevuje navenek ve vztahu ke svému okolí, a to po stránce fyzické, duchovní a duševní. [151]

---

[147] DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5, s. 248.

[148] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 506.

[149] Srov. rozsudek Nejvyššího soudu ze dne 28. ledna 2010, sp. zn. 30 Cdo 2095/2008.

[150] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 290.

[151] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 290.

V právním pojetí pojem osobnost zahrnuje především morální a fyzickou integritu člověka, včetně jejích vnějších projevů, jeho psychofyzickou identitu, ale i prostředí, ve kterém se člověk pohybuje, tj. jeho prostor a jeho soukromí.[152]

2.1.2 Historický vývoj ochrany osobnosti

Pojem „osobnost“ je v právu poměrně nový fenomén, který se nejprve objevil v 19. století v německé právní vědě (jako tzv. *Rechtspersönlichkeit*) a vytvořil základ pro úpravu v § 823 německého občanského zákoníku (BGB – Bürgerliches Gesetzbuch).[153] Ochrana osobnosti se přitom poměrně významně liší napříč různými právními řády a i v Evropě je tato úprava (a její historický vývoj) značně roztříštěná.[154] Německá právní nauka (tzv. historicko-právní škola hlásící se k tradičním zdrojům římského práva) však byla poměrně ojedinělá, když odmítala myšlenkového odkazy přirozenoprávní teorie a kanonického práva a kladla důraz zejména na smluvní svobodu, majetková práva a náhradu majetkové újmy.[155] Naopak ochrana cti a důstojnosti se přesunula na pole práva trestního.[156]

Odlišně, avšak s německou naukou paradigmaticky, postupovala francouzská úprava, která v souladu s Deklarací práv člověka a občana vycházela z přirozenoprávní generální klauzule deliktního práva vedoucí k možnosti jednotlivce v případě zásahu do jeho osobnostních práv požadovat náhradu nemateriální újmy. Francouzskou úpravu pak převzala i Belgie, Nizozemí, Švýcarsko a zpočátku rovněž Rakousko a Itálie.[157]

---

[152] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 511.

[153] DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5, s. 248.

[154] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 504.

[155] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 505.

[156] Blíže pak viz BRÜGGEMEIER, Gert. Protection of personality rights in the law of delict/torts in Europe: mapping out paradigms. Personality Rights in European Tort Law [online]. Cambridge University Press, 2010, 5-37 [cit. 2022-03-20]. ISBN 0521194911. Dostupné z: doi:10.1017/CBO9780511676161.005.

[157] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 505.

Významným elementem ochrany osobnostních práv v evropském pojetí je zejména důraz kladený na ochranu lidské důstojnosti (což je významné např. oproti Spojeným státům americkým, kde je výchozím bodem lidská svoboda).[158]

Na území České republiky se pak formálně poprvé pojem „ochrana osobnosti" objevil v socialistické Ústavě z roku 1960[159] dále pak rozvinutý jako institut v § 11 a násl. zákona č. 40/1964 Sb., občanského zákoníku.[160] To však neznamená, že do té doby nebyla osobnostním právům na našem území poskytována ochrana. Základy ochrany (ačkoliv nikoliv výslovně) vycházely z obecného ustanovení § 16 rakouského občanského zákoníku z roku 1811 (ABGB – Allgemeines bürgerliches Gesetzbuch), podle kterého *„každý člověka má vrozená, již rozumem poznatelná práva, a nutno jej tudíž považovat za osobu"*.[161] Ochrana dle § 16 ABGB pak zahrnovala, kromě jiného, rovněž právo na občanskou čest, právo na osobní tajemství nebo práva statusová, kde všechna tato práva byla považována za práva vrozená.[162]

Úprava vycházející z ABGB[163] pak byla na našem území v platnosti až do roku 1951, kdy došlo k přijetí tzv. středního občanského zákoníku[164], který v duchu tehdejších politických rozměrů zcela opustil koncepci přirozených osobnostních práv a redukoval jakoukoliv ochranu na vymezení právní způsobilosti fyzických

[158] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 505.

[159] Článek 19 zákona č. 100/1960 Sb., Ústava Československé socialistické republiky: „*Ve společnosti pracujících, ve které je odstraněno vykořisťování člověka člověkem, jsou rozvoj a zájmy každého jejího příslušníka v souladu s rozvojem a zájmy celé společnosti. Práva, svobody a povinnosti občanů slouží tedy svobodnému, všestrannému rozvoji a uplatnění osobnosti občanů a zároveň upevnění a rozvoji socialistické společnosti; s jejím rozvojem se dále rozšiřují a prohlubují.*"

[160] DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5, s. 248.

[161] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 505.

[162] SEDLÁČEK in ANDRES, Bedřich, Antonín HARTMANN, František ROUČEK a Jaromír SEDLÁČEK. Komentář k československému obecnému zákoníku občanskému a občanské právo platné na Slovensku a v Podkarpatské Rusi. Díl 1, (§§ 1 až 284). Praha: Linhart, 1935, 1192 s., s. 186.

[163] ABGB byl do československého právního řádu přijat tzv. recepčním zákonem č. 11/1918 Sb. z. a n.

[164] Zákon č. 141/1950 Sb., občanský zákoník.

osobu a ochranu jejich jména.[165] Ačkoliv tedy pak občanský zákoník z roku 1964 (tj. zákon č. 40/1964 Sb.) ve spojení s Ústavou 1960 přinesly komplexní ochranu osobnosti[166], k návratu k přirozenoprávnímu základu osobnostních práv došlo až přijetím LZPS v roce 1991.[167]

2.2 Právní úprava ochrany osobnosti a soukromí

2.2.1 Mezinárodněprávní a ústavněprávní ochrana osobnosti

Ochrana osobnosti (a tedy i soukromí) vychází z lidskoprávních mezinárodních smluv, které se na základě čl. 10 Ústavy stávají součástí ústavněprávního pořádku.[168] Značný vliv na podobu ochrany osobnosti má rovněž Všeobecná deklarace lidských práv vyhlášená po druhé světové válce, která však nemá povahu mezinárodní smlouvy a není tak právně závazná; přesto ovlivnila další celosvětový i evropský vývoj a promítla se pak napříč jednotlivými lidskoprávními mezinárodními dohodami.[169]

Ochrana osobnosti je pak zakotvena zejména v Úmluvě (tj. Úmluvě o ochraně lidských práv a základních svobod), Úmluvě na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny – Úmluvě o biomedicíně z r. 1997, v Dodatkovém protokolu o klonování lidských bytostí z r. 1998 i v Úmluvě o právech dítěte z r. 1989.[170] Rovněž se jedná o Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, oba z r. 1966.[171]

---

[165] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 288.

[166] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 289.

[167] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 290.

[168] K tomu blíže kapitola 1.3.2.1 této práce.

[169] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 507.

[170] DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5, s. 250.

[171] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 508.

Významnou roli pak hraje rovněž právo EU[172], jak je ve vztahu k ochraně soukromí blíže popsáno v kapitole 1.3.1 této práce. Nejvýznamnější je pak zejména Listina EU.[173]

Veškeré mezinárodní i ústavněprávní zakotvení přirozených osobnostních práv hraje významnou roli při tvorbě, výkladu a použití norem (obyčejného) práva v občanském zákoníku, což se odráží rovněž v judikatuře Ústavního soudu i Evropského soudu pro lidská práva.[174]

2.2.2 Občanský zákoník

Osobnostní práva jsou v občanském zákoníku chráněna zejména v rámci ustanovení § 81 a násl. o. z. (vážnost a čest člověka) a ve spojení s § 77 až 79 o. z. (ochrana jména). Vedle toho ještě stojí ochrana názvu právnické osoby (§ 138 o.z.).

Ustanovení § 81 odst. 1 o. z. pak představuje tzv. generální klauzuli, podle které platí: *„Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.“*

Výčet osobnostních práv podle § 81 odst. 2 o. z. je demonstrativní a může být výkladovou praxí doplňován v návaznosti na vývoj lidské společnosti a změnu potřeb a hodnotových akcentů.[175] Zejména právo na soukromí je např. v judikatuře ESLP mimořádně flexibilní a pokrývá velké spektrum situací.[176] Podle Ryšky a Kokeše takto rovněž došlo k institucionalizaci práva být zapomenut rozsudkem SDEU ve věci Google Spain (k tomu viz kapitola 5.2.2 této

[172] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 507.

[173] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 507.

[174] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 289.

[175] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 127.

[176] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 127.

práce) do té doby částečně předvídaného v doktrinální praxi pro účely kolize práva na svobodu projevu a práva na informace.[177]

Kromě samotné osobnosti člověka, kterým se občanský zákoník věnuje ve výše uvedených ustanovení, jsou chráněna i přirozená práva člověka, ke kterým se občanský zákoník výslovně hlásí v § 19 o.z.[178] Tím se občanský zákoník tedy hlásí k iusnaturalistickému pojetí práv a ochrany osobnosti obdobně, jako činil např. rakouský ABGB a osobnostní práva chrání jako práva přirozená. Významným aspektem přirozených práv pak zůstává, že je není nutné zákonem vyhlašovat, neboť předcházejí právnímu řádu a jsou každému sama sebou poznatelná.[179]

2.2.3 Povaha práva na ochranu osobnosti

2.2.3.1 Všeobecné osobnostní právo

Osobnost člověka je ucelený celek hodnot, který tak jakožto jednotu dílčích osobnostních práv vytváří všeobecné osobnostní právo. Dílčí osobnostní práva se pak vážou k jednotlivým hodnotám lidské osobnosti, avšak jsou vždy pouhou součástí tohoto celku.[180] Jednotlivé osobnostní atributy (dílčí práva) jsou tak součástí jediného práva a vytvářejí monistickou koncepci lidské osobnosti; nelze tak hovořit o několika osobnostních právech, ale jen o celku této ochrany.[181]

Stejně jako každé jiné subjektivní právo i osobnost lze rozdělit na práva ryze osobní (resp. osobnostní; angl. *non-property rights*, něm. *Persönlichkeitsrechte*) a majetková (angl. *property rights*, něm. *Vermögensrechte*). Zatímco občanská majetková práva mají vždy určitý ekonomický obsah, subjektivní práva osobností

[177] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 127.

[178] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 511.

[179] Srov. např. SOBEK, MELZER in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 264.

[180] DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5, s. 249.

[181] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 127.

se upínají na osobnost v její fyzické a morální jednotě (např. život, zdraví a tělo člověka, osobní svobodu, čest, důstojnost, jméno, soukromí, slovní projevy osobní povahy). Osobnostní práva tak ve své podstatě zabezpečují nemajetkové (duchovní, morální) zájmy člověka, které nepodléhají ohodnocení v penězích.[182]

Všeobecné osobnostní právo člověka je chráněno již formou generální klauzule v § 81 odst. 1 o.z., přičemž odst. 2 nabízí demonstrativní výklad statků, které jsou předmětem ochrany všeobecného osobnostního práv.[183] Konkrétní ochrana, kterou poskytují ustanovení § 84 a násl. o.z. je tak jen doplněním, nikoliv zvláštní ochranou této materie.[184] Jednotlivé osobnostní atributy jsou chráněny komplementárně, prostředky a nástroje soukromého a veřejného práva se doplňují.[185] Vedle toho rovněž stojí tzv. zvláštní osobnostní práva, která souvisí s projevem tvůrčích schopností člověka, jako jsou osobnostní práva autorská, osobnostní práva výkonných umělců, osobnostní práva vynálezců nebo původců technických výtvorů.[186]

Pro účely vymezení práva být zapomenut v této práci je nejdůležitějším prvkem ochrany osobnosti právo na ochranu soukromí, které tvoří integrální součást všeobecného osobnostního práva[187] a je rovněž blíže vymezené v kapitole 1.2 této práce. Pro rozsah uplatňování práva být zapomenut pak může být rovněž významné právo na ochranu projevů osobní povahy. Vedle toho je rovněž nezbytné zvažovat jako ostatní dílčí součásti ochrany osobnosti, jako zejména

[182] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 89.

[183] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 543.

[184] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 543.

[185] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 122.

[186] DOLEŽAL T. a A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 509.

[187] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 543.

ochranu důstojnosti, jakožto stavebního kamene ochrany osobnosti[188], a rovněž ochranu jména člověka.

Nicméně vzhledem k významu jednotlivých složek a konceptu osobnosti založené na jeho integritě[189] je pro účely této práce nezbytné na ochranu osobnosti hledět jako celek, jelikož např. narušení práva na soukromí může mít vždy hlubší propojení na ochranu osobnosti jako celku, která se může propisovat na různých rovinách a dílcích ochrany osobnosti. Ačkoliv tak rozbor všech těchto dílčích prvků může mít pro účely práva být zapomenut částečnou relevanci, jejich podrobná analýza by významně přesahovala rozsah a cíle této práce. Pro účely této práce se tak soustředím primárně na ochranu soukromí, jehož je právo být zapomenut inherentní součástí (coby právo dovozované zejména v souvislosti s ochranou osobních údajů a legislativně zakotvené v čl. 17 GDPR), případně pak ochranu osobnosti (resp. osobností práva) jako celek, bez podrobnějšího rozlišování těchto dílčích prvků.

Složka soukromí jakožto součást osobnostních práv je navíc sama o sobě velmi významná a všezahrnující, jak potvrzuje judikatura ESLP. Podle ESLP je právo na soukromí v oblasti privátní sféry člověka skutečně všezahrnující a pohlcuje jinak běžně separátně uváděná další dílčí osobnostní práva (právo na čest a důstojnost, na tělesnou integritu atd).[190]

Jednou ze složek ochrany osobnosti tak bude rovněž právo být zapomenut. K obdobnému závěru dospěli rovněž Ryška a Kokeš, podle kterých došlo zakotvením práva být zapomenut v obecném nařízení o ochraně osobních údajů k jeho institucionalizaci, a tedy výslovného začlenění do ochrany osobnosti.[191] Ke stejnému závěru dospěl rovněž Nejvyšší soud, který uzavřel, že *„k zásahu do*

[188] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 505.

[189] Srov. např. DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 511.

[190] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 551.

[191] Srov. RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 127.

osobnostních práv nepravdivým dehonestujícím tvrzením nebo nepřiměřeným hodnotícím soudem může dojít i jejich publikací na internetu. Osoba těmito informacemi dotčená má v prvé řadě tzv. právo být zapomenut.“[192]

2.2.3.2 Absolutní působnost a relativnost (omezitelnost) osobnostních práv

Právo na ochranu osobnosti je právem absolutní povahy, avšak pouze v soukromoprávním významu – tedy ve smyslu jeho působení *erga omnes*. Tato povaha vyplývá z přirozenoprávní povahy osobnosti, kde stát zakotvením této úpravy v občanském zákoníku uznává způsob výkonu a ochrany těchto práv na území České republiky.[193] Smyslem zákonné úpravy ochrany osobnosti je v soukromoprávní oblasti zabezpečit respektování ochrany osobnosti člověka a jeho všestranný svobodný rozvoj[194], přičemž se ve své podstatě jedná o rozvedení a konkretizaci, kromě jiného, článku 7 a 10 LZPS (rovněž dále čl. 8, 13 a 14 LZPS)[195], které jsou rovněž blíže popsány v kapitole 1.3.2.1 této práce.

Zároveň však platí, že ve významu ústavněprávním jsou osobní práva považována za relativní, tedy nikoliv neomezitelné, které připouští možnost omezení a vyvažování.[196] Právo na ochranu osobnosti tak musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy a chráněnými hodnotami.[197]

Omezitelné tak bude i právo být zapomenut. Jedná se tedy o relativní právo, jehož uplatnění není neomezené, jak dovodil rovněž Soudní dvůr Evropské unie ve věci Manni, podle kterého „*není možné vyloučit, že mohou existovat zvláštní situace, v nichž vážné a legitimní důvody související s konkrétní situací subjektu údajů*

[192] Rozsudek Nejvyššího soudu ze dne 15. prosince 2020, 25 Cdo 27/2020.

[193] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 292.

[194] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 289.

[195] K tomu srov. např. rozhodnutí Nejvyššího soudu ze dne 26. července 2000, sp. zn. 30 Cdo 2304/99.

[196] Srov. BARTOŇ, Michal, Jan KRATOCHVÍL, Martin KOPA, Maxim TOMOSZEK, Jiří JIRÁSEK a Ondřej SVAČEK. Základní práva. Praha: Leges, 2016, 608 s. ISBN 978-80-7502-128-1, s. 75 – 78.

[197] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 125.

výjimečně odůvodňují, aby byl po uplynutí dostatečně dlouhé doby od likvidace dotčené společnosti omezen přístup k osobním údajům zapsaným v rejstříku, které se jej týkají, ve vztahu ke třetím osobám, které prokáží zvláštní zájem na nahlížení do těchto údajů.“[198]

2.2.3.3 Pozitivní a negativní složka

Pozitivní složka zahrnuje oprávnění člověka svou osobnost užívat a v mezích právního řádu s ní i disponovat.[199] Garantuje tedy sebeurčení ve smyslu zásadního rozhodování o sobě samém, včetně uspořádání vlastního života[200], a zajištění tedy vlastních potřeb a zájmů.[201] Např. právo na podobu v sobě zahrnuje možnost fyzické osoby zachytit svou podobu, ale i udělovat jinému svolení k jejímu zachycení.[202]

Negativní složka práva pak představuje oprávnění člověka vzepřít se všem třetím osobám v neoprávněných zásazích a možnosti uplatit obranu proti takovým zásahům.[203] Toto oprávnění slouží funkčně k zabezpečení ochrany osobnosti člověka v případě jejího neoprávněného porušení, resp. ohrožení ze strany jiných subjektů s rovným právním postavením (např. tedy bránit se neoprávněnému zachycení své podoby ze strany jiného).[204]

Právě z důvodu existence těchto dvou složek ochrany osobnosti (pozitivní a negativní) se dovozuje, že všeobecné osobnostní právo má každá osoba,

---

[198] Rozhodnutí Soudního dvora EU ze dne 9. 3. 2017, ve věci C-398/15 - Manni. Dostupné z: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-398/15.

[199] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 125.

[200] Rozhodnutí Ústavního soudu ze dne 6. března 2012, sp. zn. I. ÚS 1586/09.

[201] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 295.

[202] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 94.

[203] RYŠKA, KOKEŠ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 125.

[204] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 94.

a to i před jejím narušením. Z tohoto hlediska je jedním z nejvýznamnějších prvků dílčích osobnostních práv především oprávnění disponovat s osobností, resp. jejími jednotlivými hodnotami.[205]

2.3 Dispozice s osobností a jiné oprávněné zásahy do osobnosti

Pro zkoumání narušení osobnosti je rovněž nezbytné vymezit případy, kdy, ačkoliv dochází k zásahu do osobnosti (resp. osobnostních práv), nedochází k jejich narušení. Je tedy vždy nezbytné zkoumat, zda je daný zásah skutečně neoprávněný nebo zda neexistují okolnosti, který by protiprávnost zásahu vylučovaly. Těmito okolnostmi mohou být zejména (i) svolení (souhlas) dotčené osoby, (ii) zákonem povolený zásah, (iii) plnění právní povinnosti nebo (iv) výkon jiného subjektivního práva.[206] Veškeré tyto možnost zásahu je nezbytné vykládat restriktivně.[207]

Jedná se tedy o případy, ve kterých může za zákonem vymezených okolností docházet k zásahu do osobnosti vylučujícím protiprávnost. V zásadě nejširší možnost zásahu pak představuje svolení člověka, které vyplývá zejména z oprávnění člověka disponovat se svými právy potvrzující vymezení pozitivní a negativní složky jeho osobnostních práv (srov. předcházející kapitolu). Nicméně ani svolení nesmí být v rozporu s dobrými mravy nebo pak oprávněnými zájmy jiných osob[208] a v každém případě nesmí zasahovat do integrity člověka[209]. Zákonné zásahy[210] osobnosti člověka (resp. v tomto případě do soukromí

[205] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 94.

[206] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 529.

[207] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 376.

[208] DOLEŽAL T., in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 529.

[209] Srov. ustanovení § 93 o.z.

[210] Resp. tedy zásahy na základě zákonných licencí: (i) licence výkonu nebo ochrany práv a zájmu jiných (§ 88 odst. 1 o.z.), (ii) úřední licence (§ 88 odst. 2 o.z.), (iii) licence veřejných záležitostí (§ 88 odst. 2 o.z.), (v) vědeckou licenci (§ 89 o.z.), (v) uměleckou licenci (§ 89 o.z.) a (vi) zpravodajskou licenci (§ 89 o.z.). K tomu srov. např. RYŠKA in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 160.

a podoby) musí být vždy přiměřené a v souladu s oprávněnými zájmy člověka.[211] Vždy tak bude např. nezbytné zohledňovat postavení dotčeného člověka, konkrétní způsob zásahu apod. Jakýkoliv nepřiměřený zásah by narušoval nedotknutelný základ osobnosti každého člověka, na jehož respektování je nutné v souladu s ohledem na zachování elementární důstojnosti člověka vždy a za všech okolností trvat.[212]

Zákonné zásahy do ochrany osobnosti přitom mají zásadní dopad, jelikož dochází k legitimaci takového zásahu ze strany státu a jakékoliv ochrany je tak možné dovolávat se v zásadě jen prostřednictvím napadení příslušné zákonné úpravy na základě rozporu s ústavněprávně chráněnými základními právy, zejména tedy pro rozpor s ochranou soukromí jednotlivce. Pokud by se jednalo o zásahy do soukromí ze strany státu, resp. orgánů veřejné moci, jakýkoliv takový zásah veřejné moci do práva na soukromí musí být v souladu s čl. 8 Úmluvy, mimo jiné, proveden v souladu se zákonem, jenž musí být dostupný a dostatečně předvídatelný, tj. vyjádřený s velkou mírou přesnosti tak, aby jednotlivci dovolil v případě potřeby regulovat své chování.[213] Rozsah zákonné úpravy tak v ochraně osobnosti (obdobně je tomu pak i ve specifické oblasti ochrany osobních údajů) hraje zásadní roli. Tato pravidla musí být vždy navíc stanovena dostatečně přesně, jasně a detailně, a to takovým způsobem, aby jednotlivci disponovali dostatečnými zárukami proti riziku jejich zneužití a svévole.[214] Takto např. Nejvyšší soud aproboval uchování vzorků (profilu) DNA pachatele úmyslné trestné činnosti Policií ČR, která podle závěrů Nejvyššího soudu tak činila zcela v souladu s platnou právní úpravou, tudíž se v dané věci nemohlo jednat o neoprávněný zásah do práva na ochranu osobnosti.[215]

---

[211] Srov. ustanovení § 90 o.z.

[212] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 377.

[213] Rozsudek ESLP ze dne 16. 12. 1997 ve věci Camenzind proti Švýcarsku č. 21353/93.

[214] Srov. např. rozhodnutí ESLP ze dne 29. 6. 2006 ve věci Weber a Saravia proti Německu č. 54934/00 nebo rozhodnutí ESLP ze dne 1. 7. 2008 ve věci Liberty a další proti Spojenému království č. 58243/00.

[215] Rozsudek Nejvyššího soudu ze dne 17. ledna 2020, 30 Cdo 2003/2018.

Pro účely této práce pak nejsou konkrétní možnosti dispozice a (oprávněných) zásahů do osobnostních práv blíže rozebírány. Pro vymezení dopadů práva být zapomenut bude rozhodující zejména skutečnost, že právní úprava předjímá možnosti určitých kvalifikovaných zásahů do těchto osobnostních práv – resp. naopak, že může dojít k nenaplnění nebo odpadnutí těchto kvalifikovaných výjimek. Ty jsou přitom v zásadě velmi podobné podrobnější úpravě tzv. právních základů zpracování podle obecného nařízení o ochraně osobních údajů (srov. kapitolu 3.1.4 této práce). Přesto platí, že nesplnění povinností podle pravidel pro zpracování osobních údajů (např. tedy absence právního základu zpracování) nutně nemá zásadní význam pro posouzení existence zákonného důvodu zásahu dle pravidel soukromého práva.[216] Domnívám se ale, že z praktického hlediska bude právo být zapomenut vždy primárně uplatňované (a uplatnitelné) především jako součást ochrany osobních údajů (a takto bude i vymáhané); pouze v případě, že v konkrétním případě nebude možné postupovat podle pravidel ochrany osobních údajů (např. se bude jednat o tzv. „domácí užití“ nespadající do režimu obecného nařízení o ochraně osobních údajů nebo se nemusí jednat o zpracování osobních údajů), bude subsidiárně nastupovat ochrana osobnosti ve smyslu občanského zákoníku.

2.4 Doba trvání ochrany

Člověk je po celou dobu svého života se svou osobností a absolutním subjektivním osobnostním právem přirozeně a neodlučitelně spjat, přičemž ochrana některých osobnostních zájmů člověka za zákonem stanovených podmínek vzniká ještě před narozením člověka a v omezeném rozsahu přetrvává i po jeho smrti.[217] Jako součást osobnosti jsou tedy chráněné hodnoty, které jsou dány každému člověku od jeho narození, případně početí, a trvají po celou dobu

[216] K tomu srov. např. NONNEMANN, František. Využití nahrávky fyzické osoby jako důkazního prostředku z pohledu ochrany osobních údajů. Právní rozhledy [online]. 2015 [cit. 2022-03-26].

[217] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 290.

jeho života až do smrti, přičemž jejich ochrana není podmíněna žádnou jinou skutečností či právním jednáním.[218]

Bez pochyb je tak dán rozsah poskytované ochrany v průběhu života člověka. Před jeho narozením právo poskytuje ochranu tzv. nasciturovi, na kterého se podle § 25 o.z. hledí jako na živého. Navíc podle čl. 6 odst. 1 LZPS právo na život zahrnuje jeho ochranu i před narozením. Specifikem ochrany nascitura je jeho podmíněná ochrana (vzniká podmíněně narozením) a z hlediska ochrany osobnostních práv se tak, v případě, že se dítě narodí živé, v zásadě uplatňuje zpětně – *ex tunc*, tedy od početí.[219] V každém případě platí, že nasciturovi osobnostní práva náležejí.

Moderní právní stát zabezpečuje občanskoprávní ochranu osobnosti fyzické osobě i po její smrti (tzv. postmortální ochrana).[220] V případě smrti člověka se tak jeho osobnostních práv mohou domáhat jeho pozůstalí, resp. tedy kterákoli z osob jemu blízkých[221]. V právní teorii ani judikatuře však nepanuje jednotný názor na to, které stránky osobnosti člověka jsou předmětem této posmrtné ochrany a které nikoli[222] a stejně tak nepanuje shoda na povaze těchto práv[223]. V zásadě však panuje shoda na tom, že obsah postmortální ochrany je užší než obsah práv za života člověka.[224]

---

[218] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 291.

[219] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 517.

[220] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 81.

[221] Srov. § 82 odst. 2 o..z

[222] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 345.

[223] DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 537.

[224] RYŠKA in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 135.

Dále rovněž KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 83.

Zatímco o ochraně člověka v průběhu jeho života (a v zásadě i před jeho narozením coby nascitura) není příliš pochyb, rozsah postmortální ochrany osobnosti není jednoznačně vymezen. Zatímco napříč doktrinální praxí panuje poměrná shoda, že se tento rozsah zužuje, již není vyjasněno jak. K tomu rovněž chybí i soudní praxe, která by tento rozsah specifikovala. Pro uplatňování práva být zapomenut přitom může být postmortální ochrana v mezích ochrany osobnosti vcelku zásadní – ať už čistě z hlediska limitů dopadů ochrany poskytovanou předpisy na ochranu osobních údajů, které postmortální ochranu neposkytují (srov. kapitolu 3.3.3 níže), tak z hlediska permanence dat v digitálním světě (srov. kapitolu 4.1).

Na základě těchto skutečností se domnívám, že právo být zapomenut by mělo existovat, coby integrální součást osobnostních práv, i po smrti člověka. Odmítnutí tohoto práva by znamenalo nepřiměřený zásah do ochrany osobnosti a jejího přirozenoprávních východisek. Soukromí je totiž chráněno i po smrti člověka a může mít navíc přímý dopad na příbuzné, pozůstalé či osoby blízké nebožtíka. Proto by možnosti zapomínat a domáhat se smazání dat/informací měly existovat i po smrti. Rozsah jeho reálného aplikačního uplatnění nicméně bude vždy záležet na konkrétních skutkových okolnostech.

2.5 Ochrana „osobnosti“ právnických osob

Ústavní soud dlouhodobě přiznává základní práva i právnickým osobám, které tedy mohou nabývat a být předmětem základních lidských práv.[225] Právnické osobě svědčí taková práva, u kterých je to z povahy věci možné.[226] K obdobným závěrům dochází ESLP, který přiznává právnickým osobám soudní ochranu podle

Stejně tak DOLEŽAL T., A. DOLEŽAL in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s. 537.

Stejně tak TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 345.

[225] Srov. např. nález Ústavního soudu ze dne 19. 1. 1994, sp. zn. Pl. ÚS 15/93, nález Ústavního soudu ze dne 1. 11. 1995, sp. zn. II. ÚS 192/95, nález Ústavního soudu ze dne 3. 9. 1998, sp. zn. IV. ÚS 13/98, nebo nález Ústavního soudu ze dne 10. 7. 2008, sp. zn. III. ÚS 3118/07.

[226] Srov. např. nález Ústavního soudu ze dne 6. 1. 1998, sp. zn. I. ÚS 282/97 nebo nález Ústavního soudu ze dne 10. 7. 2008, sp. zn. III. ÚS 3118/07.

Úmluvy, pokud je taková právnická osoba dostatečně nezávislá na státu, aby ji bylo možné považovat za „nevládní organizaci“ ve smyslu čl. 34 Úmluvy.[227]

Stejně tak je tomu u práva na soukromí ve smyslu čl. 10 LZPS, které se přiznává i právnickým osobám.[228] Ústavní soud se obdobně vyjádřil např. při zvažování povahy ochrany dobré pověsti právnické osoby, které v zásadě tedy přiznal ústavní rozměr, jenž dále poměřoval s možnostmi (oprávněné) kritiky ve smyslu práva na svobodu projevu.[229]

Ochrana názvu právnické osoby tak není považována za ochranu osobnostních práv ve smyslu občanského zákoníku. Vedle předmětů přirozených osobnostních práv lidí stanoví občanský zákoník totiž předmětově obdobnou ochranu některých složek právnických osob, a to konkrétně názvu právnické osoby, její pověsti a soukromí (srov. § 135 o.z.). Z povahy věci se však nejedná o předměty práva přirozeného, nýbrž o ochranu udělenou v souvislosti s přiznáním (fikcí) právní existence právnických osob a jejich fiktivní právní osobnosti.[230] Právní ochrana hodnot nemajetkové hodnoty upínající se k právnickým osobám tedy není ochranou ve smyslu všeobecného osobnostního práva, nýbrž samostatnou ochranou[231], kterou občanský zákoník v omezeném rozsahu přiznává, a to zejména právě prostřednictvím zejména § 135 o.z. Jedná se tak v zásadě o *sui generis* úpravu, kterou zákon v omezeném rozsahu právnickým osobám poskytuje; nicméně platí, že právní prostředky dobrého jména právnické osoby jsou pak analogické s právními prostředky ochrany osobnosti.[232] Podle Nejvyššího

[227] Srov. např. rozhodnutí ESLP ze dne 10. 7. 2006 ve věci 19101/03 - Sdružení Jihočeské matky proti České republice; nebo KMEC, Jiří. Evropská úmluva o lidských právech: komentář. Praha: C.H. Beck, 2012, xxvii, 1660 s. ISBN 978-80-7400-365-3, s. 26.

[228] PAVLÍČEK, Václav, Ján GRONSKÝ, Jiří HŘEBEJK, et al. Ústavní právo a státověda. II. díl, Ústavní právo České republiky. 3. vydání. Praha: Leges, 2020, 1160 s. ISBN 978-80-7502-468-8, s. 524.

[229] Srov. nález Ústavního soudu ze dne 20. února 2018, I. ÚS 3819/14.

[230] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 292.

[231] KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 73.

[232] ROZEHNAL, Ales. Mediální právo, 2. vydání. ISBN 80-7380-549-9, s. 217.

soudu se tak jedná v zásadě o „zvláštní“ osobní právo.[233] V jistém slova smyslu lze proto hovořit o celkové „osobnosti“ právnické osoby, která je dána několika samotnými atributy (pozitivní i negativní složky).[234]

Rovněž ochrana názvu právnické osoby působí vůči každému (*erga omnes*). Zasáhne-li tak kdokoliv do práva k názvu právnické osoby ve smyslu § 135 odst. 1, náležejí právnické osobě práva zakotvená v tomto ustanovení.[235] Obdobná práva pak náleží právnické osobě, pokud dojde ke kvalifikovanému zásahu do její pověsti nebo soukromí právnické osoby ve smyslu § 135 odst. 2 o.z. (tj. bez zákonného důvodu zásahu do chráněných složek, ledaže se jedná o účely vědecké či umělecké nebo o tiskové, rozhlasové, televizní nebo obdobné zpravodajství; ani takový zásah však nesmí být v rozporu s oprávněnými zájmy právnické osoby).

Podle judikatury Nejvyššího soudu[236] zároveň sama skutečnost, že právní osobnost člověka a právnické osoby není z povahy věci totožná, nebrání tomu, aby závěry přijaté v rámci ochrany osobnosti člověka nemohly být (jsou-li pro posuzovanou věc přiléhavé) uplatněny i při výkladu ochrany „osobnosti“ právnických osob (zejména tedy ve smyslu § 135 o.z.).[237]

Ochrana „osobnosti“ právnické osoby zahrnuje zejména ochranu dobrého jména, pověsti a soukromí právnické osoby. Ačkoliv se nejedná o „standardní“ ochranu všeobecných osobnostních práv, která český právní řád přiznává fyzickým osobám, tyto jednotlivé složky jsou specificky chráněny dle § 135 o.z. Tato ochrana má zároveň ústavně-právní garance, když v zásadě provádí právo

---

[233] Srov. rozhodnutí Nejvyšší soudu ze dne 18. března 2007, 30 Cdo 1385/2006, podle kterého: *„Dobrá pověst právnické osoby vzniká okamžikem vzniku právnické osoby a trvá po celou dobu její existence. Dobrá pověst právnické osoby má - podobně jako název právnické osoby - povahu osobního práva.“*

[234] TOMAN, Petr a Stanislav DEVÁTÝ. Ochrana dobré pověsti a názvu právnických osob. 2. aktualiz. a dopl. vyd. Praha: Linde, 2001, 199 s. ISBN 80-7201-297-5, s. 38.

[235] LASÁK in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 521.

[236] Srov. např. rozhodnutí Nejvyššího soudu ze dne 3. září 2002, sp. zn. 28 Cdo 1375/2002, nebo usnesení Nejvyššího soudu ze dne 26. června 2014, sp. zn. 23 Cdo 1323/2012.

[237] JANOŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s. 207.

na soukromí ve smyslu čl. 10 LZPS, které je právnickým osobám rovněž poskytováno. Z těchto důvodů se domnívám, že i právnickým osobám náleží právo být zapomenut. Nicméně bude platit, že rozsah poskytované ochrany bude obecně užší než u lidí.

2.6 Závěr

Osobnost je velmi rozmanitý pojem, který představuje spojení biologických, psychologických a společenských aspektů, či spíš hodnot lidské osobnosti. Představuje předmět vrozených osobnostních práv člověka a zahrnuje vše, čím se člověk projevuje navenek ve vztahu ke svému okolí, a to po stránce fyzické, duchovní a duševní. Ochrana osobnosti přitom vyplývá z přirozenoprávní vědy a poprvé začala být na našem území chráněna v rámci obecných pravidel chránících přirozená práva člověka. V socialistickém státě nebyl na přirozená práva, tedy ani osobnost či soukromí člověka kladen důraz a v popředí tehdejšího prosazovaného světonázoru stál spíše občan a jeho úloha v (socialistické) společnosti. Občan byl středem ochrany i po přijetí ústavy z roku 1960 a občanského zákoníku v roce 1964, nicméně tehdejší právní úprava přinášela poměrně komplexní ochranu osobnosti; k návratu k přirozenoprávnímu pojetí člověka, jeho osobnosti i soukromí však došlo až po revoluci, konkrétně přijetím Listiny základních práv a svobod v roce 1991.

Dnešní pojetí ochrany osobnosti plynně navazuje na přirozenoprávní pojetí ochrany osobnosti, která je rovněž chráněna jako základní lidské právo každého člověka. Ochrana osobnosti je poskytována na úrovni lidskoprávních mezinárodních dohod (například v Úmluvě o ochraně lidských práv a základních svobod), na úrovni práva Evropské unie (zejména v Listině EU) i v ústavní rovině (v Listině základních práv a svobod, která je však v souladu s principy monistického pojetí lidskoprávních mezinárodních dohod přímo spojená se všemi těmito mezinárodního dohodami a jimi doplňovaná). Občanský zákoník poskytuje ochranu osobnosti na úrovni tzv. generální klauzule (§ 81 o.z.), která je následně provedena a specifikována pro některé složky (ochrany) osobnosti jednotlivými ustanoveními oddílu 6 hlavy II části první (tj. v § 81 až § 114).

Osobnost je multidimenzionální pojem a obdobně je koncipována její ochrana v právním systému. Občanský zákoník neposkytuje taxativní výčet všech složek osobnosti nebo jejich částí ochrany a výčet je čistě demonstrativní – subsidiárně vždy chráněný generální klauzulí. Osobnost člověka (a stejně tak jeho ochrana) je tedy ucelený celek hodnot, který tak jakožto jednotu dílčích osobnostních práv vytváří všeobecné osobnostní právo. Dílčí osobnostní práva se vážou k jednotlivým hodnotám lidské osobnosti, avšak jsou vždy pouhou součástí tohoto celku. Jednotlivé osobnostní atributy (dílčí práva) jsou součástí jediného práva a vytvářejí monistickou koncepci lidské osobnosti; nelze tak hovořit o několika osobnostních právech, ale jen o celku této ochrany. Tato dílčí práva se navíc stále rozvíjejí spolu s rozvojem společnosti a jejích potřeb. Součástí osobnosti se tak stalo i právo být zapomenut, které představuje jedno z dílčích práv inherentně spojených s osobností. I právo být zapomenut tak bude působit *erga omnes*, ale vždy jen v rozsahu, ve kterém lze poskytovat ochranu osobnosti jako celku. Z tohoto hlediska se tedy jedná o relativní právo, jehož uplatnění není neomezené, a je vždy nezbytné jej v souladu s principy proporcionality poměřovat a balancovat s jinými chráněnými zájmy.

K legitimním zásahům do osobnosti může docházet jen v předem předvídaných situacích, jak plyne z přirozenoprávní povahy těchto práv a jejich lidskoprávní ochrany. Kromě svolení k zásahu ze strany daného člověka budou vždy zásadní především zákonem povolené zásahy, resp. zásahy při plnění právních povinností – jinými slovy zásahy předem aprobované zákonem, které zákonodárce buď výslovně povoluje, nebo předvídá. Zákonodárce musí vždy vycházet z principů proporcionality a musí ctít charakter těchto práv. Pokud by došlo k zásahu nad rámec těchto legitimně předvídaných situací, bude moci dojít, kromě jiného, k uplatnění práva být zapomenut.

Právo být zapomenut, coby integrální součást osobnosti, má tedy rovněž svou pozitivní a negativní složku – člověk nejen disponuje možností své právo být zapomenut užívat a v mezích právního řádu s ním i disponovat (pozitivní složka), ale v případě jeho porušení se jej domáhat a dožadovat se právní ochrany (negativní složka). Zejména z hlediska konkrétní ochrany však bude hrát velký význam ochrana osobních údajů (srov. kapitolu 3) a v zásadě subsidiárně bude

vystupovat uplatňování práva být zapomenut mimo oblast ochrany osobních údajů (civilněprávně) – bude se tak zpravidla jednat o případy, kdy nebude možné postupovat podle pravidel ochrany osobních údajů (např. se bude jednat o tzv. „domácí užití“ nespadající do režimu obecného nařízení o ochraně osobních údajů).

S tím souvisí i doba trvání poskytované ochrany. Zatímco pravidla ochrany osobních údajů zpravidla působí jen za života člověka, civilněprávní ochrana osobnosti, a tedy i možnosti uplatňování práva být zapomenut, budou bez výjimky vždy náležet i nasciturovi a stejně tak zemřelým v rámci jejich postmortální ochrany osobnosti. Ačkoliv platí, že po smrti dochází k zúžení poskytované ochrany, nelze právo být zapomenut (zcela) vyloučit z postmortální ochrany osobnosti člověka. Odmítnutí tohoto práva by znamenalo nepřiměřený zásah do ochrany osobnosti a jejích přirozenoprávních východisek. Soukromí je totiž chráněno i po smrti člověka a jeho narušování může mít přímý dopad na příbuzné, pozůstalé či osoby blízké nebožtíka. Proto by možnost zapomínat a domáhat se smazání dat/informací měly existovat i po smrti. Rozsah jeho reálného aplikačního uplatnění nicméně bude vždy záležet na konkrétních skutkových okolnostech.

Domnívám se, že právo být zapomenut nenáleží pouze fyzickým osobám (lidem), ale rovněž osobám právnickým. Ochrana „osobnosti“ právnické osoby zahrnuje zejména ochranu dobrého jména, pověsti a soukromí právnické osoby, která má zároveň ústavně-právní garance v podobě práva na soukromí ve smyslu čl. 10 LZPS. Ačkoliv se nejedná o „standardní“ ochranu všeobecných osobnostních práv, která český právní řád přiznává fyzickým osobám, tyto jednotlivé složky jsou specificky chráněny dle § 135 o.z. Proto dovozuji, že i právnickým osobám náleží právo být zapomenut, ač tedy rozsah poskytované ochrany bude obecně užší než u lidí.

3 Právo na ochranu osobních údajů

3.1 Základní relevantní pojmy ochrany osobních údajů

V této kapitole blíže analyzuji některé vybrané pojmy právní oblasti ochrany osobních údajů. Cílem této práce není poskytnout komentářový výklad všech pojmů, se kterými právní předpisy ochrany osobních údajů (zejména tedy obecné nařízení o ochraně osobních údajů) pracují. V této práci se zaměřuji pouze na několik vybraných pojmů, jejichž výklad považuji za významný pro uplatnitelnost práva být zapomenut. Z hlavních pojmů, se kterými v této práci běžně pracuji, avšak nejsou blíže analyzovány, se jedná zejména o pojmy správce[238] a zpracovatel[239] osobních údajů, kde bez dalšího vycházím z jejich definice v GDPR a nepodrobuji je bližší analýze.

3.1.1 Osobní údaj a subjekt údajů

Obecné nařízení o ochraně osobních údajů definuje osobní údaje jako „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“[240]

Jedná se tedy o jakékoliv údaje, které přímo identifikují konkrétní fyzickou osobu, slovy nařízení tedy tzv. subjekt údajů, nebo jsou tento subjekt údajů schopné identifikovat (zpravidla ve spojení s dalšími údaji). a contrario platí, že takový údaj (data), který nenaplňuje tyto kvality, nespadá pod ochranu poskytovanou GDPR.[241] Takový příkladem může být např. telefonní číslo – tel. číslo veřejné

[238] Srov. čl. 4 odst. 7 GDPR.

[239] Srov. čl. 4 odst. 8 GDPR.

[240] Článek 4 odst. 1 GDPR.

[241] PINKAVOVÁ, A. a FOŘT, F. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 61.

telefonní budky samo o sobě osobním údajem nebude[242], ale mohlo by jím např. ve spojení se záběrem z kamerového systému či jinými dalšími údaji, které by vedly k identifikaci konkrétní osoby. Jak připomněl Soudní dvůr EU např. v případě YS[243], je rovněž důležité rozlišovat mezi osobním údajem a nosičem takového osobního údaje, resp. tedy dokumentem, ve kterém je osobní údaj zachycen – dokument obsahující osobní údaje (v posuzovaném případě správní rozhodnutí týkající se poskytnutí azylu) se jako osobní údaj nekvalifikuje a nelze na něj tedy uplatnit právo na přístup.

Každý osobní údaj tak má čtyři základní definiční znaky: (i) jakákoliv informace [tj. „*veškeré informace*“, v anglickém znění „*any information*“] bez ohledu na její povahu, obsah a formu, (ii) vztahující se [angl. *„relating to“*] k osobě, (iii) tato osoba je identifikovaná nebo identifikovatelná [angl. *„identified or identifiable“*] a (iv) předchozí tři podmínky se týkají fyzické osoby [angl. *„natural person“*].[244]

V každém případě platí, že definice pojmu osobního údaje je velmi široká a neustále se rozšiřující, kdy dochází k rozšiřování tohoto pojmu prostřednictvím soudního výkladu. To souvisí rovněž s exponenciálním nárůstem shromažďování různých identifikátorů v online prostředí v posledních letech.[245] Takto došlo např. k rozšíření definice o IP adresy v situaci, v níž je možné určit konkrétního uživatele[246], nebo pak o dynamickou IP adresu[247] (tj. taková IP adresa, která je uživateli přiřazována na základě komunikace jeho zařízení s poskytovatelem připojení na tzv. dobu zapůjčení).

---

[242] PINKAVOVÁ, A. a FOŘT, F. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 63.

[243] Rozsudek Soudního dvora Evropské unie ze dne 17. července 2014 ve věci C-141/12 a C-372/12 – YS a další.

[244] POKORNÁ, Andrea. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek. Praha: Wolters Kluwer ČR, 2020, xviii, 331. ISBN 978-80-7598-309-1, s. 9.

[245] PINKAVOVÁ, A. a FOŘT, F. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 63.

[246] Rozhodnutí Soudního dvora Evropské unie ze dne 24. listopadu 2011 ve věci C-70/10 Scarlet Extended.

[247] Rozhodnutí Soudního dvora Evropské unie ze dne 19. října 2016 ve věci C-582/14 Patrick Breyer v. Bundesrepublik Deutschland.

Výčet osobních údajů tak není taxativní ani definitivní. Soudní praxe kazuisticky hodnotí, v jakých případech se daný identifikátor kvalifikuje jako osobní údaj, přičemž ne vždy platí, že pokud se v jednom případě daný údaj identifikuje jako osobní údaj ve smyslu čl. 4 GDPR, bude tomu tak i v jiných případech. V tomto případě je možné poukázat právě na příklad dynamické IP adresy, která se kvalifikují jako osobní údaj jen v subjektivních případech – tj. v takových případech, kdy držitel takového údaje bude mít dostačující právní prostředky (např. tedy možnost si vyžádat od třetí osoby, jakou je např. poskytovatel internetového připojení, doplňující údaje spojené s IP adresou[248]).

Subjektivní vymezení definice osobních údajů je pak významné zejména v případě nepřímých identifikátorů, tedy takových údajů, které ve svém souhrnu mohou identifikovat konkrétní subjekt údajů, avšak pouze za předpokladu, že daný držitel této množiny dat disponuje takovým množstvím údajů, které mu umožní osobu identifikovat, anebo alespoň takovými právními prostředky, které mu umožní takové údaje získat.[249] Cílem definice „osobních údajů" v obecném nařízení o ochraně osobních údajů má tak být co největší flexibilita zahrnující jakékoli informace, které se mohou týkat fyzické osoby.[250] Platí pak, že vztah k *identifikovatelné* osobě může být jak přímý, tak nepřímý.[251]

Příkladem jsou zejména výše uvedené IP adresy. Zároveň platí, že právní rozbor, ačkoliv obsahuje osobní údaje konkrétní fyzické osoby, jako celek osobní údaj netvoří.[252] Naopak osobním údajem bude pracovní evidence zaměstnance, která

[248] MATYSOVÁ, Monika, Robert NEŠPŮREK a Richard OTEVŘEL. Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj: 24.05.2017 [online]. [cit. 2022-03-16]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj.

[249] PINKAVOVÁ, A. a FOŘT, F. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 63.

[250] RÜCKER, D. in KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0, s. 13.

[251] RÜCKER, D. in KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0, s. 14.

[252] K tomu srov. rozsudek Soudního dvora Evropské unie ze dne 17- července 2014 ve spojených věcech C-141/12 and C-372/12, YS (C-141/12) proti Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel (C-372/12) proti M, S.

obsahuje informace o tom, v kolik jednotliví pracovníci začínají a končí svou pracovní dobu.[253]

3.1.2 Specifické kategorie osobních údajů

3.1.2.1 Zvláštní kategorie osobních údajů

Zvláštní ochrany dále požívají tzv. zvláštní kategorie osobních údajů[254], které jsou vymezené v čl. 9 odst. 1 GDPR a jejichž zpracování je povolené pouze při splnění některé z taxativně stanovených výjimek v čl. 9 odst. 2 GDPR. Jedná se tedy o takové osobní 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.“*[255]

I v případě těchto zvláštních kategorií je nezbytné nuancovat kontext takového zpracování. Ačkoliv tak např. definice těchto zvláštních kategorií osobních údajů výslovně zahrnuje osobní údaje o politických názorech[256], dle Ústavního soudu[257] nelze bez dalšího údaj o členství v komunistické straně považovat za citlivý údaj. O citlivý údaj nejde dle názoru Ústavního soudu vzhledem k výraznému přesahu do sféry veřejné, jelikož smyslem členství v politické straně je úsilí podílet se na správě věcí veřejných či přímo působit ve veřejném životě.[258]

Za důležité pak stojí připomenout, že údaje o dětech nejsou specificky chráněné ve smyslu těchto zvláštních kategorií osobních údajů; obecné nařízení o ochraně

[253] Rozsudek Soudního dvora Evropské unie ze dne 30. května 2013 ve věci C-342/12 Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT).

[254] Ty byly v předcházející právní úpravě dle směrnice 95/46/ES a zákona č. 101/2000 označované jako tzv. citlivé údaje.

[255] Článek 9 odst. 1 GDPR.

[256] a stejně tak tomu bylo v případě směrnice 95/46/ES, podle kterého se zvláštní kategorie ve smyslu čl. 8 odst. 1 této směrnice považovaly *„osobní údaje, které odhalují […] politické názory“*.

[257] Srov. Nález Ústavního soudu ze dne 15. 11. 2010, sp. zn. I. ÚS 517/10.

[258] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 140.

osobních údajů pouze stanoví některá specifická pravidla pro získávání souhlasu v čl. 8 GDPR.[259] Stejně tak nejsou žádným zvláštním způsobem chráněna rodná čísla[260], ač jejich ochrana bývá v českém právním prostředí často velmi zdůrazňována.[261]

3.1.2.2 Zvláštní kategorie osobních údajů – biometrické údaje

Za zcela specifickou kategorií osobních údajů lze považovat biometrické údaje[262]. Ty jsou chráněné jako zvláštní kategorie osobních údajů, jejichž zpracování podléhá režimu článku 9 GDPR pouze v případě, že jsou zpracovávané „*za účelem jedinečné identifikace fyzické osoby*“, kde tedy zároveň platí, že musí naplňovat definici biometrických údajů, a tedy umožňovat nebo potvrzovat jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.[263]

Aby se tedy jednalo o zpracování biometrických údajů podléhající čl. 9 GDPR, musejí tyto (i) vyplývat z technického zpracování fyzických či fyziologických znaků, (ii) umožňovat jedinečnou identifikaci fyzické osoby a (iii) účelem jejich zpracování musí být jedinečná identifikace.[264]

---

[259] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 138.

[260] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 138.

[261] K tomu rovněž srov. stanovisko Úřadu pro ochranu osobních údajů K využívání rodných čísel [online]. 21.3.2013. Dostupné z https://www.uoou.cz/k-vyuzivani-rodnych-cisel/d-1600#:~:text=Vzhledem%20k%20tomu%2C%20%C5%BEe%20rodn%C3%A9,lex%20specialis%20k%20tomuto%20z%C3%A1konu.

[262] Ty jsou blíže definovány v čl. 4 odst. 14 GDPR, podle kterého se biometrickými údaji rozumí takové „*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.*“

[263] Čl. 4 odst. 14 GDPR.

[264] POKORNÁ, Andrea. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek. Praha: Wolters Kluwer ČR, 2020, xviii, 331. ISBN 978-80-7598-309-1, s. 287.

Např. zdroje biometrických údajů, jako jsou např. vzorky lidských tkání, nejsou samy o sobě považovány za biometrické údaje.[265] Nakládání s fotografiemi by pak nemělo být systematicky považováno za zpracování biometrických údajů za účelem identifikace osoby, pokud není stanoveno jinak.[266] Naopak využívání biometrických podpisů pro autentizaci fyzické osoby porovnáním jejích biometrických údajů s identitou uvedenou v databázi (1:1) se jako takové zpracování biometrických údajů dle čl. 9 GDPR kvalifikovat bude.[267] Pravidla dle čl. 9 odst. 1 GDPR by se v každém případě měla vztahovat jak na případy autentizace, tak identifikace.[268]

3.1.2.3 Osobní údaje týkající se trestních věcí a trestných činů

Obecné nařízení o ochraně osobních údajů pak zcela samostatně dále vyčleňuje *„osobní údaje týkající se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření“*, které lze podle čl. 10 GDPR zpracovávat pouze pod dozorem orgánu veřejné moci nebo pokud tak předvídá právo EU nebo členského státu.[269] Od účinnosti obecného nařízení o ochraně osobních údajů se přitom jedná o odchýlení se od dosavadní praxe, jelikož zákon č. 101/2000 údaj o „odsouzení za trestný čin“ považoval za citlivý údaj[270] a nepovažoval tento typ údajů za separátní kategorii osobních údajů. Zároveň došlo k rozšíření takto chráněných údajů, kdy režimu tohoto čl. 10 GDPR podléhají nejen soudní rozhodnutí o uznání viny, ale rovněž ostatní osobní údaje, např. údaje o zastavení

[265] Pracovní skupina pro ochranu osobních údajů zřízené podle čl. 29, čj. 00720/12/EN, WP 193, Stanovisko č. 3/2012 k vývoji biometrických technologií, ze dne 27. dubna 2012, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_cs.pdf.

[266] K tomu srov. bod 51 úvodních ustanovení GDPR, podle kterého by se na zpracování fotografií by systematicky považovat za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby.

[267] POKORNÁ, Andrea. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek. Praha: Wolters Kluwer ČR, 2020, xviii, 331. ISBN 978-80-7598-309-1, s. 288.

[268] MATEJKA, Ján, Alžběta KRAUSOVÁ a Vojen GÜTTLER. Biometric data and its specific legal protection. Praha: Institute of State and Law of the Czech Academy of Sciences, [2020]. ISBN 978-80-87439-43-2, s. 36.

[269] Srov. čl. 10 GDPR.

[270] Ve smyslu dle čl. 4 písm. b) ZOOÚ; dnes tedy jako zvláštní kategorie osobních údajů ve smyslu čl. 9 odst. 1 GDPR.

trestního stíhání, které dle zákona č. 101/2000 byly považované za „standardní“ osobní údaje.[271]

Zpracování těchto údajů tak primárně spadá pod působnost směrnice 2016/680, která je v českém právním řádu implementována v zákoně o zpracování osobních údajů (především tedy pak Hlavě III tohoto zákona).

3.1.3 Zpracování osobních údajů

Zpracováním osobních údajů se podle čl. 4 odst. 2 GDPR rozumí *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“*.

V zásadě se tak jedná o jakoukoliv operaci související s osobními údaji. Jedná se tak o činnost, kterou provádí správce[272] či zpracovatel[273] za konkrétním účelem, a to bez ohledu na prostředky, jimiž je zpracování prováděno.[274] Jedná se o jakoukoliv jednotlivou operaci nebo soubor operací, jejichž demonstrativní výčet je zahrnut přímo v definici výše. Soubor operací se pak může týkat situací, kdy s danými osobními údaji nakládá jedna osoba (správce či zpracovatel), ale rovněž když v sérii paralelních nebo na sobě navazujících krocích se stejným souborem údajů nakládá více než jedna osoba.[275]

---

[271] VIMPELOVÁ M. a KRÁL, Š. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 37 - 39.

[272] K pojmu správce viz čl. 4 odst. odst. 7 GDPR.

[273] K pojmu zpracovatel viz čl. 4 odst. 8 GDPR.

[274] PINKAVOVÁ A. a FOŘT, F. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 64.

[275] RÜCKER, D. in KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0, s. 10.

Pro účely práva být zapomenut, a tedy této práce, je pak zásadní, že se zpracováním rozumí i jakékoli „finální“ operace (či soubor operací) s osobním údajem, jako je zejména jeho výmaz, případně anonymizace.

Zpracováním je pak rovněž načítání obsahu webových stránek[276], stejně jako činnost vyhledávače spočívající ve vyhledávání informací zveřejněných nebo umístěných na internetu třetími osobami, v jejich automatickém indexování, v jejich dočasném ukládání a konečně v jejich poskytování uživatelům internetu v určitém preferenčním pořadí.[277]

K vymezení pojmu zpracování je pak rovněž zásadní věcné vymezení působnosti celého obecného nařízení osobních údajů – zejména pak automatizovaného zpracování (k tomu viz kapitola 3.2.2.1 níže) a neautomatizovaného zpracování (k tomu pak kapitola 3.2.2.2 níže).

3.1.4 Právní základ zpracování

Jakékoliv zpracování osobních údajů musí být založené na platném právním základu ve smyslu čl. 6 odst. 1 GDPR.[278] Ten tak podrobně rozebírá nejdůležitější zásady obecného nařízení o ochraně osobních údajů, tedy zásadu zákonnosti zpracování dle čl. 5 odst. 1 písm. a) GDPR a částečně i zásady účelového omezení vyjádřené v čl. 5 odst. v čl. 5 odst. 1 písm. a) GDPR.[279]

Zpracování konkrétního setu údajů může být pro jeden nebo více účelů, a tedy rovněž na základě jednoho nebo více právních základů stanovených v čl. 6 odst. 1 GDPR.[280] Hlavními, resp. v praxi nejvyužívanějšími, právními základy pro

[276] Rozhodnutí Soudního dvora Evropské unie ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist.

[277] Rozhodnutí Soudního dvora Evropské unie ve věci Google Spain (rozhodnutí ze dne 13. května 2014, ve věci C-131/12).

[278] Srov. znění uvozovací věty ustanovení čl. 6 odst. 1 GDPR: *„Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu“.*

[279] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 88.

[280] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 89.

zpracování osobních údajů je pak plnění smluvních povinností[281], plnění právní povinnosti[282] a oprávněný zájem správce či třetí strany[283]. Za zcela specifický právní základ zpracování osobních údajů lze pak považovat souhlas subjektu údajů[284], na který obecné nařízení o ochraně osobních údajů klade další specifika[285] a který by v zásadě měl být využíván jen subsidiárně, v případech, kdy jiné právní základy již nepřicházejí v úvahu. Pokud ke zpracování osobních údajů pro daný účel dojde na základě souhlasu, je nezbytné tento právní základ zachovávat a nelze jej dále měnit.[286]

Pro zvláštní kategorie osobních údajů pak dále platí, že musí naplňovat rovněž některou z výjimek stanovených v čl. 9 odst. 2 GDPR. Pro podrobnější vymezení vztahu mezi čl. 9 odst. 2 a čl. 6 odst. 1 GDPR pak srov. kapitolu 4.3.2 této práce (specificky tedy ve vztahu ke zpracování zveřejněných osobních údajů).

3.1.5 Anonymizace osobních údajů

Pro účely této práce a vymezení možností práva být zapomenut je rovněž významný pojem anonymizace osobních údajů. K dopadům anonymizace na právo být zapomenut pak srov. zejména možnosti výmazu osobních údajů v kapitole 6.2.3 níže.

Obecné nařízení o ochraně osobních údajů ani jiné předpisy anonymizaci ani anonymní či anonymizované osobní údaje nijak blíže nespecifikují. Pouze v bodu 26 úvodních ustanovení GDPR nalezneme zmínku, podle které se anonymní ani anonymizované údaje nepovažují za osobní údaje, a tedy na ně nedopadají

[281] Rep. *„zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“* ve smyslu čl. 6 odst. 1 písm. b) GDPR.

[282] Resp. *„zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje“* ve smyslu čl. 6 odst. 1 písm. c) GDPR.

[283] Resp. *„zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě“* ve smyslu čl. 6 odst. 1 písm. f) GDPR.

[284] Resp. *„subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů“* ve smyslu čl. 6 odst. 1 písm. a) GDPR.

[285] Srov. zejména čl. 7 GDPR.

[286] Srov. rovněž Guidelines 05/2020 on consent under Regulation 2016/679. [online]. [cit. 2022-03-14]. Dostupné z https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

pravidla o ochraně a zpracování osobních údajů ve smyslu GDPR.[287] V případě, kdy daná informace neidentifikuje ani není způsobilá identifikovat fyzickou osobu, bude se jednat o anonymní údaj/informace mimo rámec GDPR.[288]

Rozsah anonymizace, tedy zajištění toho, že konkrétní set údajů bude skutečně anonymní a nebude moci sloužit k identifikaci (přímé, nepřímé či jen hypotetické ve spojení s dalšími údaji), pak záleží na konkrétní situaci, kterou by měl správce údajů vždy vyhodnotit v kontextu konkrétních zpracovatelských činností.

Jako vzorový příklad anonymizace v konkrétní praxi lze použít anonymizaci soudních rozhodnutí – ať už ve smyslu jejich zveřejňování nebo zpřístupňování veřejnosti na základě práva na informace a ve smyslu zákona o svobodném přístupu k informacím. Zejména v případě zpřístupnění soudních rozhodnutí na žádost (ve smyslu zákona o svobodném přístupu k informacím) platí, že soud by měl vždy zvažovat možnost anonymizace a její rozsah; pro tyto účely by měl zvažovat rozpoznatelnost konkrétní osoby (např. pachatele trestného činu, kterého se rozhodnutí týká, případně žalobce/žalované) podle osobních údajů, ale rovněž pohnutky žadatele, a dále také zájem žadatele či veřejnosti na znalosti těchto údajů.[289] Soud v takovém případě tedy musí balancovat právo na přístup k informacím a ochranu osobních údajů a soukromí dotčených osob.[290] Ač může být tento příklad poměrně extrémní – a to zejména vzhledem ke specifickým povinnostem soudní moci k ochraně základních práv[291], interním instrukcím

[287] Srov. bod 26 úvodních ustanovení GDPR, podle kterého: *„Zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným. Toto nařízení se tedy netýká zpracování těchto anonymních informací, včetně zpracování pro statistické nebo výzkumné účely.“*

[288] DIENST, S. in KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0, s. 13

[289] GEALFOW, John Altair a Christian MAY. Anonymizace osobních údajů v soudních rozhodnutích. Revue pro právo a technologie [online]. 2019, 10(19), 3 [cit. 2022-03-16]. ISSN 1804-5383, s. 19. Dostupné z: https://www-ceeol-com.ezproxy.is.cuni.cz/search/viewpdf?id=797575.

[290] GEALFOW, John Altair a Christian MAY. Anonymizace osobních údajů v soudních rozhodnutích. Revue pro právo a technologie [online]. 2019, 10(19), 3 [cit. 2022-03-16]. ISSN 1804-5383, s. 19. Dostupné z: https://www-ceeol-com.ezproxy.is.cuni.cz/search/viewpdf?id=797575.

[291] K otázce ochrany základních práv soudní soustavou srov. nález Ústavního soudu ze dne 21. října 2008, sp. zn. IV. ÚS 1735/07.

Ministerstva spravedlnosti[292], ale rovněž k některým specifickým zákonným povinnostem[293], např. Ústavního soudu – je názornou ukázkou problematiky anonymizace, na které vysvětluje, že anonymizaci je vždy nezbytné poměřovat a aplikovat v konkrétním kontextu a nelze ji vykládat plošně.[294]

Anonymizace je rovněž významný nástrojem ochrany osobnosti v případě poskytování informací ve smyslu zákona o svobodném přístupu k informacím.[295] To připomněl Nejvyšší správní soud, když zvažoval možnosti zpřístupnění zvukového záznamu ze zasedání zastupitelstva obce, kde NSS konstatoval, že povinný subjekt je povinen poskytnout informaci v plném rozsahu v anonymizované podobě, tedy bez chráněných osobních údajů, a to bez ohledu na to, že jsou zachyceny jako zvukový záznam.[296]

I anonymizovaný soubor údajů tak může představovat pro subjekty údajů (zbytkové) riziko.[297] V zásadě tak platí, že i anonymizovaný set se může v čase (znovu) kvalifikovat jako osobní údaj(e), který je schopen identifikovat konkrétní subjekt údajů. Na anonymizaci tudíž nelze pohlížet jako na jednorázový úkon

[292] Instrukce Ministerstva spravedlnosti ze dne 24. července 2009, č.j. 13/2008-SOSV-SP,kterou se provádějí některá ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

[293] Srov. § 59 odst. 3 zákona 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů.

[294] V rámci zveřejňování soudních rozhodnutí rovněž může přicházet v úvahu právo být zapomenut – ačkoliv se v poměrně značném množství případů domáhají výmazu svých údajů (s odvoláním na právo být zapomenut ve smyslu čl. 17 GDPR – k tomu srov. kapitolu 6 této práce) – správní soudy standardně tyto námitky zamítají právě s odkazem na standardní pravidla anonymizace a nedostatečnou souvislost s materií dané věcí.

K tomu pak srov. např. rozsudek Městského soudu ze dne 8. 11. 2021, 1 a 61/2020 – 35 nebo rozsudek Krajského osudu v Hradci Králové ze dne 16. 7. 2020, 32 a 7/2018 – 39.

[295] Podle § 8a odst. 1 zákona svobodném přístupu k informacím platí, že *„informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu.“*

[296] Rozsudek Nejvyššího správního soudu ze dne 27. února 2014, sp. zn. 7 As 20/2013 – 23.

[297] Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

a správci údajů by měli související rizika pravidelně přehodnocovat[298]. Mělo by se tak jednat o opakovaný, pravidelný proces.[299]

Anonymizace osobních údajů se kvalifikuje jako zpracovatelská operace[300], která je však obecně slučitelná s původním účelem zpracování (správce si tak zpravidla odůvodní oprávněný zájem ve smyslu čl. 6 odst. 1 písm. f) GDPR k provedení takové anonymizace původního setu osobních údajů).[301]

Existuje několik možností anonymizace, přičemž jako základní jsou vyzdvihovány randomizace[302] a generalizace[303] osobních údajů. Jako jednu z možností postupné anonymizace je rovněž možné pro správce zvážit dvoukolový proces – v prvním kroku provede pseudonymizaci[304] osobních údajů, a jakmile nejsou pseudonymizované údaje třeba, může smazat identifikátory a tím údaje nenávratně smazat a ponechat si tak pouze údaje neumožňující identifikaci

[298] Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[299] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3, s. 122.

[300] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3, s. 99.

[301] Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[302] Tj. skupina technik, kterými se mění věrohodnost údajů, čímž je odstraněna silná vazba mezi údaji a fyzickou osobou; přičemž randomizace samotná neubere žádnému záznamu na jedinečnosti, neboť každý záznam bude nadále odvozen od jediného subjektu údajů. V podrobnostech pak Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[303] Tj. proces spočívající v generalizování nebo naředění atributů subjektů údajů tak, že se pozmění příslušné měřítko nebo řád (tj. region místo města, měsíc místo týdne). V podrobnostech pak Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[304] Pojem pseudonymizace je definován přímo na úrovni obecného nařízení o ochraně osobních údajů – konkrétně v čl. 4 odst. 5 GDPR, podle kterého se jedná o *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“*

fyzických osob.[305] K takovému postupu je však nezbytné zvolit vhodný postup pseudonymizace[306] (kterým může být např. tzv. tokenizace), který následně umožní z pseudonymizovaného setu osobních údajů vytvořit údaje anonymní.

K nalezení optimálního řešení tak vždy bude nezbytné zvažovat konkrétní situaci a opatření vhodné pro daný případ.[307] Vzhledem k tomu, že Evropská unie neposkytuje žádný standard anonymizace, správce by měl vždy zvažovat co nejúčinnější metody anonymizace, včetně např. potenciální kombinace randomizace a generalizace.[308]

3.2 Působnost práva na ochranu osobních údajů

3.2.1 Rozsah ochrany poskytované GDPR[309]

Podle čl. 1 odst. 2 GDPR toto nařízení poskytuje fyzickým osobám ochranu základních práv a svobod v souvislosti se zpracováním jejich osobních údajů, a to bez ohledu na jejich státní příslušnost nebo bydliště (k místní působnosti obecného nařízení o ochraně osobních údajů viz kapitola 3.2.3 níže). Podle čl. 1 odst. 2 GDPR toto nařízení upravuje zejména právo na ochranu osobních údajů.

---

[305] PATTYNOVÁ, J. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 81-82.

[306] K tomu rovněž srov. Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[307] Council of Europe, European Union Agency for Fundamental Rights: "Handbook on European data protection law" Luxembourg, 2018, ISBN 978-92-871-9849-5, s. 93.

[308] VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7, s. 15.

[309] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

Formulace *„zejména“* naznačuje, že nařízení se netýká výlučně ochrany osobních údajů a že dopady nařízení je nutné vykládat šířeji. Nařízení kromě práv subjektů údajů na ochranu jejich osobních údajů rovněž upravuje povinnosti členských států a dozorových úřadů, včetně podmínek jejich spolupráce. Rovněž se stanoví podmínky pro vedení soudních řízení a podávání stížností souvisejících s ochranou osobních údajů.

Formulace, že GDPR chrání „práva a svobody fyzických osob, *zejména* jejich právo na ochranu osobních údajů“, může evokovat širší aplikaci i ve vztahu k chráněným lidským právům a může se zdát, že GDPR cílí zároveň na ochranu soukromí fyzických osob jako celku. Čl. 1 odst. 1 a body odůvodnění 1, 2, 10 a další uvádějí souvislost ochrany osob se zpracováním osobních údajů. Lze se tedy domnívat, že obecné nařízení ochrany osobních údajů chrání soukromí fyzických osob v míře, ve které toto soukromí souvisí s ochranou osobních údajů. Pro ochranu soukromí mimo souvislost se zpracováním osobních údajů existují jiné nástroje, včetně široké judikatury ESLP a SDEU, a neměla by být tedy předmětem této regulace.

GDPR navazuje na původní cíle směrnice 95/46/ES, která sloužila především k harmonizaci úpravy pro účely fungování vnitřního trhu a zajištění volného pohybu údajů mezi členskými státy. Vzhledem k tomu, že se jednalo o směrnici, kterou každý členský stát transponoval a implementoval do svého právního řádu, vznikly napříč jednotlivými státy odchylky v právních úpravách, přičemž navíc každý dozorový úřad rozvinul vlastní výkladovou praxi.

Evropský zákonodárce si je této nejednotnosti úpravy vědom, což stvrzuje v bodě 9 úvodních ustanovení, kde zdůrazňuje, že ačkoliv cíle a zásady směrnice 95/46/ES nadále platí, nezabránilo to roztříštěnosti v provádění ochrany údajů v celé Unii, právní nejistotě ani rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud jde o činnosti prováděné online. Rozdíly mnohdy dosahují až takové míry, že zatímco zpracování v jednom členském státě je zcela v souladu s národními předpisy, v sousedním státě je běžně pokutováno. Tyto rozdíly mohou bránit volnému

pohybu osobních údajů v rámci EU a mohou být překážkou pro výkon hospodářských činností.

V souladu s čl. 16 odst. 2 a čl. 288 SFEU evropský zákonodárce zvolil pro novou úpravu ochrany osobních údajů formu nařízení. Nařízení jako forma legislativního dokumentu má oproti směrnici nesporné výhody, kterými je zejména přímá aplikovatelnost. Členské státy tak nemusejí – a dokonce ani nemohou (srov. rozsudek SDEU ve věci *Variola*[310]) – nařízení nijak implementovat do svých právních řádů. Nařízení tak působí obdobně jako národní právo, aniž by členské státy musely pro jeho aplikovatelnost podnikat další kroky. Pro vymáhání nařízení je však často nezbytné přijmout alespoň prováděcí či jiné doprovodné předpisy, které aplikaci nařízení uzpůsobí tuzemským podmínkám, viz např. přijetí zákona o zpracování osobních údajů v České republice.

Právní předpisy ve formě nařízení mají rovněž vůči národním předpisům aplikační přednost (srov. rozsudky SDEU ve věci *Van Gend en Loos*[311] či *Costa v. ENEL*[312]). To v důsledku znamená, že pokud je jakékoliv ustanovení vnitrostátního práva v rozporu s požadavky GDPR, použije se vždy dané ustanovení GDPR bez ohledu na odlišnou úpravu vnitrostátního práva. Státy se tak nemohou od úpravy GDPR odchýlit a ve všech oblastech, ve kterých se GDPR aplikuje[313], jsou plně vázány pravidly zakotvenými v GDPR. Členské státy zároveň nemohou přijmout úpravu, která by stanovila přísnější podmínky ochrany, a tím znesnadňovala volný pohyb osobních údajů.

Výjimkou jsou ustanovení GDPR, která výslovně odchylnou úpravu povolují nebo připouštějí. Nejširší zmocnění v tomto poskytují ustanovení čl. 23 a dále čl. 85–91 GDPR. Různá zmocnění se však prolínají napříč celým nařízením, čímž evropský zákonodárce dává prostor jednotlivým členským státům reflektovat své

[310] Rozsudek Soudního dvora Evropské unie ze dne 10. října 1973 ve věci C-34/73, Fratelli Variola S.p.A. proti Amministrazione italiana delle Finanze.

[311] Rozsudek Soudního dvora Evropské unie ze dne 5. února 1963 ve věci C-26/62, Van Gend en Loos proti Nederlandse Administratis der Belastigen.

[312] Rozsudek Soudního dvora Evropské unie ze dne 15. července 1964 ve věci C-6/64, Costa proti ENEL.

[313] Srov. kapitola 3.2.2 níže.

kulturní a společenské odlišnosti. Jedním z takových příkladů je zmocnění stanovené v čl. 8 odst. 1 GDPR, které umožňuje nastavení různé věkové hranice pro zpracování osobních údajů dětí v souvislosti se službami informační společnosti. Forma nařízení tedy nezajistí jednotnou aplikaci pravidel GDPR napříč celou EU. Národní dozorové orgány i soudy při aplikaci i nadále vycházejí ze svých dosavadních zkušeností a kulturních aspektů své země, čímž i nadále (ač v menší míře) dochází k částečnému rozkolu aplikace pravidel ochrany osobních údajů.

3.2.2 Věcná působnost obecného nařízení o ochraně osobních údajů[314]

3.2.2.1 Automatizované zpracování osobních údajů

GDPR se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Působnost nařízení tak vychází z technologicky neutrální definice, která je nezávislá na použitých technologiích.

---

[314] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 39 - 49.

Další použité literární zdroje v této kapitole:

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016, xi, 338. ISBN 978-80-7400-610-4.

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0.

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

Výjimky z této působnosti jsou pak stanoveny v čl. 1 odst. 2 GDPR (k tomu viz kapitola 3.2.2.3 níže).

Věcná působnost nařízení se tak neliší od působnosti pravidel ochrany osobních údajů dle ustanovení čl. 3 odst. 1 směrnice 95/46/ES, podle kterého platilo, že *„směrnice se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů, jakož i na neautomatizované zpracování osobních údajů, které jsou obsaženy v rejstříku nebo do něj mají být zařazeny.“* Rovněž dosavadní zákon č. 101/2000, který směrnici 95/46/ES transponoval do českého právního řádu, se uplatnil na zpracování osobních údajů, *„ať k němu dochází automatizovaně nebo jinými prostředky“*, avšak podle § 3 odst. 4 se nevztahoval na nahodilé shromažďování osobních údajů, pokud tyto údaje nebyly dále zpracovávány.

V případě, kdy začne docházet k automatizovanému zpracování, budou takové činnosti podléhat podmínkám obecného nařízení o ochraně osobních údajů. Nařízení nikde nedefinuje, co je považováno za automatizované zpracování (a žádnou definici neposkytovala ani směrnice 95/46/ES). Dnes však již není pochyb, že zpracování údajů prostřednictvím počítačových programů je zpracováním automatizovaným. Není určující, o jaké konečné zařízení se bude jednat, tudíž se nemusí jednat jen o zpracování prostřednictvím počítačů, ale rovněž o zpracování osobních údajů prostřednictvím smartphonů, kamerových systémů či různých dronů vybavených kamerovým systémem či webkamerou. Naopak za částečně automatizované zpracování může být považován např. proces, při kterém je část postupu nakládání s daty zajišťována manuálně – např. při zadávání dat do počítačového systému.

Absence bližšího vymezení automatizovaného zpracování může vést ke vzniku kazuistické úpravy založené na soudním posouzení konkrétních případů. Např. v případu Lindqvist[315] tak Soudní dvůr Evropské unie konstatoval, že úkon, který spočívá v poskytnutí odkazu na internetové stránky na různé osoby, které jsou identifikovány buď svým jménem, nebo jinými prostředky (např. telefonním

[315] Rozsudek Soudního dvora Evropské unie ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist.

číslem, údaji o pracovních poměrech či údajem o zálibách), je nezbytné považovat za zcela nebo částečně automatizované zpracování osobních údajů.

Dále uvádím několik příkladů zpracování, u kterých by nemělo být pochyb, že je lze považovat za automatizované zpracování, a podléhají tak tomuto nařízení (pokud není splněna některá z podmínek odst. 2 nebo 3):

- sběr dat prostřednictvím nositelné elektroniky (*smart wearables*) či jiných chytrých zařízení, včetně chytrých automobilů a jiných zařízení (často spojovaných s tzv. internetem věcí);
- krátkodobé uchovávání osobních údajů v informačním systému, např. v mezipaměti (*cache*) webového prohlížeče;
- zobrazení dat na obrazovce počítače.

U automatizovaných zpracování, která probíhají online, se navíc mohou uplatnit i další předpisy – do budoucna především předvídané tzv. *ePrivacy Regulation*, které nahradí stávající *ePrivacy* směrnici– v českém prostředí implementovanou zejména do zákona o elektronických komunikacích a zákona o některých službách informační společnosti.

3.2.2.2 Neautomatizované zpracování osobních údajů

Na rozdíl od automatizovaného zpracování, které pod režim GDPR spadá automaticky, je pro aplikaci nařízení v rámci neautomatizovaného zpracování nutné splnit další podmínky. Pokud nejsou obě podmínky splněny kumulativně, takové nakládání s osobními údaji není předmětem regulace GDPR:

a. osobní údaje jsou zařazené v evidenci a/nebo do ní mají být zařazeny; a zároveň
b. osobní údaje jsou uspořádané podle určitého systematického hlediska (např. abecedně seřazené).

Aplikace pravidel GDPR na neautomatizované zpracování je tak podmíněna zařazením do evidence (angl. *filing system*, fran. *fichier* či něm. der *Dateisystem*). Tato podmínka není novým požadavkem. Stejná podmínka platila pro uplatnění pravidel dle směrnice 95/46/ES, která se vztahovala i na neautomatizované

zpracování osobních údajů, které jsou obsaženy v rejstříku (angl. *filing system*, fran. *fichier* či něm. *die Datei*) nebo do něj mají být zařazeny (srov. čl. 3 odst. 1 směrnice 95/46/ES). Dosavadní zákon č. 101/2000 toto vymezení nepřevzal doslova a svou působnost vztahoval na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky, nikoliv však nahodilé shromažďování údajů, které nejsou dále zpracovávané (srov. § 3 odst. 2 a 4 ZOOÚ). Přestože český zákon s pojmem evidence ani rejstřík nepracoval, vzhledem ke shodnému (viz anglická či francouzská verze) nebo velmi podobnému (viz česká či německá verze) významu v jiných jazykových verzích se použije dosavadní výkladová praxe k pojmu rejstřík ve smyslu směrnice 95/46/ES.

Za neautomatizovanou evidenci se tak podle stávající výkladové praxe považuje např. i soubor osobních údajů shromážděných neautomatizovaným způsobem členy náboženského společenství spočívající v zapisování poznámek o tom, koho navštívili, co jim dotyčný o sobě a své rodině řekl a jak případně reagoval na pastorační činnost, bez ohledu na to, zda jsou tyto údaje shromážděny v rejstřících nebo v kartotékách, a to i v případě, kdy se tak děje bez jakéhokoliv jednotného systému, k těmto údajům nemá přístup každý z členů společenství a shromážděné údaje neumožňují provádět vyhledávání.[316]

Typickým neautomatizovaným zpracováním je tak např. vedení kartotéky nebo evidence prostřednictvím registratury.[317] Naopak, pokud organizace nenakládá se záznamy nebo soubory záznamů ani jejich titulními stranami, které nejsou uspořádány podle určených hledisek, nemělo by takové nakládání v souladu s bodem 15 úvodních ustanovení GDPR spadat do působnosti obecného nařízení o ochraně osobních údajů.

[316] Srov. stanovisko generálního advokáta Paola Mengozziho ze dne 1. února 2018 ve věci C-25/17, Tietosuojavaltuutettu.

[317] Srov. např. rozhodnutí SDEU ze dne 10. července 2018 ve věci C-25/17 Tietosuojavaltuutettu.

Jak je patrné z vymezení věcné působnosti nařízení dle tohoto ustanovení a dále z definice osobních údajů[318] a zpracování[319], aplikační dopad pravidel obecného nařízení o ochraně osobních údajů je velmi široký. U většiny korporací tak nařízení dopadá téměř do všech činností jejich působnosti a lze vycházet z jednoduchého pravidla – GDPR se uplatní vždy, pokud neexistuje výslovná výjimka, která by konkrétní činnost vyňala z obecného režimu tohoto nařízení.

3.2.2.3 Negativní vymezení působnosti obecného nařízení o ochraně osobních údajů

Odstavec 2 stanoví obecné výjimky, na které se nařízení bez dalšího nevztahuje, a to ani kdyby se jednalo o zpracování osobních údajů splňující podmínky odst. 1. Jedná se o různorodé důvody, mezi kterými není vzájemná souvislost.

3.2.2.3.1 Zpracování osobních údajů při výkonu činností, které nespadají do oblasti působnosti práva Unie

Podle čl. 2 odst. 2 písm. a) GDPR se obecné nařízení o ochraně osobních údajů nevztahuje na činnosti, které nespadají do působnosti práva EU. Jedná se o logickou výjimku, která by z podstaty působnosti evropského práva platila, i pokud by nebyla v GDPR výslovně zakotvena. Její explicitní zakotvení tak slouží spíše jako připomínka toho, že působnost práva EU, jež vycházejí ze zakládajících smluv SEU a SFEU, působí pouze v explicitně vymezených oblastech. Zbylé oblasti, kterými jsou především veřejný pořádek, obrana a národní bezpečnost, do práva EU nespadají, a v těchto oblastech se tak nelze domáhat ani ochrany osobních údajů zajišťovanou nařízením. Tím však není

[318] Podle čl. 4 bodu 1 GDPR se osobními údaji rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

[319] Podle čl. 4 bodu 2 GDPR se zpracováním rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

dotčena soukromoprávní ochrana soukromí, která je chráněna zejména podle občanského zákoníku, jak je blíže popsáno v kapitole 2 této práce.

U některých oblastí mohou vznikat pochybnosti, zda spadají do působnosti práva EU, nebo ne. Jedná se tak např. o ochranu osobních údajů při správě některých daní, které právo EU neupravuje (ač např. oblast daně z přidané hodnoty je harmonizována). Zákon o zpracování osobních údajů [§ 4 odst. 2 písm. a)] stanoví, že ustanovení GDPR se použijí i při zpracování osobních údajů, k němuž dochází při výkonu činností, které nespadají do oblasti působnosti práva EU. Z této aplikace naopak ZZOÚ vyjímá oblasti, které spadají do působnosti směrnice 2016/680, jak shodně stanovuje čl. 2 odst. 2 písm. d) GDPR (viz. Hlava III ZZOÚ).

Vzhledem k tomuto plošnému rozšíření aplikace pravidel stanovených v zákoně o zpracování osobních údajů se pravidla ochrany osobních údajů zakotvená v obecném nařízení o ochraně osobních údajů uplatní plošně na jakékoliv zpracovatelské činnosti v rámci České republiky (s výjimkou oblastí pokrytých Hlavou III a IV ZZOÚ, které jsou tedy samostatnou úpravou pro oblast působnosti směrnice 2016/680).

3.2.2.3.2 Zpracování osobních údajů členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU

Podle čl. 2 odst. 2 písm. b) GDPR se pravidla obecného nařízení o ochraně osobních údajů nepoužijí při výkonu činností, které se týkají společné zahraniční a bezpečnostní politiky. K uplatnění této výjimky může dojít i v případě, že některé údaje byly původně získané za jiným (např. komerčním) účelem a nastane potřeba tyto údaje použít pro účely zahraniční a bezpečnostní politiky.

3.2.2.3.3 Zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních či domácích činností

Zcela identická podmínka byla zakotvena již v čl. 3 odst. 2 směrnice 95/46/ES, kterou pak český zákon o ochraně přeformuloval jako *„zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.“* Tato výjimka by se tak měla vykládat zcela v souladu s dosavadní praxí (do které je však rovněž

nezbytné reflektovat aktuální technologický vývoj a např. způsob využívání sociálních sítí).

Výjimka pro domácí použití se tak uplatní pouze na činnosti, které provádí fyzická osoba výlučně pro svou domácí či osobní potřebu. Nemělo by tak být sporu, že vytváření alba rodinných fotografií nebo vedení vlastní databáze kontaktů (včetně kontaktů ukládaných v mobilním telefonu) pod tuto podmínku spadne. Vždy by se však mělo jednat o zpracování pouze pro osobní/domácí potřebu – tedy vytváření činnosti spojené s volnočasovými aktivitami, dovolenou, vlastní zábavou apod. Jakmile však dojde k využívání – byť např. stejné databáze kontaktů – i ke komerčním účelům, tato výjimka se neuplatní. Tento výklad je obecně přijímán a dovozován zejména z velmi restriktivního „výlučně". Pravidla obecného nařízení o ochraně osobních údajů tak dopadnou i na případy, kdy osobní údaje, které byly původně zpracované pro osobní potřebu, budou následně použity ke komerčním účelům. Například v případě použití osobních údajů ze soukromého adresáře pro nově zahájenou podnikatelskou činnost.

Výjimku z působnosti GDPR zásadně nepředstavuje ani privátní zpracování osobních údajů v prostředí internetu, zejména v případě jejich zveřejnění. Ne každé zveřejnění by však mělo být považováno za zpracování osobních údajů a spadnout automaticky do působnosti GDPR. V dnešní době tak pod výjimku domácího použití může spadnout např. využívání sociálních sítí v uzavřeném okruhu přátel. V případě, kdy běžný uživatel Facebooku uveřejní na svém profilu (na svém *Timeline*) fotografie, které bude sdílet s okruhem svých přátel, neměla by taková činnost spadat pod regulaci GDPR. Na druhou stranu je pravděpodobné, že se tato výjimka neuplatní, pokud informace budou sdíleny s předem neurčeným okruhem osob – tj. např. na zcela veřejném facebookovém profilu či na Twitteru, který je ze své podstaty zcela veřejný. Obdobné podmínky vymezil rovněž SDEU ve věci *Lindqvist*[320], kde pod tuto výjimku domácího užití odmítl podřadit umístění údajů na veřejně přístupnou internetovou stránku.

[320] Rozhodnutí Soudního dvora Evropské unie ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist.

Korektivem aplikace GDPR je v tomto směru rovněž princip *ultima ratio* správního trestání. Využití prostředků správního práva a správního trestání by se tak mělo použít pouze tehdy, kdy užití jiných (soukromoprávních) prostředků obrany nepřichází v úvahu nebo by bylo zjevně neúčelné. Případy, kdy okruh přátel mezi sebou (byť prostřednictvím globální sociální sítě) sdílí určité osobní údaje, by tak neměly bez dalšího spadat pod režim ochrany osobních údajů dle nařízení; tím však není dotčena aplikovatelnost těchto pravidel na samotné platformy (sociální sítě).

Dalším příkladem zpracování osobních údajů pro osobní potřebu, které však může být rovněž na pomezí aplikovatelnosti GDPR, je provozování bezpečnostních kamer pro účely ochrany vlastního majetku. Samotnou instalaci a provozování bezpečnostní kamery na vlastním pozemku lze považovat za zpracování primárně pro osobní potřebu a podléhající tak pouze obecným pravidlům občanského práva (v souladu s rozsudkem Nejvyššího soudu je kamera zabírající pozemek souseda považována za imisi ve smyslu § 1013 o.z.)[321]. Je však nutno vzít v potaz, zda provoz této bezpečnostní kamery nemůže neoprávněně a nepřiměřeně zasahovat do soukromí jiných osob – tedy neměla by nikdy zasahovat na veřejné prostranství nebo na pozemek sousedů. Pokud by tomu tak bylo, toto zpracování by porušovalo podmínku legality, a tudíž by se nemohlo jednat o zpracování pro osobní potřebu a tato výjimka by se pak neuplatnila.

Osobní potřeba se nemusí vztahovat pouze k osobě, která zpracování provádí. Tato osoba může zpracováním sledovat taky zájmy svých rodinných příslušníků, členů domácnosti nebo blízkých osob a stále se bude jednat o zpracování pro osobní potřebu, na které se GDPR proto nebude vztahovat.

[321] Rozsudek Nejvyššího soudu ze dne 30. října 2012, sp. zn. 22 Cdo 583/2011.

3.2.2.3.4 Zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení

Pravidla GDPR se nepoužijí v případech, kdy zpracování provádí orgány činné v trestním řízení za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestu a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Pro tyto případy se uplatní podmínky stanovené v Hlavě III ZZOÚ.

Příslušnými orgány, na které se úprava vztahuje, jsou tak především orgány činné v trestním řízení. Dopad bude mít i na další orgány nebo subjekty pověřené právem členského státu plnit veřejnou funkci a vykonávat veřejnou moc. Podle ZZOÚ by příslušným orgánem měla být zejména Policie ČR, Generální inspekce bezpečnostních sborů, Vojenská policie či Probační a mediační služba. Z působnosti tohoto zákona by naopak měly být vyloučeny zpravodajské služby a obecní policie.

Pokud se účel zpracování neslučuje s účely směrnice 2016/680, uplatní se GDPR, ledaže by zpracování bylo možné zahrnout pod výjimku zakotvenou v čl. 2. odst. 2 písm. a) GDPR. Na příslušný orgán se tedy v některých případech mohou vztahovat pravidla GDPR i směrnice 2016/680 (resp. národního předpisu implementujícího tento předpis), a to v závislosti na účelu zpracování. Pokud příslušný orgán sdělí údaje osobě, na kterou se směrnice 2016/680 neaplikuje, nebo jinému příslušnému orgánu, ale za jiným účelem, uplatní se v těchto případech subsidiárně GDPR. Jednotlivé spravující orgány by vždy měly mít přehled, zda zpracovávají údaje pouze podle nařízení nebo zda může podléhat i režimu směrnice 2016/680; obdobně se pak uplatní úprava na zapojení zpracovatelů, kde je nezbytné rozlišit, o jaký režim se bude jednat (GDPR či směrnice 2016/680).

3.2.2.3.5 Zpracování osobních údajů orgány, institucemi a jinými subjekty Evropské unie

GDPR se nevztahuje na zpracování osobních údajů, které provádějí orgány, instituce či jiné subjekty EU. Takové zpracovatelské činnosti podléhají zvláštnímu nařízení Evropského parlamentu a Rady (EU) č. 2018/1725. Kontrolu nad dodržováním tohoto zvláštního nařízení provádí Evropský inspektor ochrany údajů (European Data Protection Supervisor), který rovněž zveřejňuje některé soft-law materiály sloužící k výkladu tohoto nařízení[322], které slouží k další interpretaci těchto předpisů, jak je rovněž popsáno v kapitole 1.3.1.3 výše.

3.2.2.3.6 Výjimky z odpovědnosti pro poskytovatele služeb informační společnosti

Podle čl. 2 odst. 4 GDPR platí, že pravidla obecného nařízení o ochraně osobních údajů nijak neovlivňují uplatňování a aplikaci směrnice 2000/31/ES (tzv. *eCommerce směrnice*)[323], která upravuje pravidla poskytování služeb informační společnosti. Ustanovení odst. 4 zdůrazňuje, že pravidla ochrany osobních údajů dle GDPR by neměla zejména ovlivnit aplikaci pravidel omezené odpovědnosti poskytovatelů zprostředkovatelských služeb dle čl. 12–15 *eCommerce směrnice*, která byla v ČR implementována v podobě § 3–5 zákona o některých službách informační společnosti (tj. pravidla upravující zvláštní režim odpovědnosti u poskytovatelů služeb informační společnosti v podobě *mere conduit*, *caching a hosting*).

I nadále by tak mělo platit, že poskytovatelé těchto služeb, za předpokladu, že naplňují podmínky pro uplatnění této omezené odpovědnosti, nebudou nést odpovědnost za obsah, nad kterým nemají kontrolu. V takovém případě provozovatelé sociálních sítí (např. YouTube, Twitter či Facebook) neponesou odpovědnost za obsah, který sdílí její uživatel a který případně porušuje pravidla

[322] Tyto materiály jsou zveřejňované na internetových stránkách Evropského inspektora ochrany osobních údajů - https://edps.europa.eu.

[323] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), dostupná z https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32000L0031.

ochrany osobních údajů. Z tohoto hlediska tak poskytovatelé těchto sítí vystupují pouze jako poskytovatelé platformy, která není odpovědná (dle a v rozsahu pravidel v *eCommerce* směrnici). Na druhou stranu ale tito poskytovatelé vždy budou odpovědní za ochranu osobní údajů svých uživatelů, ve vztahu ke kterým jsou obvykle v postavení správců.

3.2.3 Působnost zákona o zpracování osobních údajů[324]

Limity věcné působnosti obecného nařízení o ochraně osobních údajů do působnosti práva členských předpisů identifikované v kapitole 3.2.2 jsou pro český právní řád částečně zhojené prostřednictvím § 2 ZZOÚ, které upravuje působnost zákona o zpracování osobních údajů jako celku. Dílčí oblasti působnosti uvedené v písmenech a) až e) tohoto ustanovení tak obsahově odpovídají hlavám II až V zákona o zpracování osobních údajů.

Zákon o zpracování osobních údajů rozšiřuje věcnou působnost GDPR na všechna zpracování osobních údajů s výjimkou těch, která spadají pod působnost hlavy III a IV ZZOÚ, tedy zajištění bezpečnostních zájmů České republiky a zpracování osobních údajů orgány činnými v trestním řízení upravené směrnicí 2016/680 a implementovanou v hlavě II ZZOÚ (srov. § 2 písm. b) a c) ZZOÚ).

Ustanovení § 2 písm. a) a d) potvrzují působnost nařízení [písm. a)] a dále jeho působnost rozšiřují na veškeré ostatní činnosti, které jsou jinak z působnosti nařízení (a obecně evropského práva – k tomu viz komentář k čl. 2 nařízení) vyňaty. Český zákonodárce pro zachování jednotnosti úpravy napříč veřejnoprávní (s výše uvedenou výjimkou) i soukromoprávní sférou pouze v § 2 písm. d) a § 4 ZZOÚ rozšířil věcnou působnost nařízení i na tyto zbývající oblasti. Pokud ZZOÚ výslovně nestanoví jinak (hlava III a IV), pravidla stanovená v GDPR doplněná o pravidla hlavy II ZOOÚ se uplatní plošně na veškeré zpracovatelské činnosti na území ČR či prováděné osobami podléhajícími českému právnímu řádu. Český zákonodárce tak zvolil v zásadě minimalistickou

[324] Části textu v této kapitole byly publikován jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 505 - 506.

zákonnou úpravu na rozdíl např. od Slovenska, kde slovenský zákonodárce pro oblast neupravenou nařízením [tj. zejména výkon činností, které nespadají do oblasti působnosti práva Unie dle čl. 2 písm. a) nařízení] přijal samostatnou úpravu (provedenou zákonem č. 18/2018 Z. z., o ochrane osobných údajov). Tímto způsobem jsou tedy rozšířená i pravidla pro výmaz osobních údajů ve smyslu čl. 17 GDPR na všechny oblasti zpracování, které jinak nejsou formou obecného nařízení o ochraně osobních údajů o ochraně osobních údajů pokryty (srov. zejména kapitolu 3.2.2.3.1 a 3.2.2.3.2).

Ani podle českého zákona o zpracování osobních údajů se však pravidla zpracování osobních údajů nevztahují na fyzickou osobu v průběhu výlučně osobních nebo domácích činností.[325]

Limitovaná pravidla se uplatní pro oblast zajišťování obranných a bezpečnostních zájmů České republiky[326], pro kterou český zákonodárce využil možnosti derogace od obecných pravidel obecného nařízení o ochraně osobních údajů dle čl. 23 GDPR. V souladu s článkem 23 GDPR je rovněž omezené uplatnění práva na výmaz ve smyslu čl. 17 GDPR. Možnosti zpracování osobních údajů jsou specifiky vymezeny v § 43 odst. 3 ZZOÚ. Vzhledem ke specifičnosti této úpravy však nejsou nadále v této práci analyzovány. Zpravidla však platí, že jednotlivec by se tak v této oblasti musel dovolávat ochrany svých osobnostních práv, nikoliv postupovat prostřednictvím ochrany osobních údajů.

[325] Srov. ustanovení § 2 písm. d) ZZOÚ.

[326] Srov. zejména ustanovení § 2 písm. c) a § 43 ZZOÚ.

3.2.4 Místní působnost obecného nařízení o ochraně osobních údajů[327]

3.2.4.1 Vymezení místní působnosti obecného nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů má velmi vysoké ambice, co se týká své teritoriální působnosti. Obecně se obecné nařízení o ochraně osobních údajů vztahuje na veškeré zpracovatelské operace probíhající na území EU nebo v souvislosti s provozovnou správce/zpracovatele v EU.

Ambicí evropského zákonodárce však nebylo postihnout jen zpracování probíhající v rámci Evropské unie, ale rovněž veškerá zpracování týkající se osob nacházejících se v EU, ačkoliv správce či zpracovatel pocházejí ze třetí země a zároveň své služby míří na subjekty údajů nacházející se v Evropské unii či monitorují chování těchto subjektů údajů na území EU. Vzhledem k široké extrateritoriální působnosti se tak GDPR stává pravděpodobně nejvýznamnějším předpisem upravujícím ochranu (a zabezpečení) osobních údajů (či dat obecně) na světě. V zásadě jedinou možností pro organizace, jak se vyhnout působnosti

[327] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 46 - 53.

Další použité literární zdroje v této kapitole:

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016, xi, 338. ISBN 978-80-7400-610-4.

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0.

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

obecného nařízení o ochraně osobních údajů, je nijak necílit na evropský trh. Jakmile začne organizace působit a nabízet své služby na území Evropské unie, je prakticky nemožné vyloučit aplikaci obecného nařízení o ochraně osobních údajů. Nařízení též předvídá možnost, že správce/zpracovatel fakticky působí v EU, avšak nemá zde provozovnu. Jednou z hlavních povinností takového správce/zpracovatele je pak jmenovat zástupce v EU podle čl. 27 GDPR.

Exteritoriální působnost GDPR by rovněž měla vyloučit tzv. *treaty shopping*, tedy zabránit situacím, kdy si zahraniční subjekty vybírají sídlo podle jurisdikce, která jim ukládá nejmírnější povinnosti – zde v oblasti ochrany osobních údajů. I pokud se tedy organizace usídlí z důvodu mírnější regulace ochrany osobních údajů mimo EU (zcela stranou ponechme tzv. daňové ráje a jiné důvody usídlení v jiných jurisdikcích) s cílem působit na evropském trhu, bude i tak zpracování podléhat pravidlům GDPR. Zcela samostatnou otázkou však i nadále zůstává faktická vymahatelnost těchto pravidel.

Působnost nařízení může být rovněž rozšířena na oblasti, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného.

Pro tyto účely je nezbytné poznamenat, že GDPR je text s relevancí i pro Evropský hospodářský prostor (EHP). V případě, kdy obecné nařízení o ochraně osobních údajů hovoří o zpracování týkající se území EU, automaticky se předpokládá působnost i na území států, které jsou součástí EHP – Norsko, Island a Lichtenštejnsko. Zpracování týkající se těchto států či datové přenosy do těchto států se tak vždy považují za zpracování v rámci Evropské unie. Pro zjednodušení se v této práci používá jen „území EU“, které však zahrnuje rovněž Norsko, Island a Lichtenštejnsko.

3.2.4.2 Působnost GDPR na činnosti provozovny správce či zpracovatele v rámci Evropské unie

Každý správce či zpracovatel, jehož provozovna se nachází na území EU, spadá bez dalšího pod režim GDPR. Taková aplikace je z podstaty věci zcela logická – správce/zpracovatel se nachází v jurisdikci (členského státu) EU a musí se tak řídit jejími právními předpisy, včetně předpisů na ochranu osobních údajů.

GDPR pojem provozovna (angl. *establishment*) dále specifikuje v bodu 22 úvodních ustanovení, podle kterého pojem provozovna předpokládá účinný a skutečný výkon činnosti prostřednictvím stálého zařízení. Právní forma této provozovny, ať již jde o pobočku, nebo (dceřinou) společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. Ve smyslu rozsudku SDEU ve věci *Weltimmo*[328] by tak skutečnost, zda se jedná o provozovnu, měla být posuzována na základě druhu ekonomických aktivit a nabízených služeb. Ve smyslu tohoto rozhodnutí tak platí, že i jeden zástupce na území jediného členského státu může představovat provozovnu, pokud jsou v konkrétním případě tímto zástupcem poskytovány služby relativně stabilně (stálé zařízení). Výklad pojmu provozovna hrál rovněž významnou roli v rámci rozsudku SDEU ve věci *Google Spain.*

Nařízení se pak uplatní na každé zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozovny (angl. *in the context of the activities of an establishment*). Stejná podmínka existovala již podle úpravy směrnice 95/46/ES. Ačkoliv se může na první pohled zdát, že čl. 3 GDPR ustanovení rovněž rozšiřuje působnost obecného nařízení o ochraně osobních údajů, jedná se zjevně jen o nepřesný překlad. Podle českého znění ustanovení čl. 4 odst. 1 písm. a) směrnice 95/46/ES se směrnice vztahuje na zpracování, které je „prováděno v rámci činností provozovny“, což evokuje užší dopad než „v souvislosti“ dle GDPR. V ostatních jazykových verzích však i původní znění čl. 4 odst. 1 písm. a) směrnice 95/46/ES stanovilo, že se má jednat o zpracování „v souvislosti s činnostmi“ (srov. angl. *in the context of the activities of an establishment*) a rozsah dopadů těchto předpisů podle této podmínky tak zůstává zachován.

Podmínkami pro posouzení toho, zda konkrétní zpracování probíhá v souvislosti s činnostmi provozovny, se rovněž zabýval SDEU, a to ve věci *Google Spain*. Aby se jednalo o zpracování související s činností provozovny, podle tohoto rozhodnutí postačí, pokud provozovna usazená v EU ekonomicky podporuje jinou provozovnu, v rámci které zpracování osobních údajů probíhá. Není proto nutné, aby zpracování probíhalo přímo v provozovně umístěné na území EU. Podporou

[328] Rozsudek Soudního dvora Evropské unie ze dne 1. října 2015 ve věci C-230/14 Weltimmo.

se pak rozumí např.: prodej reklamy, marketingové činnosti aj. Mezi ekonomickou činností podporující provozovny sídlící na území EU a samotnou zpracovatelskou činností (prováděnou provozovnou mimo EU) však musí existovat prokazatelné neoddělitelné spojení. Dle WP29 nelze toto „neoddělitelné spojení“ (angl. *inextricable link*) vykládat příliš široce.[329] Pouze skutečnost, že se jedná o dva subjekty patřící do stejné skupiny, sama o sobě nestačí k doložení takového spojení, a je tedy potřeba hledat další souvislosti.

Příklad:

Organizace sídlící mimo EU má v některém z členských států EU pobočku, která sama o sobě sice nevykonává žádné operace zpracování, nicméně navazuje vztahy se zákazníky a získává tak pro tento subjekt značné množství klientů (prostřednictvím vytváření reklamy), čímž se významně podílí na jeho hospodářském úspěchu. V tomto případě evropská pobočka subjektu rozvíjí vztahy se zákazníky a vyznačuje se tak vysokou mírou stálosti, proto ji lze považovat za provozovnu subjektu podle GDPR. Tato provozovna nevykonává žádnou zpracovatelskou činnost, avšak přesto podstatným způsobem přispívá k hospodářskému úspěchu subjektu. S ohledem na výklad SDEU v případu Google Spain se proto v tomto případě bude GDPR vztahovat na samotný subjekt, i když ten má sídlo mimo EU.

Hlavní případy, kdy se uplatní pravidla obecného nařízení o ochraně osobních údajů spojené s činnostmi provozovny správce či zpracovatele na území Evropské unie ve smyslu čl. 3 odst. 1 GDPR, lze tak shrnout do následujících bodů:

a. EU provozovna sbírá a zpracovává osobní údaje sama;

b. EU provozovna sbírá osobní údaje v jednom členském státě a zpracovává je provozovna v jiném státě;

c. EU provozovna zpracovává osobní údaje prostřednictvím entity (zpracovatele) usazené mimo území EU;

[329] Stanovisko WP29 „Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain“ ze dne 16. prosince 2015, 176/16/EN. [online]. [cit. 2022-03-14]. Dostupné z https://ec.europa.eu/newsroom/article29/redirection/document/56127.

d. EU provozovna zpracovává osobní údaje pro entitu (správce) usazenou mimo území EU;

e. EU provozovna nezpracovává žádné osobní údaje (tedy ani v postavení zpracovatele), avšak svou činností ekonomicky významně podporuje mimoevropskou entitu (svou mateřskou společnost, se kterou má úzký vztah), která pak provádí zpracovatelské operace.

3.2.5 Extrateritoriální působnost obecného nařízení o ochraně osobních údajů[330]

3.2.5.1 Působnost nařízení na činnosti související s provozovnou mimo území Evropské unie

Obecné nařízení o ochraně osobních údajů se dále vztahuje i na zpracovatelské aktivity, které provádí správce/zpracovatel, jehož provozovna je mimo území jakéhokoliv členského státu, avšak k tomu zpracování splňuje jednu z následujících podmínek:

---

[330] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 47 - 53.

Další použité literární zdroje v této kapitole:

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016, xi, 338. ISBN 978-80-7400-610-4.

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0.

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

a. zpracování souvisí s nabídkou zboží nebo služeb těmto subjektům údajů v EU (bez ohledu na to, zda je požadována platba); a/nebo

b. zpracování zahrnuje monitorování chování subjektů údajů, ke kterému dochází na území EU.

Dle tohoto ustanovení se tak pravidla ochrany osobních údajů dle obecného nařízení o ochraně osobních údajů aplikují na základě skutkových činností na správce/zpracovatele, který jinak nepodléhá jurisdikci žádného členského státu, a to na základě principu *lex loci solutionis*, tedy podle toho, kde je příslušné smluvní plnění nabízené. Nařízení v tomto ohledu velmi posiluje ochranu evropských spotřebitelů (resp. subjektů údajů) při využívání zahraničních služeb. Jakmile zahraniční služba začne cílit své služby na evropské subjekty, musí dodržovat pravidla ochrany osobních údajů vyžadovaná obecným nařízením o ochraně osobních údajů.

V případě, že správce/zpracovatel nemá provozovnu v rámci žádného členského státu EU, vzniká mu dále povinnost jmenovat svého zástupce ve smyslu čl. 27 GDPR. Tento zástupce následně slouží jako kontaktní bod pro evropské subjekty údajů a evropské dozorové úřady.

3.2.5.2 Zpracování osobních údajů související s nabídkou zboží nebo služeb těmto subjektům údajů v Unii bez ohledu na to, zda je od subjektů údajů požadována platba

První případ extrateritoriální působnosti GDPR podle čl. 3 odst. 2 písm. a) GDPR[331] cílí především na internetové služby (resp. služby informační společnosti), které, ač jsou provozovány ze zahraničí, míří i na evropský trh. Podmínkou uplatnitelnosti ustanovení čl. 3 odst. 2 písm. a) GDPR je tak úmysl správce/zpracovatele cílit své služby na evropský trh, resp. na evropské spotřebitele.

[331] Podle tohoto ustanovení čl. 3 odst. 2 písm. a) GDPR platí, že *„[obecné nařízení o ochraně osobních údajů] se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba.“*

Podle bodu 23 úvodního ustanovení GDPR pak navíc platí, že k určení, zda může být činnost zpracování považována za monitorování chování subjektu údajů, by mělo by být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, které se jí týká, nebo za účelem analýzy či odhadu jejích osobních preferencí, postojů a chování.

Přesná kritéria pro vymezení úmyslného cílení nabídky zboží nebo služeb na evropského spotřebitele nejsou nikde vymezena. Podle rozsudku Soudního dvora ve věci *Pammer*[332] a podle bodu 23 úvodního ustanovení GDPR se může jednat o různé náznaky, které dohromady zjevně prokazují, že má správce nebo zpracovatel v úmyslu nabízet služby subjektům údajů v jednom nebo více členských státech v EU.

Může se jednat například o následující faktory:

- nabídka zboží či služeb probíhá v jazyku jednoho či více EU států;
- správce/zpracovatel přijímá měnu některého členského státu, včetně EUR;
- zmínky o evropských zákaznících či uživatelích;
- nabídka doručení zboží/služeb v členských státech;
- webová stránka, na které probíhá nabídka zboží/služeb se nachází na doméně (prvního řádu) některého z členských států (služba.es, služba.fr, ale také např. služba.com/de) či na celoevropské webové doméně .eu.

Ve věci *Pammer* SDEU dále uvedl, že dalšími okolnostmi, které mohou dokládat úmysl cílit na evropské zákazníky, mohou být:

- zaplacení služeb souvisejících s četností vyhledávání ve vyhledávači; a/nebo

[332] Rozhodnutí SDEU ze dne 7. prosince 2010 ve spojených věcech C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) a Hotel Alpenhof GesmbH v Oliver Heller (C-144/09).

– „mezinárodní rozměr“ dané činnosti (např. turistické aktivity, zmínky o telefonních číslech s mezinárodní předvolbou), mezinárodní klientela z různých členských států.

Podmínkou uplatnění GDPR není úplatnost nabízeného zboží a služeb. Tedy i v případě, že se jedná o služby (typicky např. mobilní aplikace, sociální sítě aj.) nabízené zdarma, které však splňují další podmínky dle tohoto ustanovení, uplatní se pravidla nařízení.

Příklad:

Americký e-shop nabízí na svých stránkách platby v eurech a navíc běžně nabízí doručení do všech členských států EU, na čemž rovněž staví svou reklamu. Na takový e-shop se uplatní pravidla GDPR.

Příklad:

Developer z Jižní Ameriky vytvoří mobilní aplikaci, kterou zdarma zpřístupní na svých webových stránkách. Jedna z funkcionalit aplikace je možnost ji – díky strojovému překladači – používat až ve 100 různých jazycích, včetně němčiny, polštiny a francouzštiny. Na evropský trh však nijak nemíří ani aktivně svou aplikaci nenabízí evropským uživatelům. Na takového developera by se pak GDPR nemělo uplatnit.

3.2.5.3 Zpracování osobních údajů související s monitorováním jejich chování, pokud k němu dochází v rámci Unie

Podle čl. 3 odst. 2 písm. b) GDPR se pravidla ochrany osobních údajů dle tohoto nařízení rovněž uplatní, jestliže zpracování souvisí s monitorováním chování subjektů údajů, pokud k tomuto chování dochází v Unii. Z českého znění této podmínky (*zpracování souvisí s monitorováním jejich chování, pokud k němu dochází v rámci EU)* není zjevné, zda má v rámci EU docházet k monitorování či samotnému chování, které správce/zpracovatel monitoruje. Tyto pochybnosti vylučuje anglické znění GDPR, podle kterého se nařízení uplatní *as far as their behaviour takes place within the Union*.

Správce/zpracovatel tak musí vyvíjet aktivity, které vedou k monitorování chování subjektů údajů. K tomuto chování pak musí docházet na území EU. Pokud by správce/zpracovatel monitoroval chování mimo území EU, není naplněna podmínka ustanovení čl. 3 odst. 2 písm. b) GDPR.

Podle bodu 23 úvodního ustanovení GDPR pak navíc platí, že k určení, zda může být činnost zpracování považována za monitorování chování subjektu údajů, by mělo být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, které se jí týká, nebo za účelem analýzy či odhadu jejích osobních preferencí, postojů a chování.

Je zjevné, že uplatnění GDPR podle tohoto ustanovení rovněž míří na prostředí internetu a využití nových technologií. Za monitoring tak může být považována jakákoliv forma *web trackingu*, jako např. sledování chování na internetu prostřednictvím *cookies* či různých forem využívání sociálních služeb a např. sledování jejich využití pro přihlašování k jiným službám (prostřednictvím *social media plug-ins*). Využití těchto nástrojů velmi často samo o sobě umožňuje monitorování uživatelů a jejich chování na internetu.

Může se též jednat např. o monitoring chování uživatelů při využívání mobilní aplikace – jak dlouho má uživatel mobilní aplikaci otevřenou, jak často ji užívá, jakým způsobem ji užívá (vyhledávání, reklama) apod. Rovněž se může jednat o sběr různých preferencí uživatele, díky kterému si správce/zpracovatel vytváří jeho konkrétní profil – a na základě toho mu pak např. nabízí konkrétní reklamu.

Veškeré takové operace by měly být považovány za sledování chování uživatele a budou předmětem GDPR. Tyto operace jsou navíc předmětem speciální sektorové regulace, kterou je dnes *ePrivacy* směrnice, u které se předpokládá nahrazení připravovaným nařízením tzv. *ePrivacy Regulation*. Již dnes *ePrivacy* směrnice (implementovaná především do zák. o některých službách informační společnosti a zák. o el. komunikacích) upravuje např. využívání cookies.[333] Od *ePrivacy Regulation* se pak očekává komplexní úprava otázek spojených se

[333] Pozn. v této oblasti došlo k úpravě české implementace v zákoně o elektronických komunikacích.

zpracováním osobních údajů v internetovém prostředí, včetně využívání *cookies*, cílené reklamy, šifrování aj.

Ustanovení čl. 3 odst. 2 písm. b) GDPR nestanoví žádné podmínky pro samotné subjekty údajů. Podmínkou aplikace GDPR tak není státní příslušnost či trvalý pobyt na území EU. Podstatné je, že k samotnému chování dochází na území EU.

3.2.5.4 Působnost obecného nařízení o ochraně osobních údajů na základě mezinárodních dohod

Ustanovení čl. 3 odst. 3 GDPR stanoví, že obecné nařízení o ochraně osobních údajů se uplatní také na zpracování osobních údajů prováděné správcem, který není usazen v EU, avšak sídlí na místě, kde se právo některého z členských států EU uplatní na základě mezinárodního práva veřejného. Cílem článku 3 odst. 3 GDPR je zohlednit případy, kdy se nařízení aplikuje na základě mezinárodních smluv, jako je tomu například v případě velvyslanectví a konzulátů členských států EU nebo letadel a lodí. Pro velvyslanectví a konzuláty obecně platí, že se na ně nevztahuje právo státu, ve kterém se nacházejí, ale právo státu, který zastupují.

Význam tohoto ustanovení v obchodním kontextu bude pro správce/zpracovatele pouze nepatrný.

3.2.6 Volný pohyb osobních údajů[334]

Pro nakládání s osobními údaji v rámci Evropské unie je významný institut volného pohybu osobních údajů, který byl hlavním účelem směrnice 95/46/ES.[335] Pro osobní údaje je zásada volného pohybu těchto dat výslovně zakotvená v čl. 1 odst. 3 GDPR a vyplývá z potřeb jednotného trhu Evropské unie. Tato úprava

[334] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European and US constitutionalism: comparing essential elements. Cambridge: Cambridge University Press, 2005.

[335] Srov. rozhodnutí Soudního dvora Evropské unie ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist, bod 41.

navazuje na čl. 16 odst. 2 SFEU, který předvídá přijetí pravidel o volném pohybu osobních údajů. Volný pohyb osobních údajů v rámci EU je navíc nezbytným požadavkem pro rozvoj digitální ekonomiky na celém vnitřním trhu, jak předpokládá bod 7 úvodních ustanovení GDPR.

Členské státy by neměly klást překážky pro volný pohyb osobních údajů a neměly by stanovit např. požadavky na umístění některých údajů pouze na území svého státu nebo požadovat přísnější požadavky na přenos některých údajů do ostatních členských států. Takové požadavky by byly v rozporu s GDPR a nebyly by uplatnitelné. Zásada volného pohybu osobních údajů by se měla zachovat rovněž v případech, kdy GDPR členským státům umožňuje, aby si zvláštní záležitosti upravovaly samy, tedy např. v případě omezení některých práv z důvodu národní bezpečnosti (k tomu srov. Hlava IV ZZOÚ) nebo jiných výjimek, kde se členské státy mohou odchýlit od obecné úpravy GDPR (zejména čl. 23 GDPR). I v takovém případě by však měly členské státy dbát na to, aby nedocházelo k omezování volného pohybu údajů v rámci EU. Za území EU se pak považují i státy, které jsou součástí Evropského hospodářského prostoru (GDPR je tedy na základě dohody o Evropském hospodářském prostoru aplikovatelné i v rámci těchto států, které nejsou jinak členy EU – jedná se o Norsko, Island a Lichtenštejnsko).

Opačně GDPR přistupuje k předávání osobních údajů mimo území Evropské unie, resp. Evropský hospodářský prostor. Aby správce či zpracovatel mohli osobní údaje předávat mimo území EU (resp. EHP), musí splnit konkrétní podmínky dále stanovené v čl. 44–50 GDPR.

Úřad pro ochranu osobních údajů v souvislosti se zásadou volného pohybu osobních údajů v Evropské unii zdůrazňuje, že toto pravidlo nelze považovat za právní důvod k předávání osobních údajů jinému správci v rámci EU (resp. EHP)[336]. Možnost předávat osobní údaje bez omezení v Evropské unii se týká institucionálního zabezpečení, tj. pouze vyjadřuje, že v zemích EU platí stejně vysoký standard právního rámce ochrany osobních údajů při jejich zpracování

[336] Úřad pro ochranu osobních údajů ve věci „Předávání osobních údajů do jiných zemí“. [online]. [cit. 2022-03-14]. dostupné z https://www.uoou.cz/10-predavani-osobnich-udaju-do-jinych-zemi/d-27284.

a není tak nutné zajišťovat jejich institucionální bezpečnost. K samotnému předání jinému správci musí mít správce právní důvod, jelikož i předání je jednou z činností zpracování. Právní důvod musí mít správce i tehdy, pokud předává osobní údaje do země mimo Evropskou unii, kdy navíc musí být splněny podmínky pro předání osobních údajů i z hlediska jejich institucionálního zabezpečení.

Se zásadou volného pohybu osobních údajů zároveň úzce souvisí i pohyb jiných než osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii. To v čl. 4 stanovuje, že požadavky na lokalizaci údajů jsou zakázány, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality.

Vliv regulatorní praxe, zejména pak GDPR, připouští i americká doktrína, která se pro regulaci zájmů spotřebitelů odvolává právě na GDPR.[337]

3.3 Limity ochrany osobních údajů dle obecného nařízení o ochraně osobních údajů[338]

3.3.1 Aplikovatelnost pouze na fyzické osoby

Působnost obecného nařízení na ochranu osobních údajů je omezena jen na ochranu fyzických osob. Právnické osoby ochranu dle nařízení nepožívají. Ačkoliv právnické osoby mají rovněž ústavně zajištěná osobnostní práva, jejich údaje nelze považovat za osobní údaje a nepodléhají tak ochraně poskytované

[337] Srov. např. Elvy, Stacy-Ann. "PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY." Columbia Law Review 117, no. 6 (2017): 1369–1459. http://www.jstor.org/stable/44392955.

[338] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 29 - 39.

Další použité literární zdroje v této kapitole:

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European

tímto nařízením. Podle bodu 14 úvodního ustanovení se GDPR nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby. Nicméně i údaje týkající se právnických osob mohou být předmětem ochrany dle GDPR, pokud je možné z nich dovodit identitu konkrétní fyzické osoby. Typickým příkladem budou kontaktní e-mailové adresy či telefonní čísla právnické osoby přiřazené konkrétním osobám (např. jméno.příjmení@společnost.cz). Ochrany dle GDPR naopak nepožívají kontaktní údaje právnických osob, které nelze přiřadit žádné fyzické osobě (např. info@společnost.cz), případně telefonní číslo na ústřednu či helpdesk.

Stejnou míru ochrany jako obecné nařízení o ochraně osobních údajů pak přiznává i český zákon o zpracování osobních údajů, který chrání soukromí „každého“, tedy každé fyzické osoby. Dikce koresponduje s Listinou, která garantuje základní lidská práva, včetně práva na soukromí, rovněž každému, a to bez ohledu na občanství či jiná kritéria. Ačkoliv judikatura dlouhodobě přiznává některá lidská práva i právnickým osobám[339], jedná se však o taková lidská práva, u kterých to specifická povaha právnických osob připouští. S ohledem na skutečnost, že ZZOÚ zaručuje naplnění práva na soukromí v rovině ochrany osobních údajů a je pouze prováděcím předpisem nařízení, uplatní se, stejně jako nařízení, pouze na ochranu fyzických osob. Údaje právnických osob tak přímo nepodléhají ochraně poskytované obecným nařízením ochraně osobních údajů ani zákonem o zpracování osobních údajů.

V každém případě však platí, že ochrana osobních údajů se vztahuje jak na fyzické osoby nepodnikatele, tak na fyzické osoby podnikatele – v České republice tedy tzv. osoby samostatně výdělečně činné (OSVČ), včetně osob vykonávajících svobodná povolání (advokáti, lékaři aj.) Údaje týkající se podnikání fyzické osoby mohou být povinně zveřejňovány dle zákona či zpracovávány např. orgány veřejné moci dle zákona či ve veřejném zájmu, avšak nejsou v principu vyňaty z působnosti GDPR.

[339] Srov. např. nález Ústavního soudu ze dne 10. října 1996, sp. zn. I. ÚS 181/95, nebo nález Ústavního soudu ze dne 6. září 2010, sp. zn. I. ÚS 1744/10.

Navzdory nálezu Ústavního soudu ČR z roku 2004, který dovodil, že osobní údaje o podnikatelské činnosti nespadají do působnosti zákona o ochraně osobních údajů[340], jsou dnes údaje o fyzických podnikajících osobách běžně považovány za osobní údaje podléhající ochraně GDPR. Původní nález ÚS byl tak překonán judikaturou SDEU. Osobní údaje OSVČ proto požívají stejné úrovně ochrany jako údaje každé jiné (nepodnikající) fyzické osoby, ač OSVČ musí strpět určitou vyšší míru zásahu (např. zveřejnění údajů ve veřejných rejstřících apod.).

3.3.2 Nenarozené děti

Poslední spornou skupinou fyzických osob jsou z hlediska aplikace pravidel GDPR nenarozené děti. GDPR se k této otázce nijak nevyjadřuje a lze tak předpokládat, že pravidla ochrany osobních údajů se na nenarozené dítě (tzv. nasciturus) vztáhnou v tom rozsahu, v jakém mu národní předpisy přiznávají jiná práva.

V českém právním řádu se tak uplatní § 25 o. z.: *„Na počaté dítě se hledí jako na již narozené, pokud to vyhovuje jeho zájmům. Má se za to, že se dítě narodilo živé. Nenarodí-li se však živé, hledí se na ně, jako by nikdy nebylo.“* Pokud se tedy bude jednat o údaje nenarozeného dítěte, podléhají stejné ochraně dle GDPR jako údaje každé jiné fyzické osoby. Pokud by se dítě však nenarodilo živé, tyto údaje přestanou požívat ochrany poskytované nařízením, a to od počátku *(ex tunc)*. V případě zpracování osobních údajů nascitura (kterým může být např. záznam z ultrazvuku, zdravotnická dokumentace aj.) za něj budou jednat zákonní zástupci dle obecných pravidel občanského zákoníku (srov. kapitolu 2.4 výše). Lze však předpokládat, že tyto údaje budou v naprosté většině případů zároveň osobními údaji matky, a proto v praxi budou téměř vždy požívat ochrany dle GDPR z tohoto titulu.

3.3.3 Zesnulé osoby

Podle bodu 27 úvodních ustanovení se nařízení nevztahuje na osobní údaje zesnulých osob. V případě, kdy subjekt údajů zemře, přestanou jeho údaje podléhat ochraně dle GDPR. Tím však nejsou dotčena práva na ochranu osobnosti

[340] Srov. nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02.

podle občanského zákoníku, kterých se následně mohou domáhat pozůstalí (srov. § 81 a násl. o. z.), jak je blíže analyzováno v kapitole 2.4 výše.

Údaje o zesnulých osobách mohou být v některých případech zároveň osobními údaji jiných dosud žijících osob (např. anamnéza, údaje o příbuzenských vztazích apod.). Takové údaje požívají nadále ochrany dle obecného nařízení o ochraně osobních údajů. Některé dokumenty týkající se zemřelých osob, jako např. oznámení o úmrtí osoby, mohou obsahovat i údaje o jiných dosud žijících osobách (pozůstalých), se kterými bude nezbytné nakládat jako s osobními údaji dle GDPR.

3.4 Vliv GDPR mimo EU[341]

Členské státy, díky jednotné právní úpravě, nabízejí rovnocennou ochranu pro data uchovávaná a/nebo přenášená přes jejich území, a právě díky tomu nelze v rámci EU stanovit jakákoliv dílčí omezení (s výjimkou např. vnitřní bezpečnosti). V této souvislosti se však nejedná pouze o volný přenos osobních údajů[342], ale stejně tak o zajištění volného pohybu všech neosobních dat, k čemuž bylo přijato nařízení o volném pohybu neosobních údajů.[343]

Z globálního hlediska se pak obecně zdá, že Evropská unie stanovila přijetím GDPR a ostatních souvisejících předpisů digitálního trhu nový světový standard ochrany soukromí jednotlivce. Zároveň, jak uvedl *The New York Times,* se díky GDPR stal z Evropy přední technologický kontrolor („*Europe World's Leading Tech Watchdog*“).[344]

---

[341] Části textu v této kapitole byly publikovány jako VÍTEK, Dominik. Evropa jako světový standard pro bezpečnost (osobních) dat [online]. 31.7.2018 [cit. 2022-03-16]. Dostupné z: https://jinepravo.blogspot.com/2018/07/evropa-jako-svetovy-standard-pro.html.

[342] Volný pohyb osobních údajů je stěžejním principem GDPR a základních pravidel pro ochranu osobních údajů v rámci Evropy – ze stejného principu vycházela rovněž předcházející směrnice 95/46/ES, a rovněž také např. Úmluva č. 108.

[343] Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[344] G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. [online]. [cit. 2022-03-27]. Dostupný z https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

Celosvětově se začaly objevovat nové národní předpisy, které často přejímají základní koncepty ochrany osobních údajů zakotvené v evropském právu, resp. přímo v GDPR. Jedním z příkladů může být zákon o ochraně osobních údajů státu Kalifornie.[345] Obdobně byla přijata nová pravidla ochrany soukromí a osobních údajů v Jihoafrické republice[346], Thajsku[347] či Singapuru[348]. V každém případě alespoň 19 z 20 zemí má implementován právní rámec, který umožňuje uplatnění práva být zapomenut coby součástí ochrany osobních údajů a soukromí.[349] Zdá se tak, že evropské principy ochrany osobních údajů jsou (a budou) postupně přebírány a implementovány ostatními státy světa, které mají zájem (i) umožnit svým společnostem bezproblémový obchod s evropskými hráči, (ii) zajistit svým občanům odpovídající úroveň ochrany osobních údajů. S dopady obecného nařízení o ochraně osobních údajů a implementaci jeho požadavků však rovněž přicházejí zásadní náklady, které mohou být především pro menší podniky značně zatěžující; zákonodárci (včetně evropského zákonodárce) by tak měli zvážit univerzální aplikaci pravidel, popř. naopak její např. progresivní aplikaci.[350]

Tato vlna nových předpisů samozřejmě nepřišla svévolně. Evropské předpisy (zejména tedy GDPR) ztěžují přenosy osobních údajů do zemí, které nenabízejí odpovídající úroveň ochrany soukromí osob a podmiňují takové přenosy dalšími právními konstrukty – ať se jedná o tzv. *adequacy decisions*, uzavření

[345] California Consumer Privacy Act. Assembly Bill No. 375. [online]. [cit. 2022-03-14]. Dostupný z https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[346] South Africa - Data Protection Overview. [online]. [cit. 2022-03-14]. https://www.dataguidance.com/notes/south-africa-data-protection-overview.

[347] Thailand - Data Protection Overview. [online]. [cit. 2022-03-14]. Dostupné z https://www.dataguidance.com/notes/thailand-data-protection-overview.

[348] Singapore - Data Protection Overview. [online]. [cit. 2022-03-14]. Dostupné z https://www.dataguidance.com/notes/singapore-data-protection-overview.

[349] ERDOS, David and GARSTKA, Krzysztof, The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frameworks (September 10, 2019). University of Cambridge Faculty of Law Research Paper No. 31/2019. [online]. 10.9.2019. [cit. 2022-02-20]. https://ssrn.com/abstract=3451269 or http://dx.doi.org/10.2139/ssrn.3451269.

[350] K tomu srov. např. FREY, Carl Benedikt a Giorgio PRESIDENTE. The GDPR effect: How data privacy regulation shaped firm performance globally [online]. 10.3.2022 [cit. 2022-03-27]. Dostupné z: https://voxeu.org/article/how-data-privacy-regulation-shaped-firm-performance-globally.

standardních smluvních doložek či závazných podnikových pravidel.[351] S tím rovně souvisí významné aspekty přenosu osobních údajů mimo území EU.

Rozbor přenosů osobních údajů mimo území EU však značně přesahuje rozsah této práce. Přesto si dovolím uvést jeden příklad za všechny – přenosy osobních údajů mezi Evropou a Spojenými americkými, které prošly v poslední dekádě značně turbulentním vývojem a které jsou přitom zcela zásadní pro transatlantickou spolupráci (zejména technologických gigantů). Vývoj právního rámce přenosů osobních údajů mezi EU a USA přitom poměrně výstižně demonstruje význam obecného nařízení o ochraně osobních údajů pro globální, resp. přinejmenším pro transatlantickou ekonomiku a kontinuální vliv a posuny v oblasti ochrany soukromí.

Přenos osobních údajů původně spadal právě pod tzv. adequacy decision – resp. tzv. Safe Harbour (tedy jakýsi bezpečný přístav)[352]. To bylo následně zrušeno v roce 2015 rozhodnutím SDEU ve věci Schrems[353] pro nedostatek ochrany poskytované ochraně osobních údajů ze strany Spojených států. Evropa spolu s USA vcelku obratem reagovaly přijetím tzv. Privacy Shield (tj. „štítu soukromí“) v podobě nového adequacy decision[354]. I tento právní rámec byl však následně, v roce 2020, prohlášen za neplatný Soudním dvorem ve věci Schrems II[355]. Soudní dvůr v tomto rozsudku navíc nezpochybnil jen Privacy Shield jako konkrétní právní instrument pro přenosy dat mezi EU a USA, ale zároveň i

[351] Srov. kapitola V GDPR.

[352] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), dostupné z https://op.europa.eu/en/publication-detail/-/publication/10e48a32-d701-4524-b7e9-8f270365c5c0/language-en. Více informací o přenosu dat mezi EU a USA je rovněž dostupných např. z https://iapp.org/resources/article/us-eu-safe-harbor-guidance-and-resources/.

[353] Rozhodnutí Soudního dvora Evropské unie ze dne 6. 10. 2015 ve věci C-362/14 Maximillian Schrems v Data Protection Commissioner.

[354] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 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) (Text s významem pro EHP).

[355] Rozhodnutí SDEU ze dne 16. července 2020 ve věci C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems.

legalitu jakýchkoliv přenosů osobních údajů do Spojených států (ač založených na jiných právních základech, jako jsou např. tzv. standardní smluvní doložky[356]) – a to zejména pro příliš extenzivní oprávnění některých amerických bezpečnostních složek. Ačkoliv na rozsudek Schrems II navázaly dozorové orgány (včetně Evropského sboru pro ochranu osobních údajů) vydáním několika výkladových stanovisek[357], právní režim přenosu osobních údajů do USA zůstal přinejmenším rozporuplný a pro dotčené subjekty (správce / zpracovatele) jen těžko uchopitelný.[358] Řešení by však měl s velkou mírou pravděpodobnosti přinést nový právní rámec pro transatlantickou ochranu soukromí („*Trans-Atlantic Data Privacy Framework*"), který Evropská komise oznámila dne 25. března 2022.[359]

3.5 Závěr

Oblast ochrany osobních údajů je podmnožinou práva na ochranu osobnosti a soukromí, které jsou chráněné na ústavní úrovni. Kromě občansko-právní ochrany poskytované osobnosti existuje rovněž specifická právní úprava týkající se ochrany osobních údajů, přímo navazující na čl. 8 Listiny EU, v podobě obecného nařízení o ochraně osobních údajů, jehož působnost byla zkoumána v této kapitole.

Obecné nařízení o ochraně osobních údajů v čl. 17 výslovně zakotvuje právo být zapomenut (právo na výmaz), které je předmětem zkoumání v kapitole 6 této práce. Pro jeho aplikaci je přitom stěžejní vymezení základních pojmů, jejichž definice je rovněž poskytnuta v čl. 4 GDPR.

---

[356] Srov. čl. 46 odst. 2 písm. b) nebo písm. c) GDPR.

[357] Např. Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU ze dne 10. listopadu 2020, dostupné z https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_cs.pdf-

[358] Srov. např. Zalnieriute, Monika, Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security (April 14, 2021). Vanderbilt Journal of Transnational Law, (2022) 55(1), pp. 1-48 , UNSW Law Research, Available at SSRN: https://ssrn.com/abstract=3826878.

[359] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework ze dne 25. 3. 2020 [online]. Dostupné z https://ec.europa.eu/commission/presscorner/detail/cs/ip_22_2087.

Základní pojmy, které vymezují rovněž možnosti aplikace GDPR jako takové, jsou osobní údaje a zpracování osobních údajů. V případě, kdy se konkrétní data nekvalifikují jako osobní údaje, nelze aplikovat pravidla vyplývající z GDPR. Stále však může dojít k uplatnění ochrany osobnosti, jak je popsaná v kapitole 2 výše. Osobní údaje jsou přitom vymezeny velmi široce a neustále dochází k rozšiřování tohoto pojmu prostřednictvím judikatury (zejména) SDEU. Od roku 2011 je takto např. vyjasněné, že osobním údajem je i IP adresa a od roku 2016 pak i dynamická IP adresa. Výklad pojmu osobní údaj je přitom do značné míry subjektivní a vždy bude záležet na tom, zda konkrétní subjekt (resp. správce/zpracovatel) disponuje dostačujícím množství (právních) prostředků k tomu, aby získal přístup k doplňujícím údajům, které mu umožní v daném případě identifikovat konkrétní osobu.

Obecné nařízení pak vymezuje rovněž další podmnožiny dat, kterým poskytuje vyšší míru ochrany – tzv. zvláštní kategorii osobních údajů, pro jejichž zpracování správce vždy musí splnit některou z výjimek zakotvenou v čl. 9 GDPR, přičemž správce musí vždy naplnit podmínky čl. 6 odst. 1 GDPR (tj. disponovat dostačujícím právním základem zpracování), jak je blíže analyzováno a demonstrováno na příkladu opětovného zpracování zveřejněných osobních údajů v kapitole 4.3 níže.

Rovněž pojem zpracování osobních údajů je vymezen velmi široce a jedná se tak v zásadě o jakékoliv nakládání s osobními údaji, a to včetně jejich „terminální“ fáze – tj. výmaz/likvidace těchto údajů, případně jejich anonymizace. Pojem anonymizace je přitom velmi zásadní pro případné další nakládání s konkrétním setem osobních údajů, kde bylo dokázáno, že anonymizace může mít, při splnění všech podmínek, které zaručí, že data jsou skutečně anonymizována, stejný význam jako samotný význam údajů a může být jedním z nástrojů, jak dosáhnout práva být zapomenut. S pokračujícím vývojem technologií přitom může být splnění těchto podmínek stále náročnější, jelikož aby byly splněny podmínky takové komplexní anonymizace, nesmí existovat způsob, jak daný set dat zpětně „de-anonymizovat“ a dobrat se původních osobních údajů. V justiční praxi a při naplňování práva na informace přitom anonymizace hraje významnou roli při zveřejňování a poskytování rozhodovací praxe veřejnosti.

Obecné nařízení poskytuje ochranu soukromí fyzickým osobám, nicméně jeho věcná aplikace je omezena některými výjimkami. V případě, kdy nebude možné aplikovat pravidla GDPR, vždy je možné postupovat prostřednictvím ochrany osobnosti. Předně se tedy musí jednat o oblast osobních údajů, přičemž jejich automatizované zpracování bude pod ochranu a pravidla GDPR spadat vždy, neautomatizované jen při splnění dvou kumulativních podmínek: osobní údaje jsou zařazené v evidenci (či do ní mají být zařazeny) a tyto osobní údaje jsou uspořádané podle systematického hlediska.

Vzhledem k tomu, že GDPR je nařízením Evropské unie, má přímou aplikační přednost. To však rovněž znamená, že jeho působnost je omezena rozsahem působnosti práva EU. Jakmile by se jednalo o oblast, ve které evropské právo nemá podle SEU a SFEU působnost (jako je např. veřejný pořádek, obrana a národní bezpečnost), nelze bez dalšího uplatňovat pravidla GDPR. Český zákonodárce tento případný nedostatek právní ochrany zhojil v zákoně o zpracování osobních údajů, podle kterého se pravidla GDPR uplatní i na tyto oblasti jinak nepokryté oblastí evropského práva. Vedle toho se GDPR neuplatní na oblast zahraniční a bezpečnostní politiky, trestněprávní oblasti (ve které je však ochrana osobních údajů zajištěna prostřednictvím směrnice 2016/680 implementované v podobě hlavy III zákona o zpracování osobních údajů) a zpracování osobních údajů institucemi EU (které se však řídí specifickým nařízením č. 2018/1725). Pro aplikaci pravidle je rovněž významná tzv. domácí výjimka (zpracování výlučně osobních či domácích činností) – pravidla GDPR tak nebude možné uplatnit např. na osobní údaje uložené v mobilním telefonu, počítači či jiném úložišti využívaném výlučně pro soukromou potřebu. Stejně tak se neuplatní na bezpečnostní kamery instalované na rodinných domech. Pravidla v GDPR rovněž nevylučují aplikaci pravidel *eCommerce* směrnice implementovanou v zákoně o některých službách informační společnosti a stále se tak uplatní omezení v podobě aplikace pravidel *mere conduit, cachingu* či *hostingu.*

V případě, že bude docházet k uplatnění práva být zapomenut v oblastech, které nejsou vyňaty z působnosti GDPR, vždy bude možné postupovat přímo podle pravidel zakotvených v čl. 17 GDPR. Pokud by nebylo možné uplatnit

tato pravidla, vždy zůstává k dispozici možný postup dle obecných pravidel ochrany osobnosti garantovanou na ústavní úrovni a podrobně upravenou v občanském zákoníku.

Z hlediska místní působnosti bude pravidla vyplývající z GDPR možné uplatňovat bez dalšího kdekoliv na území Evropské unie (EU) a Evropského hospodářského prostoru (EHP) – tedy, pokud má správce či zpracovatel provozovnu na území EU/EHP, které lze shrnout do následujících bodů:

a. EU provozovna sbírá a zpracovává osobní údaje sama;

b. EU provozovna sbírá osobní údaje v jednom členském státě a zpracovává je provozovna v jiném státě;

c. EU provozovna zpracovává osobní údaje prostřednictvím entity (zpracovatele) usazené mimo území EU;

d. EU provozovna zpracovává osobní údaje pro entitu (správce) usazenou mimo území EU;

e. EU provozovna nezpracovává žádné osobní údaje (tedy ani v postavení zpracovatele), avšak svou činností ekonomicky významně podporuje mimoevropskou entitu (svou mateřskou společnost, se kterou má úzký vztah), která pak provádí zpracovatelské operace.

Obecné nařízení o ochraně osobních údajů se dále vztahuje i na zpracovatelské aktivity, které provádí správce/zpracovatel, jehož provozovna je mimo území jakéhokoliv členského státu, avšak k tomu zpracování splňuje jednu z následujících podmínek:

a. zpracování souvisí s nabídkou zboží nebo služeb těmto subjektům údajů v EU (bez ohledu na to, zda je požadována platba); a/nebo

b. zpracování zahrnuje monitorování chování subjektů údajů, ke kterému dochází na území EU.

Tato extrateritoriální aplikace mimo území EU má cílit především na internetové aktivity, nicméně její praktická vymahatelnost může být velmi omezená a v případě, že nedojde k dobrovolné aplikaci, bude vyžadovat zahraniční

vymáhání tohoto práva dle pravidel mezinárodního práva soukromého. Význam této (poměrně ambiciózní) extrateritoriální působnosti je nicméně stále zásadní a ve svém důsledku (ve spojení s obecným významem Evropy a jejího právního řádu) v zásadě z GDPR vytvořil celosvětový standard ochrany osobních údajů, kterému se postupně začaly přibližovat různé lokální právní řády. Nejvýznamnější dopady lze přitom pozorovat zejména ve vztahu k USA, kde oblast těchto transatlantických přenosů osobních údajů prodělala v poslední dekádě značně dynamický rozvoj, a zásadně tak posouvá rovněž oblast ochrany osobních údajů ve Spojených státech, a s tím i spojenou potenciální vymahatelnost práv garantovaných v GDPR (vč. práva být zapomenut).

4 Data a osobní údaje

4.1 Digitální stopa a permanence dat v digitálním světě

4.1.1 Permanence informací v digitálním světě

V roce 2017 magazín The Economist uvedl, že světovým největším bohatstvím již není ropa, ale data.[360] Zatímco však v běžném (offline) životě uvedená data a informace plynutím času přirozeně vymizí z myslí jednotlivců, v prostředí internetu tyto údaje zůstávají uloženy v různých databázích, případně jsou volně šířeny, nadto i různě samovolně kombinovány a vkládány do různých kontextů, a to leckdy velmi nepřesným, účelovým (viz skandál kolem využití dat společností Cambridge Analytica k ovlivňování postojů voličů, jak je popsaný níže) či difamačním způsobem, majících potenciál závažným způsobem zasáhnout do soukromé sféry dotčeného jednotlivce.[361]

Permanence informací v digitálním světě souvisí rovněž také s tzv. digitální pamětí, která významně znesnadňuje principy a účely zapomínání.[362] Naprostá většina informací sdílených na internetu tak zůstává automaticky uložena, a pro jejich smazání musí člověk učinit vědomé rozhodnutí a vynaložit určité úsilí. Informace na internetu navíc ztrácí původní kontext, ve kterém byly zveřejněny nebo kterého se týkaly a tento kontext se vytrácí jak plynutím času, tak jakýmkoliv dalším (útržkovitým či kusým) sdílením a přebíráním jednotlivých informací.

Tyto aspekty vývoje komunikačních technologií tak vedou k tomu, že značné množství informací je dostupných napříč prostorem a časem. Kombinace obou těchto aspektů je pro naplňování legitimně očekávatelných funkcí internetu navíc

[360] The world's most valuable resource is no longer oil, but data. [online]. 6.5.2017 [cit. 2022-03-16]. Dostupné z https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[361] KOKEŠ, M. in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s 349.

[362] Srov. např. BLANCHETTE, Jean-François a JOHNSON, Deborah G. Data retention and the panoptic society: The social benefits of forgetfulness. The Information Society. 2002, 18(1), 33–45. s. 35.

zcela nezbytná, neboť informace dostupné odkudkoli, ale po nulovém množství času, stejně tak jako informace dostupné věčně, ale odnikud, nemají žádný praktický význam.[363] Tento fenomén poprvé pojmenovala cizojazyčná literatura jako *„practical obscurity"*[364] (dále používám volně přeložené jako *„praktická neznámost"*) vycházející z judikatury Nejvyššího soudu USA[365], který popisuje ochranu soukromí v před-internetové době jako přirozeně existující prvek. Díky této praktické neznámosti (vyplývající z úsilí, které je hledající nucen pro sběr a hodnocení informací o konkrétním subjektu vynaložit) dohledání informací o konkrétním tématu či osobě zpravidla vyžadovalo též elementární znalost objektu hledání a kontextu hledaných informací. Praktická neznámost je tedy podložena především plynutím času, roztříštěnosti informací a značně omezeným možnostem při získávání vstupních údajů znesnadňující další vyhledávání informací. Tento prvek je však na internetu popírán a díky vzájemné neomezené provázanosti informací a jejich indexaci značně upozaďován.

Tuto „hyperprovázanost" umožňují především internetové vyhledávače, ale rovněž jakékoliv jiné elektronické databáze umožňují (automatizovaným) způsobem provazovat jednotlivé informace. Dochází tak k vytváření jakýchsi osobních profilů, které jsou složené částečně z informací, které jsme na internetu sami a dobrovolně sdíleli (např. v podobě vlastních profilů na sociálních sítích), jakož ovšem i z informací, které o nás sdílel někdo jiný, proti naší vůli nebo i bez našeho vědomí[366] (ať už se jedná o veřejně přístupné rejstříky a seznamy,

---

[363] KORENHOF, Paulan, AUSLOOS, Jef, SZEKELY, Ivan, JONES, Meg Leta, SARTOR, Giovanni a LEENES, Ronald E. Timing the Right to Be Forgotten: a Study into „Time" as a Factor in Deciding About Retention or Erasure of Data [online]. SSRN Scholarly Paper. ID 2436436. Rochester, NY: Social Science Research Network. 2014 [cit. 21. 3. 2022]. Dostupné z: https://papers.ssrn.com/abstract=2436436.

[364] Srov. TENE, Omer. What Google Knows: Privacy and Internet Search Engines. Utah Law Review. 2008, 2008, 1433–1492;

JONES, Meg Leta. You are what Google says you are: The right to be forgotten and information stewardship. International Review of Information Ethics. 2012, 17, 22–30;

CARBONE, Chelsea E. To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age. Virginia Journal of Social Policy & the Law. 2015, 22, 525–560.

[365] Rozsudek Nejvyššího soudu USA United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

[366] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 108.

novinové články nebo např. informace zveřejňované jinými uživateli na sociálních sítích).

Příkladem takové provázanosti o informací mohou být např. informace zveřejňované právě ve veřejných rejstřících (jako v obchodním rejstříku nebo živnostenském rejstříku) doplněné o informace z veřejných seznamů (katastru nemovitostí) a např. ještě ve spojení s profilem na sociálních sítích. Takový set informací je v dnešní době snadno získatelný během pár kliknutí na základě v zásadě jen základního setu vstupních informací (jméno a bydliště nebo jméno a datum narození), na základě kterých lze získat kompletní přehled o ekonomických aktivitách a příjmech (z veřejných rejstříků/seznamů) a volnočasových aktivitách člověka, potenciálně doplněné o jeho politické preference, sexuální orientaci a jiné (mnohdy citlivé) informace. Takové spojení tak může instantně podat komplexní set informací, které jsou navíc permanentně dostupné online.

Rizika spojená se zásahem do osobnosti přitom v tomto případě nejsou spojená jen s „velkým" množstvím informací, které mohou být v konkrétní moment k dispozici kdekoliv online. Mnohdy může být ještě zásadnější riziko naopak nekompletní set informací – ať už z toho důvodu, že jsou zastaralé, část jich nikdy nebyla zveřejněna nebo se jedná jen o kusou informaci vytrženou z původního kontextu. Na podobné nebezpečí upozorňuje např. Mayer-Schönberger, který uvádí, že *„to, co vyvstává [v rámci seznamu odpovědí na dotaz na konkrétní osobu zadaný do vyhledavače] (i tehdy, odpovídají-li prezentovaná fakta realitě) není požadované shrnutí současné existence dané osoby, nýbrž podivná umělá koláž sestávající pouze z informací dostupných v digitálním formátu a opomínající vše ostatní".*[367]

Online informace a výsledky vyhledávání (navíc většinově zkrácené na jednoduchý velmi zkratkovité „googlení" spoléhající na výsledky na první straně

[367] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 108.

namísto alespoň komplexnější rešerše[368]) každého jednotlivce tak vytváří zdání jakéhosi komplexního a koherentního profilu jednotlivce. O tyto výsledky se pak většinově opírají zaměstnavatelé při dohledávání informací o uchazečích[369]. Jinými slovy – v očích ostatních uživatelů internetu jsme tím, co o nás říká Google *(„You are what Gooogle says you are").*[370]

Permanence informací (často navíc nekompletních, kusých, bez kontextu či pouze zastaralých) ve spojitosti s jejich provázaností vytváří reálné nebezpečí, které např. Kühn označuje jako „nesnesitelnou lehkost zjišťování informací"[371]. Před nástupem internetu by tyto informace byly snadno zapomenuté – ať už díky standardnímu fungování lidské paměti i díky zapomínání společnosti jako celku (srov. funkci zapomínání v kapitole 5.1). Nicméně ve věku internetu mohou tyto informace upadnout do digitální věčnosti, a tvořit tak pro některé jedince velkou překážku v jejich začlenění do společnosti.[372]

Kühn zároveň v této souvislosti připomíná, že právě v důsledku celkového vývoje technologií dochází ke kvantitativním i kvalitativním proměnám zásahů do našeho soukromí – jinými slovy zásahů je stále více a ve stále nových oblastech a úrovních soukromého života.[373] Mayer-Schönberger pak uzavírá, že digitální

[368] Podle výsledků studie z roku 2014 67 % výsledků vyhledávání skončilo u prvních pěti výsledků. Až 95 % výsledků vyhledávání pak končí na první straně výsledků, ponechávající pouze 5 % pro veškeré ostatní stránky (často ze stovek tisíc a milionů výsledků). Srov. např. LEVERAGE MARKETING. How Far Down the Search Engine Results Page Will Most People Go? [online]. [cit. 2022-03-16]. Dostupné z https://www.theleverageway.com/blog/how-far-down-the-search-engine-results-page-will-most-people-go/, obdobně pak rovněž např. LESS, Noel. SEO News – Why second page of Google might as well be the last [online]. [cit. 2022-03-16]. https://www.designforonline.com/seo-second-page-google-might-be-last/.

[369] SALM, Lauren. 70% of employers are snooping candidates' social media profiles. Career Builder [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.careerbuilder.com/advice/social-media-survey-2017.

[370] JONES, Meg Leta. You are what Google says you are: The right to be forgotten and information stewardship. International Review of Information Ethics. 2012, 17, 22–30.

[371] KÜHN, Zdeněk. Ochrana soukromí v internetové době. In ŠIMÍČEK, Vojtěch. Právo na soukromí. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. 212 s. ISBN 8021054492110.

[372] ŠOŠOLÍKOVÁ, Hana. „The Right to Be Forgotten" jako řešení problému permanence informací. Brno: Revue pro právo a technologie, 2013, 7. číslo, str. 3 – 12.

[373] KÜHN, Zdeněk. Transformace pojmu soukromí na počátku třetího milénia. Jurisprudence. 2017, XXVI(2). ISSN 1802-3843. s. 7.

paměť nás uvrhá do prostorového a temporálního panoptika[374], zatímco podle Szekelyeho se spíše než o *panoptikon* jedná o *„periptikon"*, neboť v této nové realitě lidského soukromí nevíme nejen to, zda jsme pozorováni, ale nevíme ani kým.[375]

Význam práva být zapomenut, resp. možnosti plně kontrolovat své soukromí a informace, které jsou o každém z nás (v online světě) k dispozici, se tak značně posiluje v souvislosti s neustálým vývojem nových technologií. Je proto nezbytné dávat jednotlivcům nezbytné nástroje, které jim takovou kontrolu poskytnou, a zároveň zajistit jejich právní vymahatelnost.

Snadnou zneužitelnost digitálních informací založenou na široké dostupnosti dat lze také velmi dobře demonstrovat na případu Facebook – Cambridge Analytica. Společnost Facebook dlouhodobě sbírala osobní údaje patřící až 87 milionům uživatelů[376] této sociální sítě, které bez jejich souhlasu dále předávala britské konzultantské společnosti především pro účely politické reklamy.[377] Data byla sbírána prostřednictvím aplikace „This Is Your Digital Life", která zahrnovala sérii otázek, kterou každý uživatel musel zodpovědět pro vytvoření vlastního psychologického profilu. Cambridge Analytica následně využila takto získaná data pro cílení prezidentské kampaně republikánských kandidátů Teda Cruze a Donalda Trumpa v roce 2016.[378] Cambridge Analytika je rovněž viněna za

---

[374] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 114.

[375] SZEKELY, Ivan. The right to forget, the right to be forgotten. In: Serge GUTWIRTH, Ronald LEENES, Paul DE HERT a Yves POULLET, ed. European Data Protection: In Good Health? B.m.: Springer, 2012, s. 347–363. ISBN 978-94-007-2902-5. s. 353.

[376] MEREDITS, Sam. Facebook-Cambridge Analytica: a timeline of the data hijacking scandal. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

[377] CHAN, Rosalie. The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

[378] CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

ovlivňování britského referenda o Brexitu ve stejném roce.[379] K tomu docházelo v přímé souvislosti s neužitím dat získaných o uživatelích a následné možnosti nasazení cílené reklamy v těchto politických kampaních. Jak uzavřel britský dozorový úřad ICO (*Information Commissioner's Office*), spol. Facebook významně narušila soukromí subjektů údajů, když získávala a dále zpracovávala osobních údajů bez jejich souhlasu a vědomí, což byla spol. Facebook v udělena nejvyšší možná pokuta ve výši £ 500.000.[380]

Tento případ ilustruje významnou zneužitelnost dat, které lze posbírat o jednotlivcích z online zdrojů (v tomto případě prostřednictvím jednoduché aplikace na sociální síti). Vzhledem k enormnímu množství subjektů, jejichž data byla tímto způsobem využita se navíc nejedná „jen" o narušení soukromí individuí, ale zneužití tohoto obrovského data setu pro manipulaci s demokratickými principy, a tedy zásah do fundamentálního fungování demokratické společnosti (nedílně spojenou se zásahy do soukromí a vlivem sociálních sítí na fungování jednotlivců a ovlivňování formování jejich (politických) názorů a postojů přímo spojených se zneužitím osobních údajů).

4.1.2 Data retention

S ochranou soukromí vůči státu a (dlouhodobým) uchováváním dat rovněž významně souvisí otázka tzv. data retention, která byla původně na evropské úrovni představena ve směrnici 2006/24/ES, která stanovila povinnost členských států uchovávat tzv. lokalizační a provozní údaje[381], nikoliv samotný obsah komunikace.

[379] KAMINSKA, Izabella. Cambridge Analytica probe finds no evidence it misused data to influence Brexit. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.ft.com/content/aa235c45-76fb-46fd-83da-0bdf0946de2d.

[380] INFORMATION COMMISSIONER'S OFFICE. Investigation into the use of data analytics in political campaigns [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

[381] Srov. rovněž § 90 a násl. zákona o elektronických komunikacích.

V roce 2014 však směrnici zrušil Soudní dvůr Evropské unie ve věci *Digital Rights Ireland Ltd*.[382] Přestože byla tato směrnice zrušena, nejzajímavější otázkou zůstalo to, co SDEU ponechal bez odpovědi – jak se se zneplatněním této směrnice vypořádají členské státy EU, které požadavky stanovené směrnicí implementovaly do své národní úpravy (jelikož pro zrušení směrnice tedy neexistuje povinnost, ale pouze možnost uchovávat provozní a lokalizační údaje).[383] Ke zrušení této směrnice přitom SDEU přistoupil na základě rozsáhlé argumentace, ve které dovodil, že povinnosti a nejasnost pravidel pro ukládání provozních a lokalizačních údajů představují velmi rozsáhlý a zvlášť závažný zásah do těchto základních práv v unijním právním řádu, aniž je takový zásah přesně vymezen ustanoveními umožňujícími zaručit, že je skutečně omezen na nezbytné minimum.

Český Ústavní soud se přitom otázkou shromažďování provozních a lokalizačních údajů zabýval už v roce 2011.[384] K tomuto přezkumu došlo na základě návrhu 51 poslanců, kteří napadali zákon č. 257/2008 Sb., který do zákona o elektronických komunikacích implementoval povinnost data retention ve smyslu směrnice 2006/24/ES, a to v podobě § 97 odst. 3 a 4, které stanovovaly povinnost fyzickým a právnickým osobám v postavení telefonních operátorů a poskytovatelů internetového připojení uchovávat provozní a lokalizační údaje o veškeré telefonní a faxové komunikaci, emailové a SMS komunikaci, návštěvách webových stránek a využívání některých internetových služeb, a to po dobu 6 až 12 měsíců. Na základě třístupňového testu proporcionality Ústavní soud ustanovení § 97 odst. 3 a 4 (a související prováděcí vyhlášku) zrušil, jakožto zcela neadekvátní nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů téměř o veškeré elektronické komunikaci z hlediska intenzity zásahu do soukromé sféry nepřeberného množství účastníků elektronické

[382] Rozhodnutí Soudního dvora Evropské unie ze dne 8. dubna 2014 ve spojených věcech věcech C-293/12 a C-549/12 Digital Rights Ireland Ltd.

[383] HARAŠTA, Jakub, MYŠKA, Matěj. Budoucnost data retention. Trestněprávní revue, 2015, č. 10, s. 238-241.

[384] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

komunikace nástrojem nezbytným a přiměřeným, když se neprokázalo, že by měl nějaký vážnější přínos při objasňování závažných trestných činů.

Český zákonodárce však shledal obdobnou úpravu nezbytnou a zákonem 273/2012 Sb., ji s účinností od ledna 2012 v pozměněné podobě navrátil do právního řádu – kdy tedy každý telekomunikační operátor (poskytovatel veřejné komunikační sítě nebo poskytující veřejně dostupnou službu elektronických komunikací) je povinen uchovávat plošně veškeré lokalizační a komunikační údaje po dobu šesti měsíců[385]. Tato úprava byla předmětem přezkumu Ústavního soudu ve věci *Data Retention II* roce 2019[386], kde se však Ústavní soud poměrně překvapivě[387] odchýlil od svých závěrů z roku 2011, a to i navzdory mezitímního rozhodnutí SDEU ve věci *Digital Rights Ireland* nebo ve věci *Tele2 Sverige AB a Watson*[388]. Navíc v momentě, kdy některé členské státy (například Slovensko, Nizozemsko, Rakousko či Spojené království) zcela zakázaly data retention, tj. plošného preventivního uchovávání provozních a lokalizačních údajů, a přijaly právní úpravu zakotvující méně invazivní nástroje.[389] Ústavní soud přiměřenost data retention v českém právním řádu obhajoval dostatečnými nástroji zabezpečení těchto údajů a rovněž právem na informační sebeurčení podle čl. 10 odst. 2 a 3 LZPS a čl. 13 Listiny EU (srov. rovněž kapitolu 1.3.2.1.3 výše). Ústavní soud se přitom však zabýval pouze otázkou zneužitelnosti ze strany státu (orgánů veřejné moci) a zcela vynechal možnosti zneužitelnosti ze strany soukromoprávních subjektů[390] (tedy zejména telekomunikačních operátorů, na které se tato povinnost vztahuje). Odlišné stanovisko k tomuto závěru podala

[385] Srov. ustanovení § 97 odst. 3 ZEK v aktuálním znění.

[386] Nález Ústavního soudu ze dne 14. května 2019, sp.zn. Pl ÚS 45/17.

[387] Srov. např. KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6, s. 182-188.

[388] Rozsudek SDEU ze dne 21. prosince 2016, ve spojených věccech C-203/15 a C-698/15 Tele2 Sverige AB a Watson, kde SDEU odpovídal na předběžné otázky Spojeného království a Švédska ohledně výkladu čl. 15 odst. 1 *ePrivacy* směrnice, a to právě v souvislosti se zneplatněním směrnice o data retention a z toho plynoucích důsledků pro vnitrostátní právní úpravy členských států.

[389] KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6, s. 182-188.

[390] KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6, s. 182-188.

ústavní soudkyně Kateřina Šimáčková, která uzavřela, že plošné ukládání těchto údajů není odůvodněné a neexistují dostatečné koherentní záruky pro takové ukládání. Kromě jiného uvádí, že z metadat (tj. uchovávaných lokalizačních a provozních údajů) lze sestavit komplexní komunikační a sociální profil jednotlivce, včetně jeho politických názorů a sexuální orientace, tedy se může jednat o zpracování zvláštní kategorie osobních údajů, jejichž zpracování ve smyslu obecného nařízení o ochraně osobních údajů podléhá zvýšeným nárokům.

V neposlední řadě se k otázce data retention vyjádřil SDEU těsně před uzavřením této práce ve věci *Commissioner of the Garda Síochána and Others*[391]. Soudní dvůr připomněl, že uchovávání provozních a lokalizačních údajů představuje zásah do základních práv na respektování soukromého života a na ochranu osobních údajů zakotvených v článcích 7 a 8 Listiny EU. Soud zároveň v souladu s předchozí rozhodovací praxí připomněl, že ukládání těchto údajů nemá být plošné a neomezené.[392] Soud tak uzavřel, že nelze přijímat legislativní opatření, která pro účely boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti preventivně stanoví *plošné a nerozlišující uchovávání provozních a lokalizačních údajů,* a zároveň stanovil, konkrétní podmínky, za kterých lze pro účely boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti ukládání stanovit, a to vždy za předpokladu existence dostatečných záruk.[393]

Ač není mým cílem v této práci plně rozebírat veškeré otázky související s právní úpravou data retention a tuto problematiku zmiňuji především pro ilustraci problematiky dlouhodobého uchování údajů a možností jejich zneužitelnosti, na základě výše uvedeného se domnívám, že stávající zákonná úprava data retention ve smyslu § 93 odst. 4 ZEK nesplňuje podmínky vymezené SDEU – zejména tedy z důvodu plošného nijak blíže neúčelového sbírání údajů (které však, jak se

[391] Rozsudek Soudního dvora Evropské unie ze dne 5. dubna 2022 ve věci C-140/20 - Commissioner of the Garda Síochána and Others.

[392] Bod 66 rozhodnutí ve věci C-140/20 Commissioner of the Garda Síochána and Others.

[393] Bod 101 rozhodnutí ve věci C-140/20 Commissioner of the Garda Síochána and Others.

domnívají někteří odborníci,[394] nesplňovala ani dosud, ačkoliv ji Ústavní soud ve svém nálezu ve věci *Data Retention II* zhojil) a mělo by dojít k její úpravě.

Právě právo být zapomenut pak může představovat jeden z účinných nástrojů ochrany soukromí jednotlivce[395], který by se mohl domáhat ochrany svého soukromí pro nelegálnost zpracování svých osobních údajů takovým způsob. Recentní rozsudek Soudního dvora tuto oblast může navíc významně posunout, zejména pokud by mělo dojít k další úpravě této zákonné úpravy, která by se odchýlila od existujícího plošného ukládání těchto údajů.

Zneužitelnost těchto informací ze strany státu[396] i soukromých osob je přitom enormní a zájem na tom, aby tyto údaje byly vymazávány co nejdříve (nejpozději tedy po uběhnutí povinných zákonných lhůt) je enormní. V souladu se závěry SDEU by rovněž měly existovat přezkumné mechanismy týkající se stanovení vždy konkrétní povinnosti k data retention, v rámci které by se mohly subjekty údajů rovněž domáhat výmazu svých osobních údajů.

[394] Srov. KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6, s. 182-188, nebo odlišné stanovisko Kateřiny Šimáčkové k nálezu ve věci.

[395] Srov. KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6, s. 182-188.

[396] K tomu viz rovněž nález Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. Ús 24/11 (Přístup orgánů činných v trestním řízení k údajům o telekomunikačním provozu), ve kterém se ÚS zabýval otázkou zda ustanovení § 88a trestního řádu, jímž se přikazuje telekomunikačním operátorům poskytnutí informací o uskutečněném telekomunikačním provozu orgánům činným v trestním řízení, není v rozporu s ústavním pořádkem, tedy (s ohledem na zvolený způsob úpravy) zda veřejný zájem na vyšetřování trestného činu vyváží narušení telekomunikačního tajemství, a tedy ochrany osobních údajů. Ústavní soud zrušil § 88a trestního řádu pro jeho vágní požadavky na uplatnění, jež mohly svojí širokou definicí způsobit zjevnou nerovnováhu mezi právem na informační sebeurčení a veřejným zájmem odhalování trestné činnosti. Zákonodárce v tomto případě koncipoval poskytování informací od telekomunikačních poskytovatelů nikoliv jako výjimečný prostředek v boji s trestnou činností, který je svojí závažností přiměřený zásahu do ochrany soukromí, ale jako běžný prostředek, zcela bez požadavku individuálního posouzení zásahu do základního práva s ohledem na sledovaný účel.

4.2 Povaha dat a práva k datům

4.2.1 Povaha dat

4.2.1.1 Vymezení pojmu data, informace a (další) údaje

Pro vymezení možností nakládání s daty je nezbytné určit jejich právní povahu. Podle cambridgeského slovníku se data definují jako *„informace, zejména fakta nebo čísla, shromážděné za účelem prozkoumání a zvážení a použití k usnadnění rozhodování“*[397], případně pak se ve smyslu IT může jednat o *„informace v elektronickém formátu, které mohou být počítačově ukládány a zpracovávány“*[398]. Informací se pak rozumí „novinky, fakta nebo znalost.“[399]

S odvoláním na vymezení informace rakouským fyzikem Erwinem Schröndingerem[400] Polčák vysvětluje, že informace netvoří objekt práva, nemůže být objektivizována a nemůže být předmětem právních vztahů, jelikož zároveň nemá žádnou relevantní statickou existenci.[401] Podle Polčáka je přitom zcela zásadní diferenciace mezi informací a daty, kdy připomíná, že ačkoliv se právo snaží s informací pracovat jako se statkem či sekundárním objektem právních vztahů, toto uchopení jde proti přírodním zákonům. Zároveň upozorňuje na paradox, kdy právo ve snaze regulovat informace, využívá nastavení práv k efektům užití dat, což demonstruje na ochraně informačního soukromí, kde informační efekt má zpravidla charakter materiální teleologie konkrétních pravidel regulujících nikoliv informaci, ale užití dat. Polčák uzavírá, že informaci

[397] *„Information, especially facts or numbers, collected to be examined and considered and used to help with making decisions“* in CAMBRIDGE DICTIONARY. Data. [online]. [cit. 2022-04-03]. Dostupné z https://dictionary.cambridge.org/dictionary/english/data.

[398] *„Information in an electronic form that can be stored and processed by a computer*“ in CAMBRIDGE DICTIONARY. Data. [online]. [cit. 2022-04-03]. Dostupné z https://dictionary.cambridge.org/dictionary/english/data.

[399] *„News, facts, or knowledge“* in CAMBRIDGE DICTIONARY. Information. [online]. [cit. 2022-04-03]. Dostupné z https://dictionary.cambridge.org/dictionary/english/information

[400] SCHRÖNDINGER, Erwin. What is life. Cambridge University Press, 1944. ISBN 0-521-42708-8.

[401] POLČÁK, Radim. Getting European data protection off the Ground. International Data Privacy Law [online]. 2014, (Volume 4, 4,), 282–289 [cit. 2022-04-03]. ISSN 2044-4001. Dostupné z: https://academic.oup.com/idpl/article-abstract/4/4/282/2569059.

lze tedy pro potřeby práva vnímat jako *„konkrétně aktualizovanou organizaci, která je důsledkem spojení dat, okolností jejich výskytu a času.“*[402]

Právo tak podle Polčáka naráží na zásadní problém při snaze pojetí dat (zde konkrétně osobních údajů – v angličtině tedy *„personal data“*) jako statickou veličinu podobnou věci, kterou lze právně regulovat a nakládat. Ačkoliv podle něj takové pojetí může popírat smysl ochrany soukromí a jedince, kde by bylo vhodnější zaměřit se na ochranu jedince a jeho sociální potřeby[403], v zásadě připouští, že právo s daty pracuje jako s veličinou, ke které lze nabývat práva.

Data samozřejmě existují i mimo technologický svět, nicméně jejich význam a množství se exponenciálně zvyšuje právě ve spojitosti s využíváním nových technologií a kybernetického prostoru: „*Počítače nejen zvýšily objem informací, které společnosti sbírají – zároveň zcela mění způsob, jakým mohou být data organizována, zpřístupněna či prohledávána“*.[404]

Data tak budou mít vždy velmi specifikou povahu nejen z hlediska toho, že se může jednat o nekonečně-mnohonásobné zachycení stejné informace, ale zejména v kybernetickém prostoru bude data vždy možné (při nejmenším z technologického hlediska) nekonečně mnohokrát duplikovat, kopírovat a vytvářet tak nová data nesoucí stejný set informací. Tento konflikt zároveň vytváří různé překážky spočívající ve spojení různých datasetů, které vytvářejí propojený celek. Toto propojení může být relevantní zejména ve spojení s ochranou osobních údajů, kde značné množství individuí může být propojeno jedním setem dat, což vytváří „hyper-propojené“ prostředí a značně narušuje nejen práva jednotlivých data subjektů, ale rovněž faktickou kontrolu nad jejich

[402] POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

[403] POLČÁK, Radim. Getting European data protection off the Ground. International Data Privacy Law [online]. 2014, (Volume 4, 4,), 282–289 [cit. 2022-04-03]. ISSN 2044-4001. Dostupné z: https://academic.oup.com/idpl/article-abstract/4/4/282/2569059.

[404] SCHWARTZ, Paul M. and SOLOVE, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information (December 5, 2011). New York University Law Review, Vol. 86, p. 1814, 2011, UC Berkeley Public Law Research Paper No. 1909366, GWU Legal Studies Research Paper No. 584, GWU Law School Public Law Research Paper No. 584. [online]. [cit. 2022-04-03]. Dostupné z: https://ssrn.com/abstract=1909366.

daty a možnosti výkonu práv k takovým datům, jelikož data konkrétního jedince mohou být vždy spojena s daty jiných jedinců.[405]

4.2.1.2 Informace, data a (další) údaje v českém právním řádu

Český právní řád (významně ovlivňovaný a doplněný evropskými předpisy – ať již přímo aplikovatelnými nebo dále transponovaný do lokálních právních předpisů) přitom pracuje s jednotlivými pojmy (data, informace nebo případně údaje) poměrně promiskuitně jejich vymezení je poměrně sporadické a často účelové pro potřeby konkrétního právního předpisu nebo institutu. Např. informací se pro účely zákona o přístupu k informacím rozumí *„jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“*[406]

Právní předpisy dále vždy pro potřeby konkrétních institutů vymezují konkrétní podmnožinu specificky vymezených dat, jako jsou osobní údaje[407] (z anglického *„personal data“* nebo německého *„personenbezogene Daten“*) nebo pak provozní údaje[408] (angl. *„traffic data“* nebo něm. *„Verkehrsdaten“*[409]) či lokalizační údaje[410] (angl. *„location data“* nebo něm. *„Standortdaten“*[411]).

---

[405] K tomu obdobně např. LI, Wenlong. a tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation. International Data Privacy Law [online]. 2018, 2. července 2018, (Volume 8, 4,), 309-317 [cit. 2022-04-03]. ISSN 2044-4001. Dostupné z: https://academic.oup.com/idpl/article/8/4/309/5047861?login=true#no-access-message#no-access-message.

[406] Srov. § 3 odst. 3 zákona o svobodném přístupu k informacím; odst. 4 stejného ustanovení pak dále negativně stanoví, že *„informací podle tohoto zákona není počítačový program“*.

[407] Srov. kapitolu 3.1.1 výše. Osobní údaje jsou tedy vymezeny jako „*veškeré informace o […]“*.

[408] Podle § 90 odst. 1 zákona o elektronických komunikacích se provozní údaji rozumí *„jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.“*

[409] Srov. čl. 2 písm. b) *ePrivacy* směrnice, který vymezuje provozní údaje a která je dále implementována v českém právním řádu v podobě zákona o elektronických komunikacích.

[410] Podle § 91 odst. 1 zákona o elektronických komunikacích se lokalizačními údaji rozumí *„jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“*

[411] Srov. čl. 2 písm. c) *ePrivacy* směrnice, který vymezuje lokalizační údaje.

Vymezení informace by přitom přicházelo v úvahu již pro realizaci samotného práva na svobodný přístup k informacím ve smyslu čl. 17 LZPS. Povahou informací se doktrinální ani judikaturní praxe příliš nezabývá a v zásadě za informaci je považován jakýkoliv obsah určitého sdělení[412]. Abstraktní povaha informace často vede ke vztahování výkonu konkrétních práv k nosiči informací[413] či technické způsoby realizace šíření či přijímání informací či sdělování názorů[414].

Pojem „data" není blíže specifikován, ačkoliv se objevuje napříč právním řádem. Namátkou lze uvést např. povinnosti vyplývající ze zákona o kybernetické bezpečnosti, který pro účely vymezení povinností mezi správci a provozovateli informačních systémů odkazuje na „data, provozní údaje a informace"[415], na což navazuje vyhláška o kybernetické bezpečnosti (jakožto prováděcí předpis tohoto zákona), která však většinově práva a povinnosti vztahuje pouze k „datům"[416]. O „datech" hovoří rovněž zákon o zdravotních službách, který ale zároveň některé povinnosti pro vedení zdravotnické dokumentace odkazuje na „kopie datových souborů" nebo pak „technické nosiče dat".[417] S pojmem „data" pak poměrně nesystematicky nakládají i další veřejnoprávní předpisy[418].

Trestněprávní předpisy pak s pojmem „data" pracují zejména v souvislosti s kyberkriminalitou a implementují tak do značné míry Úmluvu o kybernetické kriminalitě[419], která vymezuje pojem „počítačová data", a to jako *„jakékoli*

[412] Obdobně např. BARTOŇ, HEJČ in HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2, s. 26.

[413] Srov. např. nález Ústavní soud ze dne 28. září 2005, sp. zn. I. ÚS 394/04, nebo nález Ústavního soudu ze dne 11. září 2012, sp. zn. II. ÚS 1375/11.

[414] Srov. rozhodnutí ESLP ze dne 28. září 1990 ve věci 10890/84 - Groppera Radio AG a další proti Švýcarsku, či rozhodnutí ESLP ze dne 22. května 1990 ve věci 12726/87 - Autronic AG proti Švýcarsku.

[415] Srov. zejména § 6a a § 15a zákona o kybertnetické bezpečnosti.

[416] Srov. např. úprava likvidace dat ve smyslu § 1 písm. g) a přílohy č. 4 vyhlášky o kybernetické bezpečnosti

[417] Srov. např. § 55 zákona č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů.

[418] Srov. např. § 5 zákona č. 269/2021 Sb., o občanských průkazech, nebo § 121 zákona č. 361/2000 Sb., o silničním provozu.

[419] Sdělení č. 104/2013 Sb. m. s., Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě.

vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem"[420]. Trestní zákoník pak vymezuje v zásadě pět trestných činů, které se mohou týkat dat či informací: (i) neoprávněný přístup k počítačovému systému a nosiči informací[421], (ii) opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat[422], (iii) poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti[423], případně pak ještě (iv) porušení tajemství dopravovaných zpráv[424] a (v) porušení tajemství listin a jiných dokumentů uchovávaných v soukromí[425].[426]

Trestní řád pak rovněž pracuje s pojmem data pro institut tzv. „zmrazení dat". S účinností od 1. února 2019 podle § 7b trestního řádu mohou orgány činné v trestním řízení požadovat tzv. „zmrazení dat", kdy lze uložit jakékoli osobě, aby po stanovenou dobu (nejvýše 90 dní) uchovala v nezměněné podobě vymezená data, která jsou uložena v počítačovém systému nebo na nosiči informací, a aby zároveň znemožnila přístup k těmto datům a nezpřístupnila informaci o skutečnosti, že jí bylo takové uchování dat nařízeno.[427]

Na základě výše uvedeného lze uzavřít, že právní úprava informací, dat či jiných údajů není v českém právním řádu koherentní a ani jeden z těchto pojmů není pevně vymezen. Jedním z možných závěrů je, že data jsou v zásadě materializovaný projev informace, kde informace znamená obsah nebo část obsahu. Toto pojetí je přitom poměrně zjevné ve spojení s kybernetickým

[420] Srov. čl. 1 písm. b) Úmluvy o kybernetické bezpečnosti.

[421] Srov. § 230 trestního zákoníku.

[422] Srov. § 231 trestního zákoníku.

[423] Srov. § 232 trestního zákoníku.

[424] Srov. § 182 trestního zákoníku.

[425] Srov. § 183 trestního zákoníku

[426] K tomu srov. např. GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kol. Trestní zákoník. 2. vydání. Praha: C. H. Beck, 2012, s. 2303, marg. č. 1

[427] VÍTEK, Dominik, SUCHÁNKOVÁ, Lenka. Advokátní tajemství v cloudu. Bulletin advokacie, 2020, č. 12, s. 19-22.

prostorem, ve kterém se obvykle s daty nakládá. Data jsou tedy v zásadě materiální zhmotnění informace. Fenomén dat je pak spojen především s novými technologiemi a internetem, u kterých zákonodárce rovněž postupně projevuje další snahy tyto oblasti blíže regulovat (srov. zejména regulace osobních údajů nebo regulace v podobě *ePrivacy* směrnice).

Toto vymezení dat může částečně narušovat vymezení informace ve smyslu zákona o svobodném přístupu k informacím, která informaci vztahuje jen na takový obsah, který je hmotně zachycen (na jakémkoliv nosiči). Tím se informace cyklicky přibližuje k datům, se kterými právo primárně pracuje jako materializovaným projevem informací či obsahu.

Polčák v této souvislosti dokonce uzavírá, že, přinejmenším odvětví ochrany osobních údajů, *„trpí systematickým lapsem spočívajícím ve ztotožnění ‚dat' a ‚informací'."*[428]

Pojem data je v českém právním prostředí používán v zásadě synonymně s pojmem „údaje" (a do značné míry rovněž zaměnitelně s pojmem informace), což se projevuje zejména v oblasti úpravy osobních údajů, lokalizačních údajů či provozních údajů, které jsou přitom v jiných jazykových mutacích (zejména angličtině či němčině) označovány jako „data". Pokud tedy český právní řád (a obdobně tato práce) referuje na data, informace či údaje, tyto pojmy jsou užívány v zásadě zcela zaměnitelně, pokud není výslovně – zpravidla pro účely konkrétního právního předpisu – určeno výslovně jinak.

4.2.2 Data jako věc v právním smyslu

Jak bylo uzavřeno výše, povaha dat (a informací) není (přinejmenším) v českém ani evropském právu zcela vyjasněna. S tím souvisí rovněž možnosti vymezení práv, které k datům lze nabývat. Podle Polčáka platí, že informace není věcí a nelze ji za věc považovat, a tudíž k ní nelze nabývat jakákoliv absolutní práva[429] a poukazuje na nesprávnost pojetí informace (zaměňované s daty), resp. výsledků

[428] POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

[429] POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

myšlenkových činností, ke kterému dochází např. Telec[430]. Naopak však připouští, že povahu věci, a tím pádem rovněž možnost vazby na absolutní práva, by mohla mít data, resp. tedy že charakter mají až na výjimky práva nikoli k datům, ale k různým souvislostem jejich existence, typicky k formě a důsledku jejich užití.[431]

Podle občanského zákoníku se věcí v právním smyslu rozumí vše, co je rozdílné od osoby a slouží potřebě lidí.[432] Má-li tedy jít o věc v právním slova smyslu, musí být splněny kumulativně dvě podmínky: (i) musí jít o něco, co je odlišné od člověka či právnické osoby a (ii) musí se jednat o něco, co slouží potřebě lidí.[433] Aby se přitom jednalo o věc, musí se jednat (iii) o ovladatelnou veličinu.[434] Věcí nemohou být předměty, které nemohou uspokojovat potřeby lidí, protože je nelze objektivně ovládat (např. objekty mimo dosah člověka – kosmická tělesa – nebo neovladatelné přírodní síly). Tyto předměty se mohou proměnit ve věc v právním smyslu v momentě, kdy je člověk schopen je ovládat.[435] Občanský zákoník pak jako věc rozlišuje např. rovněž obchodní tajemství ve smyslu § 504 o.z.[436]

Pojetí věci je tak v českém právním řádu velmi široké. Pokud bychom připustili e premisu toho, že data jsou skutečně věcí ve smyslu § 489 o.z., je nezbytné se rovněž vypořádat s otázkou, jaká práva lze k datům nabýt – zejména, zda je možné k nim nabýt absolutní majetková práva. Např. Telec přitom dovozuje, že

[430] TELEC, Ivo. Není informace jako informace. Právní rozhledy. 2014, (15-16/2014), 515. ISSN 1210-6410 nebo TELEC, Ivo. Držba informací. Právní rozhledy. 2014, (4/2014), 115. ISSN 1210-6410.

[431] POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

[432] Srov. § 489 o.z.

[433] KINDL, DAVID in ŠVESTKA, Jiří, Jan DVOŘÁK, Irena PELIKÁNOVÁ, et al. ČESKO. Občanský zákoník: komentář. Svazek I. Praha: Wolters Kluwer ČR, 2013, s 1736. ISBN 978-80-7478-369-2, s. 1158.

[434] HUBKOVÁ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 521.

[435] HUBKOVÁ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 521.

[436] HUBKOVÁ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 537.

mohou existovat věci, ke kterým však nelze nabýt majetková práva, mezi které řadí rovněž osobní údaje[437], obdobně pak uzavírá Hubková.[438]

Německá doktrína pak dospívá k názoru, že data nemohou být věcí ve smyslu § 90 německého občanského zákoníku (BGB)[439], jelikož aby naplňovala definici věci, musí se jednat o předmět, který je smyslově vnímatelný, ovladatelný a ohraničený. Data tyto vlastnosti postrádají, protože nejsou bezprostředně vnímatelná, nelze je pro svou všudypřítomnost ovládat jako fyzické předměty a postrádají prostorovou vymezitelnost. Z těchto důvodů jsou data v německé pojetí považována za tzv. nehmotný statek (*immaterielles Gut*), který má tedy kvality být předmětem práva.[440] Toto pojetí však vyplývá z odlišného, a mnohem užšího pojetí věci v německém právu, kde se věcí ve smyslu § 90 BGB rozumí vždy korporální (fyzický) předmět (*körperliche Gegenstände*), vedle kterého stojí nehmotné statky.

Povahu věci také mohla pomoci objasnit zahraniční rozhodovací praxe, jak někteří autoři[441] předvídali např. v případě Microsoft Corp. v. United Sates[442], kterým se zabýval Nejvyšší soud USA (Supreme Court of the United States). Nicméně vzhledem k tomu, že americký kongres v mezičase přijal tzv. CLOUD Act[443], tato otázka zůstala nezodpovězená.

---

[437] Podle Telce se může jednat o tzv. „ideální předměty“, jako jsou různé obchodní značky, zákaznické základny (klientely) nebo know-how či denní zprávy anebo jiné tzv. prosté (pouhé) informace (i tzv. prosté či holé nápady hospodářského významu), některé osobní údaje, vědecké objevy či statistické grafy, výpočty aj. výzkumné údaje (vědecké aj. poznatky) apod. věcné údaje samy o sobě, které lze právním jednáním (tudíž i ocenitelně) převést na jiného a které zároveň připouštějí trvalé nebo opakované „použití“ či „využití“ in TELEC, Ivo. Držba informací. Právní rozhledy. 2014, (4/2014), 115. ISSN 1210-6410.

[438] HUBKOVÁ in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 529.

[439] Ustanovení § 90 Bürgerliches Gesetzbuch (BGB). Dostupné z https://www.gesetze-im-internet.de/bgb/__90.html.

[440] WIEBE, SCHUR in BRÄUTIGAM, Peter a Torsten KRAUL. Internet of Things. München: Verlag C.H. Beck oHG, 2021. ISBN 978-3-406-74898-1, s. 160.

[441] Srov. např. VÁLOVÁ, Irena. Klíčový spor o „vlastnictví“ dat v cloudu. USA vs. Microsoft a zbytek světa. [online]. 18.5.2016. [cit. 2022-04-03]. Dostupné z https://ekonomickydenik.cz/klicovy-spor-o-vlastnictvi-dat-v-cloudu-microsoft-vs-usa-a-zbytek-sveta/.

[442] Rozhodnutí Nejvyššího soudu USA ze dne 4. července 2018, ve věci United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018). Dostupné z https://casetext.com/case/united-states-v-microsoft-corp-9.

[443] H.R.4943 - CLOUD Act. Dostupné z https://www.congress.gov/bill/115th-congress/house-bill/4943.

Vzhledem k velmi široké definici věci v českém právním řádu, a i s přihlédnutím k německé doktríně, se domnívám, že data mají povahu věci ve smyslu § 489 o.z, a to sice jako nehmotná movitá věc.

Pojetí práv jako věci přitom otevírá značné množství otázek zejména z hlediska povahy a rozsahu práv, které lze k datům nabývat, případně zda tato práva mohou být omezená, a měly by být předmětem dalšího zkoumání; nicméně tyto otázky značně přesahují cíl této práce.[444] Právo nemá jednoznačnou odpověď na to, zda data mohou být např. předmětem vlastnictví.[445] Přesto se domnívám, že i k datům, jelikož se jedná o věci, lze nabývat vlastnická práva – věcí v právním smyslu by totiž mělo být v zásadě jen to, čeho se mohou týkat subjektivní majetková práva[446]. Pokud tedy připustíme, že data mohou být věcí, je nezbytné připustit i to, že k nim lze nabývat práva – pokud se uplatní závěry o možné omezitelnosti faktického rozsahu práv k takovým nehmotným statkům, jak dovozuje Telec, s velkou mírou pravděpodobnosti lze tyto závěry vztáhnout i na data. Podle Polčáka nelze ve vztahu k datům hovořit o vlastnickém právu, jelikož vlastník věci standardně disponuje pěti typy absolutních práv (právem věc držet, užívat, požívat, disponovat s ní nebo ji zničit). Vzhledem k tomu, že data budou zpravidla nehmotnou věcí, do které přímo zasahují další instituty (zejména právo na ochranu soukromí, duševní vlastnictví aj.) lze však dovozovat pouze právo na užití dat[447]. Pro data navíc platí, že jsou neomezitelně replikovatelná (ač obvykle zachycená na hmotném nosiči), a vlastnické právo by tak bylo s velkou mírou pravděpodobnosti jen těžko prokazatelné, natož pak vymahatelné. Pro výkon práva k užívání dat se tak zdá být jako vhodným institutem k nakládání s právy k

[444] Pro účely vymezení právní povahy dat přitom záměrně opomíjím další právní instituty, které mohou povahu dat ovlivňovat a dopadat na ně, jako je především *sui generis* ochrana databází, popř. rovněž autorskoprávní ochrana pro případy, že by data obsahovala, nebo formovala, dílo ve smyslu autorskoprávních předpisů.

[445] BLUME Peter, The inherent contradictions in data protection law, International Data Privacy Law, Volume 2, Issue 1, February 2012, Pages 26–34. [online]. [cit. 2022-04-03]. Dostupné z https://doi.org/10.1093/idpl/ipr020.

[446] Srov. KINDL in ŠVESTKA, Jiří, Jan DVOŘÁK, Irena PELIKÁNOVÁ, et al. ČESKO. Občanský zákoník: komentář. Svazek I. Praha: Wolters Kluwer ČR, 2013, s 1736. ISBN 978-80-7478-369-2, s. 1173.

[447] POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

datům licenční smlouva[448]. Pro každý set údajů bude rovněž nezbytné určit oprávněnou osobu (ať už by se jednalo o vlastníka, pokud připustíme, že existují vlastnická práva, či jinou oprávněnou osobu, která může s daty nakládat, a tedy k nim poskytovat další oprávnění).

Do této úpravy pak významně zasahuje oblast ochrany osobních údajů, která je však zejména pro oblast práva být zapomenut zcela zásadní. Pro vlastnictví osobních údajů např. Blume dovozuje, že subjekty údajů jsou vlastníky svých vlastních osobních údajů, což by znamenalo, že osobní údaje jsou komodita, se kterou lze nakládat jako s věcí; tento závěr dovozuje z podstaty souhlasu se zpracováním osobních údajů, který dává subjektům údajů exkluzivní kontrolu nad jejich osobními údaji. Správce osobních údajů pak dostává od subjektu údajů oprávnění s jeho osobními daty nakládat.[449] Např. Rees pak na obdobných základech dovozuje myšlenku, že se jedná přímo o vlastnický model.[450] Rovněž v české doktrinální praxi např. Nonnemann zvažuje, zda je možné osobní údaje využívat jako určitou formu platidla[451], a tedy s nimi nakládat jako s plně vlastnitelnou věcí.

Vzhledem k tomu, že právo být zapomenut se bude obvykle do velké míry překrývat s ochranou osobních údajů, je relevantnost této otázky omezená. Držitelem (popř. vlastníkem) osobních údajů bude subjekt údajů, který se v mezích čl. 17 GDPR bude domáhat svého práva být zapomenut, a tedy zároveň tak vykonávat práva k jím vlastněné věci. Relevance nicméně může vzrůstat u dalšího užívání takových údajů (včetně např. dalšího užívání zveřejněných osobních údajů, jak je blíže rozebráno v kapitole 4.3), kde se v případě zásahu do

[448] Licenci lze např. udělit k know-how (srov. Nejvyšší soud ze dne xxx ve věci NS 32 Cdo 1185/2012) nebo obchodnímu tajemství. Srov. např. VÝTISK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2373.

[449] BLUME Peter, The inherent contradictions in data protection law, International Data Privacy Law, Volume 2, Issue 1, February 2012, Pages 26–34. [online]. [cit. 2022-04-03]. Dostupné z https://doi.org/10.1093/idpl/ipr020.

[450] REES Christopher, Tomorrow's privacy: personal information as property, International Data Privacy Law, Volume 3, Issue 4, November 2013, Pages 220–221. [online]. [cit. 2022-04-03]. Dostupné z https://doi.org/10.1093/idpl/ipt022.

[451] NONNEMANN, František. Osobní údaje jako platidlo?. Právní rozhledy, 2020, č. 5, s. 174-180.

soukromí může rovněž jednat o zásah do majetkových práv. Takové vymezení může mít zásadní dopady rovněž z hlediska komercializace dat a vytváření např. derivovaných dat na základě něčího vlastnictví; subjektům údajů by v takovém případě mohla náležet spravedlivá odměna, jelikož dochází k obohacování se na úkor, resp. za využití, jejich věci.

Obdobné závěry se uplatní i ve vztahu k jiným datům, než jsou osobní údaje (zejména tedy v oblastech spadajících mimo oblast obecného nařízení o ochraně osobních údajů). Vůči těmto datům by vlastnictví (resp. jiná majetková práva) nemělo být *an sich* překážkou uplatnitelnosti práva být zapomenut. Právo být zapomenut je totiž přirozené právo, které je součástí ochrany osobnosti, resp. ochrany soukromí osob. Pokud by právo být zapomenut mělo zasahovat do majetkových (či dokonce vlastnických) práv jiné osoby, bude nezbytné na základě testu proporcionality vyhodnotit, zda v takovém případě převáží právo na ochranu soukromí dané osoby, nebo ochrana těchto majetkových práv.

Jako poznámku na konec si dovolím rovněž připomenout, že data (ať již v elektronickém světě nebo v papírovém pojetí) budou standardně zachycena na datovém nosiči a s tímto datovým nosičem mohou být rovněž neoddělitelně spojena. Takový datový nosič však bude sám o sobě věcí, ke kterému lze nabývat práva. Jak však rovněž dovozuje německá doktrína, platí, že vlastnictví datového nosiče nevede automaticky k autorizaci pro data na něm uložená; naopak oba soubory otázek je třeba rozlišovat i přes určité dopady vlastnictví majetku na sběr dat.[452] Naopak takový závěr by vedl k absurdním závěrům a zcela popíral způsob fungování moderních technologií, včetně např. technologií cloud computingu, kde by bylo nezbytné dovozovat, že vlastník datového nosiče (zde tedy např. serverů uložených v datovém centru) je zároveň vlastníkem dat zde ukládaných. Takové pojetí by zcela znemožnilo využívání obdobných technologií, jelikož nejenže by nereflektovala ekonomickou a technologickou realitu, ale rovněž by jednoznačně odrazovalo všechny potenciální uživatele cloudu od jeho užívání.

[452] WIEBE, SCHUR in BRÄUTIGAM, Peter a Torsten KRAUL. Internet of Things. München: Verlag C.H. Beck oHG, 2021. ISBN 978-3-406-74898-1, s. 160.

4.3 Využívání zveřejněných osobních údajů[453]

4.3.1 Možnosti dalšího využívání zveřejněných osobních údajů

Využívání zveřejněných osobních údajů je, zejména v online prostředí, nedílnou součástí každodenní činnosti, včetně např. dohledání a využívání kontaktních údajů poskytnutých na internetových stránkách společností. Kromě těchto každodenních činností se může zároveň jednat o plošné využívání zveřejněných osobních údajů – včetně např. veřejných katalogů firem nebo společností provádějících datovou analytiku sociálních sítí či jiných big data činností. Toto využívání může mít zároveň významný dopad na digitální stopu jednotlivce a jeho potenciální uplatňování práva být zapomenut.

Obecné nařízení o ochraně osobních údajů, na rozdíl od předchozího zákona č. 101/2000[454], neobsahuje výslovný právní základ pro zpracování oprávněně zveřejněných údajů. V případě, kdy má dojít k dalšímu využití takových zveřejněných osobních údajů, je nezbytné identifikovat nový právní základ (ve smyslu čl. 6 odst. 1 GDPR) pro takové zpracování osobních údajů. Zároveň platí, že možnost využít zveřejněné zvláštní kategorie osobních údajů je (poněkud nesystematicky) výslovně zakotvena v čl. 9 odst. 2 GDPR.

Nicméně na základě níže uvedeného rozboru lze uzavřít, že při splnění podmínek obecného nařízení o ochraně osobních údajů (zejména tedy aplikaci vhodného právního základu – zpravidla opravného zájmu, provedení balančního testu ve smyslu čl. 6 odst. 4 GDPR a splnění informační povinnosti ve smyslu čl. 14 GDPR) lze zveřejněné osobní údaje zpracovávat.[455]

Na základě systematického výkladu a na základě níže uvedeného rozboru (v kapitole 4.3.2) lze předpokládat, že zpracování zvláštních kategorií osobních údajů je i při splnění podmínek čl. 9 odst. 2 GDPR vždy třeba podřadit pod

[453] Části textu v této kapitole byly publikovány jako VÍTEK, Dominik a Jana PATTYNOVÁ. Využívání zveřejněných osobních údajů [online]. 14.6.2019 [cit. 2022-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/vyuzivani-zverejnenych-osobnich-udaju-109518.html.

[454] Ustanovení § 5 odst. 2 písm. d) zákona č. 101/2000.

[455] Obdobně pak rovněž NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. Právní rozhledy. 2018(5). ISSN 1210-6410.

některý důvod zpracování dle čl. 6 odst. 1 GDPR – ve většině případů na základě oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR (v případě zvláštních kategorií údajů pouze těch zveřejněných přímo subjektem údajů v souladu s čl. 9 odst. 2 písm. e) GDPR). V této věci lze také částečně vycházet ze závěrů českého Úřadu pro ochranu osobních údajů, který se v rámci své činnosti dospěl k závěru, že *„dané zpracování lze v této formě založit na právním titulu upraveném v čl. 6 odst. 1 písm. f) [GDPR], neboť kontrolovaná osoba má oprávněný zájem na dalším zveřejnění osobních údajů podnikatelů získaných z veřejných rejstříků (v podobě zajištění ekonomické stránky své podnikatelské činnosti).“*[456]

Jakékoliv zpracování na základě oprávněného zájmu je třeba posoudit tzv. balančním testem ve smyslu čl. 6 odst. 4 GDPR (k tomu viz kapitola 4.3.3). Zpracování bude zákonné, pokud nad oprávněným zájmem správce zpracovávat zveřejněný osobní údaj nepřeváží základní práva a svobody subjektů údajů vyžadující jeho soukromí. Základním kritériem posouzení by mělo být zejména očekávání subjektů ohledně zpracování těchto údajů a kompatibilita účelu, za nímž byly údaje primárně zveřejněny.

Zpracování osobních údajů na základě oprávněného zájmu přitom rovněž přináší zásadní limity – zejména má každý subjekt údajů právo vznášet námitky proti zpracování jeho osobních údajů. Pokud budou takové námitky odůvodněné, správce bude povinen takové osobní údaje vymazat, jelikož nadále nebude disponovat adekvátním právním základem takového zpracování (k tomu viz kapitola 6.2.4.3).

Další omezení vznikají z hlediska potenciálního následného užívání dalšími správci, kteří by museli rovněž nalézt nový vhodný právní titul (pravděpodobně rovněž oprávněný zájem, jehož slučitelnost s původním účelem může být však jen významně omezená, a zároveň pro nového správce rovněž obtížně ověřitelná). Zcela samostatnou otázkou (kterou se tento text nezabývá) je pak plnění informační povinnosti vůči subjektům údajů, jejichž zveřejněné osobní údaje se

[456] K tomu srov. Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452.

správce chystá využívat. Správce by tak měl vždy v souladu s čl. 14 GDPR zajistit, že subjekty údajů budou informováni o takovém zpracování osobních údajů.[457]

4.3.2 Právní základ zpracování zveřejněných údajů – vztah mezi čl. 6 a čl. 9 GDPR

4.3.2.1 Vymezení vztahu čl. 6 a 9 GDPR

Zpracování zveřejněných údajů se výslovně připouští v čl. 9 odst. 2 písm. e) GDPR ve vztahu ke zvláštním kategoriím údajů.[458] Obdobný důvod zpracování však není uveden mezi obecnými důvody zpracování podle čl. 6 odst. 1 GDPR. Z tohoto důvodu je nezbytné analyzovat vztah mezi čl. 6 odst. 1 GDPR a čl. 9 odst. 2 GDPR a z této analýzy dovodit závěr pro možnost zpracování zveřejněných osobních údajů nad rámec zvláštních kategorií údajů.

Obecně platí, že právní základy zpracování dle čl. 6 odst. 1 by měly pokrývat veškeré zpracování osobních údajů, přičemž zpracování zvláštních kategorií údajů je dle čl. 9 odst. 1 GDPR zakázáno. Ustanovení čl. 9 odst. 2 upravuje výjimky ze zákazu zpracování zvláštních kategorií osobních údajů. Z této legislativní konstrukce dovozujeme, že výjimky ze zákazu zpracování zvláštních kategorií údajů dle čl. 9 odst. 2 GDPR jsou pouze podmnožinou důvodů zpracování podle čl. 6 odst. 1 GDPR, nikoliv výslovně samostatnými právními důvody. Ve vztahu těchto ustanovení lze dovodit tři následující principy:

---

[457] Např. Rozhodnutí Úřadu pro ochranu osobních údajů, ve věci Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452. Úřad pro ochranu osobních údajů v této věci dospěl k závěru, že informační povinnost (bez uvedení dalších detailů) byla splněna dostatečně.

Obdobným případem (využívání zveřejněných údajů z polské obdoby obchodního a živnostenského rejstříku) se zabýval i polský dozorový orgán (více informací je rovněž dostupných zde https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_en), který v konkrétní skutkové podstatě dospěl k závěru, že správce nedostatečně informoval subjekty údajů – správce totiž při využívání zveřejněných údajů zaslal informační email o zpracování těchto osobních údajů pouze subjektů, jejichž emailové adresy byly v těchto zdrojích uvedeny; ostatní subjekty neinformoval, a tudíž nesplnil povinnosti dle čl. 14 GDPR.

[458] Podle článku 9 odst. 1 GDPR se zakazuje zpracování zde vypočtených zvláštních kategorií osobních údajů. Čl. 9 odst. 2 písm. e) pak stanoví, že ustanovení čl. 9 odst. 1 nepoužije, pokud se zpracování těchto zvláštních kategorií týká osobních údajů zjevně zveřejněných subjektem údajů.

4.3.2.2 Restriktivní požadavky na zpracování zvláštních kategorií údajů

Tam, kde jsou důvody zpracování dle čl. 9 odst. 2 GDPR konkrétní podmnožinou důvodů zpracování dle čl. 6 odst. 1 GDPR, je výklad zjevný – všechny osobní údaje je možné zpracovávat na základě důvodů v čl. 6 odst. 1 GDPR a pro zpracování zvláštních kategorií údajů dle čl. 9 odst. 2 GDPR platí restriktivnější podmínky (je nezbytné naplnit podmínky výjimky z obecného zákazu jejich zpracování). Tak je tomu např. u zpracování ve veřejném zájmu, kdy čl. 6 odst. 1 písm. e) umožňuje zpracování osobních údajů ve veřejném zájmu a čl. 9 odst. 2 písm. g) umožňuje zpracování zvláštních kategorií údajů pouze ve „významném" veřejném zájmu, a to s dodatečným testem přiměřenosti a povinností vhodných záruk. Podobně je tomu i se zpracováním na základě souhlasu, kdy čl. 9 odst. 2 písm. a) stanoví nad rámec obecných požadavků na souhlas dle čl. 6 odst. 1 písm. a) pro souhlas se zpracováním zvláštních kategorií údajů i požadavek na výslovný souhlas pro konkrétní účel a dále také možnost členského státu některé údaje z režimu souhlasu vyloučit. Stejný princip se vztahuje i na zpracování nezbytné pro ochranu životně důležitých zájmů, kdy čl. 9 odst. 2 písm. c) GDPR stanoví nad rámec zpracování dle čl. 6 odst. 1 písm. d) GDPR pro zvláštní kategorie údajů podmínku, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas.

Tento princip se dále vztahuje i na zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje, kdy dle čl. 6 odst. 1 písm. c) může správce zpracovávat běžné (tj. nikoliv zvláštní kategorii) osobní údaje pro splnění libovolné právní povinnosti, ale zpracování zvláštních kategorií údajů je přípustné pouze pro některé typy právních povinností v rámci článku 9 odst. 2 písm. b), h), i) a j) GDPR. Lze předpokládat, že právní řád nemůže správce stavět do situace, kdy by měl pro splnění právní povinnosti zpracovávat zvláštní kategorie údajů a zároveň se tím dopouštěl nezákonného zpracování dle GDPR. Tato konstrukce tak nepřímo klade požadavky na zákonodárce, aby nestanovoval zákonné povinnosti vyžadující zpracování zvláštních kategorií údajů, které nespadají do kategorií předvídaných v čl. 9 odst. 2 GDPR.[459]

[459] Tím není dotčena možnost zákonodárce stanovit další podmínky pro zpracování genetických a biometrických údajů či údajů o zdravotním stavu ve smyslu čl. 9 odst. 4 GDPR.

V této souvislosti je třeba uvést, že v souladu se stanoviskem Pracovní skupiny WP 29 č. 6/2014[460] je nutno právní povinnost vykládat restriktivně. Právním podkladem plnění právní povinnosti tak bude pouze takové ustanovení právního předpisu, které správci nedává možnost svobodně rozhodnout. Jestliže je zákonem či jiným právním předpisem dána možnost, o jejímž využití správce rozhoduje svobodně, relevantní zvláštní právní titul dle článku 9 odst. 2 již nebude možné kombinovat s právním titulem plnění právní povinnosti, ale s právním titulem oprávněného zájmu správce či třetí strany dle článku 6 odst. 1 písm. f) GDPR.

4.3.2.3 Některé důvody zpracování běžných údajů jsou pro zvláštní kategorie údajů nepřípustné

Některé důvody zpracování jsou výslovně uvedené v čl. 6 odst. 1 GDPR pro všechny osobní údaje, avšak již je nelze bez dalšího využít jako výjimku zpracování zvláštních kategorií osobních údajů ve smyslu čl. 9 odst. 2 GDPR.

Takový závěr by se vztahoval např. na zpracování nezbytné pro plnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR, které dle čl. 9 odst. 2 GDPR není přípustné pro zvláštní kategorie údajů s výjimkou plnění povinností v oblasti pracovního práva a sociálního zabezpečení ve smyslu čl. 9 odst. 2 písm. b) GDPR a případně s výjimkou zpracování nezbytného pro určení, výkon nebo obhajobu právních nároků dle čl. 9 odst. 2 písm. f) GDPR.

V takovém případě by bylo titul oprávněného zájmu dle článku 6 odst. 1 písm. f) GDPR pro zvláštní kategorie údajů možné aplikovat bez splnění dalších podmínek pouze pro oprávněné zájmy v oblasti určení, výkonu nebo obhajoby právních nároků dle čl. 9 odst. 2 písm. f) GDPR.

4.3.2.4 Výjimky ze zákazu zpracování zvláštních kategorií údajů výslovně neuvedené pro běžné údaje (včetně zpracování zveřejněných údajů)

Výjimky ze zákazu zpracování zvláštních kategorií údajů dle čl. 9 odst. 2 GDPR naopak obsahují některé důvody zpracování, které nejsou výslovně uvedeny ve

[460] Pracovní skupina pro ochranu osobních údajů zřízené podle čl. 29, čj. 844/14/CS, WP 217, Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES, ze dne 9. dubna 2014, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf.

výčtu obecných důvodů zpracování dle čl. 6 odst. 1 GDPR. Úvodní body odůvodnění GDPR k tomu neposkytují žádné vysvětlení.

Nelze předpokládat, že by čl. 9 odst. 2 GDPR připouštěl v těchto případech zpracování zvláštních kategorií údajů, pokud by takové zpracování bylo podle čl. 6 odst. 1 GDPR nezákonné a zároveň není pravděpodobné, že by účelem bylo umožnit správci zpracovávat jen zvláštní kategorie údajů, přičemž běžné osobní údaje jako např. identifikační údaje, by zpracovávat nemohl. Pro tuto diskrepanci zbývají jen dvě možná vysvětlení:

- zpracování z těchto důvodů musí být vždy podřaditelné pod některý důvod zpracování dle čl. 6 odst. 1 GDPR, nebo
- tyto důvody zpracování je třeba považovat za samostatné (další) důvody zpracování, které nejsou v čl. 6 odst. 1 GDPR výslovně uvedené.

Napárování jednotlivých důvodů zpracování nemusí být zcela zjevné pro zpracování zvláštních kategorií osobních údajů nadací, sdružením nebo jiným neziskovým subjektem dle čl. 9 odst. 2 písm. d) GDPR, zpracování údajů zjevně zveřejněných subjektem údajů dle čl. 9 odst. 2 písm. e) GDPR a zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely dle čl. 9 odst. 2 písm. j) GDPR.

4.3.2.4.1 Zpracování údajů nadací, sdružením nebo jiným neziskovým subjektem dle čl. 9 odst. 2 písm. d) GDPR

Takové zpracování je dle našeho názoru možné obecně podřadit zejména pod zpracování pro účely oprávněných zájmů dle čl. 6 odst. 1 písm. f) GDPR. Dodatečné podmínky uvedené v 9 odst. 2 písm. d) GDPR pak pravděpodobně představují kritéria pro účely balančního testu podle čl. 6 odst. 1 písm. f) GDPR, který je blíže rozveden v bodě 2 tohoto dokumentu.

4.3.2.4.2 Zpracování údajů zjevně zveřejněných subjektem údajů dle čl. 9 odst. 2 písm. e)

Lze předpokládat, že zpracování již zveřejněných údajů je možné rovněž podřadit především pod zpracování pro účely oprávněných zájmů dle čl. 6 odst. 1 písm. f) GDPR.

Podle výše uvedené argumentace vycházející především ze systematického výkladu GDPR by zpracování zveřejněných údajů bylo přípustné v rámci oprávněných zájmů správce dle čl. 6 odst. 1 písm. f) GDPR. Pro zpracování zvláštních kategorií údajů by navíc platila podmínka zjevného zveřejnění samotným subjektem údajů.

4.3.2.4.3 Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely dle čl. 9 odst. 2 písm. j) GDPR

Tyto tituly pro zpracování zvláštních kategorií dat je možné podřadit buď pod plnění právní povinnosti dle čl. 6 odst. 1 písm. c) GDPR nebo pod plnění úkolu ve veřejném zájmu dle čl. 6 odst. 1 písm. e) GDPR.

V případě tohoto specifického důvodu je rovněž případně možné zvažovat, že čl. 89 GDPR, který členským státům umožňuje derogaci[461] od některých ustanovení GDPR pro účely archivace, statistiky a výzkumu, je samostatným důvodem zpracování, jdoucím nad rámec důvodů uvedených v čl. 6 odst. 1 GDPR, přestože jeho text není takto výslovně formulován (k tomu rovněž srov. čl. 5 odst. 1 písm. b) GDPR).

4.3.3 Balanční test pro zpracování zveřejněných osobních údajů

Jestliže správce zakládá zpracování osobních údajů na oprávněném zájmu, což bude dle výše uvedené argumentace i zpracování již zveřejněných údajů, je dle bodu 47 odůvodnění GDPR povinen posoudit, zda tyto oprávněné zájmy převažují nad zájmy nebo základními právy a svobodami subjektu údajů. Pokud oprávněné zájmy správce nepřeváží, je povinen osobní údaje subjektu dále nezpracovávat.

V případě již zveřejněných údajů může být v praxi těžké abstraktně porovnat zájmy správce na straně jedné a soukromí subjektu údajů na straně druhé. Z toho důvodu je správce dle bodu 47 odůvodnění GDPR oprávněn vycházet z

[461] Čeští zákonodárci této možnosti využili v § 16 ZZOÚ. § 16 odst. 2 ZZOÚ navíc zavádí povinnost anonymizace zvláštních kategorií (citlivých) osobních povinnost tam, kde tomu nebrání oprávněné zájmy subjektu údajů.

přiměřených očekávání subjektu v konkrétní situaci. Pokud subjekt údajů zveřejnil či poskytl ke zveřejnění (viz bod 2.2 níže) údaje, aniž by mohl přiměřeně očekávat, že dojde k jejich zpracování zamýšlené správcem (resp. účel dalšího zpracování je zcela odlišný od primárního účelu zveřejnění), bude výsledek balančního testu při zpracování takových údajů na základě oprávněného zájmu správce pravděpodobně negativní. Právo na ochranu soukromí subjektu údajů, který nemohl přiměřeně předpokládat, že jeho údaje budou zpracovány určitým způsobem, převáží nad oprávněným zájmem správce takto údaje zpracovávat. Naopak ale, pokud subjekt údajů mohl při zveřejnění takové zpracování rozumně očekávat (resp. účel dalšího zpracování souvisí s účelem primárního zveřejnění), bude výsledek balančního testu pozitivní ve prospěch správce a zpracování bude přípustné.

Jestliže se tedy správci podaří prokázat, že subjekt při poskytnutí údajů mohl (a měl) přiměřeně očekávat, že údaje budou zpracovány tímto novým zamýšleným způsobem, bude to pro správce indikací pozitivního výsledku balančního testu, a tedy zákonnosti jím prováděného zpracování zveřejněných údajů.

Přestože test slučitelnosti v čl. 6 odst. 4 GDPR výslovně nezmiňuje zveřejnění osobních údajů, lze dovozovat, že další využití osobních údajů novým správcem zakládá nový účel zpracování. Toto nové využití osobních údajů (jiným) správcem tak bude podléhat tomuto testu slučitelnosti, v rámci kterého je (nový) správce povinen vyhodnotit, zda nové zamýšlené užití těchto zveřejněných údajů bude v souladu s původním účelem, pro který byly tyto osobní údaje zveřejněny (slovy čl. 6 odst. 4 písm. a GDPR: „pro který byly shromážděny“).

Výše popsaný balanční test založený zejména na přiměřených očekáváních subjektu údajů a účelu zpracování lze demonstrovat na zjevných extrémních příkladech: využití (zpracování) osobních údajů osob uvedených jako statutární orgány v obchodním rejstříku pro účely kontaktování právnické osoby prostřednictvím těchto osob (např. adresováno k jeho rukám) bude bez dalšího přípustné, protože subjekt údajů (fyzická osoba ve funkci statutárního orgánu) jednak mohl toto zpracování rozumně očekávat a navíc se jedná o účel přímo související s účelem, pro nějž jsou údaje v obchodním rejstříku primárně

zveřejňovány. Naopak stejný subjekt údajů nemůže rozumně očekávat, že adresa jeho bydliště uvedená v obchodním rejstříku bude využita za účelem nabízení spotřebitelských produktů nesouvisejících s předmětem jeho podnikání; nejedná se o účel, který by jakkoliv souvisel s primárním účelem zveřejnění.

Obdobně, pokud podnikatel – fyzická osoba zveřejní na internetových stránkách své osobní údaje, bude oprávněně očekávat, že takto zveřejněné osobní údaje budou třetí osoby zpracovávat např. za účelem jeho kontaktování v souvislosti s jeho obchodní činností (zejména za účelem zasílání objednávek zákazníků, ale rovněž nabídek potenciálních dodavatelů) a takové zpracování v obvyklých případech projde balančním testem[462]. Naopak pokud by jeho osobní údaje byly zpracovávány např. za účelem kontaktování ve věcech zcela nesouvisejících s jeho obchodní činností, tak takové zpracování subjekt údajů neočekává a pravděpodobně by (až na výjimky[463]) neprošlo balančním testem.

K obdobným závěrům dospěl při své dozorové činnosti i Úřad pro ochranu osobních údajů, když ve výše citované kontrole shledal, že: *„v daném případě je dán i zájem třetích osob, respektive veřejnosti, na dostupných a strukturovaných informacích o ekonomicky aktivních subjektech a obecně zájem na zvýšení transparentnosti podnikatelského prostředí. Další zpracování těchto osobních údajů, které se týkají výhradně ekonomické aktivity subjektů a nikoli rodinné či osobní sféry zároveň, nepředstavuje takový zásah do základních práv subjektů údajů, který by odůvodňoval závěr o tom, že zájmy subjektů údajů převáží tyto oprávněné zájmy. Zájmy subjektu údajů zásadně převáží až ve chvíli, kdy subjekt údajů vznese námitku proti tomuto zpracování.“*[464]

Rovněž využívání údajů z insolvenčního rejstříku a jejich indexace a zpřístupnění široké veřejnosti (včetně zamezení přístupu internetových vyhledavačů a robotů)

[462] V této oblasti je nezbytné upozornit, že další úpravu může přinést nové chystané nařízení *ePrivacy Regulation* upravující, mj. užívání osobních údajů při zasílání obchodních sdělení.

[463] Lze zvažovat např. oprávněný zájem v případě poskytování zpravodajství.

[464] Závěry Úřadu pro ochranu osobních údajů ve věci Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452.

již přesahuje hranice legitimního očekávání subjektů údajů a představuje významný zásah do jejich soukromí.[465]

Nicméně většina praktických reálných situací není na jedné či druhé straně spektra a test přiměřeného očekávání je pro tyto situace obtížněji odůvodnitelný a předvídatelný. Příkladem může být zpracování zveřejněných politických názorů, k němuž se vyjadřoval Úřad pro ochranu osobních údajů[466].[467]

4.4 Závěr

V roce 2017 magazín The Economist uvedl, že největším světovým bohatstvím již není ropa, ale data. Zatímco však v běžném (offline) životě uvedená data a informace plynutím času přirozeně vymizí z myslí jednotlivců, v prostředí internetu tyto údaje zůstávají uloženy v různých databázích, případně jsou volně šířeny, nadto i různě samovolně kombinovány a vkládány do různých kontextů, a to leckdy velmi nepřesným, účelovým či difamačním způsobem, jenž může závažným způsobem zasáhnout do soukromé sféry dotčeného jednotlivce. Tyto informace jsou navíc „hyper-provázané“, což zvyšuje jejich faktickou přístupnost a umožňuje spojování informací, které by v době před-internetové vyžadovaly desítky či stovky hodin rešerší v různých archivech, knižních zdrojích či matrikách napříč celým světem a mnohdy by stejně nevedly k (byť ani vzdáleně) obdobnému výsledkům.

Ve spojitosti s osobními informacemi a daty tato neustálá široká přístupnost přináší značná rizika ohledně způsobu jejich využívání a spolehlivosti. Tato data jsou navíc přístupná permanentně a stále se jen kumulují a vytvářejí propletenou

[465] K tomu srov. např. závěry Úřadu pro ochranu osobních údajů ve věci Kontrola zpracování veřejně přístupných údajů (společnost Úspěch Online s.r.o.). [online]. [cit 2019-06-01]. Dostupné z https://www.uoou.cz/kontrola-zpracovani-verejne-pristupnych-udaju-spolecnost-uspech-online-s-r-o/ds-5420/archiv=0&p1=5452.

[466] Stanovisko Úřadu pro ochranu osobních údajů ve věci „Zpracování politických názorů voličů pro kampaň je možné jen s jejich souhlasem“. [online]. 2.10.2018. [cit 2019-06-01]. Dostupné z https://www.uoou.cz/zpracovani-politickych-nazoru-volicu-pro-nbsp-kampan-je-mozne-jen-s-nbsp-jejich-souhlasem/d-31947.

[467] K tomu rovněž viz PATTYNOVÁ, Jana, Vladan RÁMIŠ, František NONNEMANN a Dominik VÍTEK. Zpracování údajů o politických názorech voličů na sociálních sítích pro volební kampaně [online]. 3.1.2019 [cit. 2022-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-udaju-o-politickych-nazorech-volicu-na-socialnich-sitich-pro-volebni-kampane-108618.html.

pavučinu různých střípků informací. Přinejmenším srovnatelné nebezpečí však vzniká i v souvislosti s nedostupností dat, resp. v souvislosti s jejich zastaráváním, roztříštěností nebo vytrháváním z kontextu. Takto používané (dis-)informace, navíc ještě veřejně dostupné na internetu, mohou vést ke značně zavádějícím výsledkům a značným zásahům do soukromí.

Oba tyto jevy tak posilují význam práva být zapomenut coby jednoho z projevů práva na informační sebeurčení, které dává jednotlivci kontrolu nad svými osobními údaji a dalšími informacemi a daty souvisejícími s jeho osobou a potenciálně tak ohrožující jeho soukromí a další osobnostní práva. Do té doby, než převládne jiný společenský zájem, by tak měl mít každý možnost plné kontroly nad rozsahem informací, které jsou o něm veřejně přístupné, a naopak i o těch, které přístupné nejsou. Obě situace totiž mohou vyvolat značné zásahy do soukromí a zneužitelnosti těchto informací.

Permanence a objem existujících informací na internetu přitom neohrožuje jen osobní sféru konkrétního jednotlivce, může ale ohrozit fungování celé demokratické společnosti. To bylo prezentováno na příkladu Facebook Cambridge Analytica, ve kterém docházelo k masivnímu zneužívání osobních údajů a informací osobní povahy k vytvoření osobních profilů a následnému ovlivňování voličských preferencí (v rámci prezidentských voleb v USA i v rámci referenda o Brexitu).

Druhým příkladem je povinné ukládání dat o elektronické komunikace, tzv. *data retention*, které představuje rizika zneužitelnosti dat ze strany soukromého sektoru (tj. telekomunikačních operátorů povinně ukládající tato data) i ze strany státu (zejména orgánů činných v trestních řízeních nebo zpravodajských služeb, které si mohou k těmto datům vyžadovat přístupy). Ačkoliv v rámci data retention povinností nedochází k ukládání obsahu komunikace, ale pouze metadat doprovázejících tuto komunikaci, tyto informace samy o sobě mohou podávat velmi komplexní obraz o daném uživateli a tím významně zasahovat do jeho soukromí. Státní moc (včetně České republiky) si význam těchto dat zjevně uvědomuje a pod záštitou boje s organizovaným zločinem a jinou závažnou trestnou činností ukládá tyto povinnosti. Ty přitom byly již předmětem několika

přezkumů na úrovni Soudního dvora EU i Ústavního soudu. Pár dnů před uzavřením této práce se k data retention opětovně vyjádřil SDEU, který připomněl, že aby nedocházelo k neodůvodněným zásahům do soukromí jednotlivců, nelze ukládat povinnosti k data retention plošně, a vždy musejí být odůvodněny konkrétním účelem a sledovanou trestnou činností. Na základě krátké analýzy a předchozích závěrů se domnívám, že česká úprava v podobě § 97 odst. 3 ZEK tyto požadavky nesplňuje a bude tak nezbytné přistoupit k její revizi, případně vypuštění z právního řádu.

V další části této kapitoly jsem se zabýval právní povahou dat, u kterých jsem dospěl k závěru, že vzhledem k širokému pojetí věci v českém právním řádu, data naplňují definici věci – nehmotné movité. Ačkoliv pojem „data“ se v českém (i evropském) právním řádu objevuje poměrně hojně a v dohledné době lze přinejmenším v EU očekávat přijetí dalších právních předpisů upravující nakládání s daty (jako např. tzv. *Data Governance Act* nebo *Data Act*), jejich bližší vymezení stále neexistuje. Zároveň je nezbytné rozlišovat informace o datech, jelikož informace je v zásadě abstraktní veličina, nijak neohraničená v prostoru ani čase, zatímco data jsou pak v zásadě *hmatatelným* projevem konkrétní informace. Data jako věc mají zároveň určitá specifika, jako je zejména v kybernetickém prostředí jejich neomezitelná replikovatelnost.

Pojetí dat jako věci však přináší značné výkladové problémy z hlediska majetkových práv, které lze k datům nabývat. V odborné literatuře existují první náznaky řešení této problematiky, jako je potenciální možnost vymezení rozsahu vykonatelných majetkových práv. Nicméně se domnívám, že k takovému řešení nelze přistupovat jen výkladově a byla by nezbytná právní úprava – inspirací by mohlo být např. autorské právo, které rozlišuje osobnostní a majetkovou složku autorských děl a vymezuje rozsah vykonatelných práv. Konkrétní řešení by vyžadovalo další analýzu v této oblasti, která však přesahuje cíle a možnosti této práce. V souvislosti s právem být zapomenut se navíc domnívám, že tato relevance je rovněž poměrně omezená, jelikož obecné nařízení o ochraně osobních údajů vymezuje konkrétní rámec aplikovatelnosti tohoto práva, a zpravidla tak převáží osobnostní složka a ochrana soukromí. V ostatních případech bude nezbytné na základě testu proporcionality poměřovat střet

základních práv – zde tedy právo na soukromí oproti (s největší pravděpodobností) právu na vlastnictví.

V rámci této kapitoly byly rovněž zkoumány možnosti dalšího využívání zveřejněných osobních údajů. Zde jsem dospěl k závěru, že za předpokladu, že správce osobních údajů splní nezbytné podmínky – zejména na základě balančního testu dostatečně zváží a zdůvodní své zájmy oproti zájmům subjektů údajů a splní své informační povinnosti – bude takové využívání údajů možné. Nicméně ani v tomto případě by nemělo docházet k omezení uplatňování práva být zapomenut. Správci, kteří obdobným způsobem budou data využívat, by měli přijmout vhodná opatření k tomu, aby např. zjistili, že došlo k výmazu původních dat, což by měli následně dostatečně reflektovat, pokud je to technicky možné. Nicméně v rámci balančního testu je nezbytné zvažovat právě i otázky permanence dat, a možnosti uplatnění práv subjektu údajů, jelikož zveřejnění údajů, tím méně jejich další používání dalšími subjekty (novými správci) v žádném případě nemůže vést ke snížení ochrany soukromí jednotlivců.

5 Pojem práva být zapomenut

5.1 Ideová východiska zapomínání

Zapomnění je důležitou součástí lidské společnosti a člověka – ať už pro samostatného jedince, jeho vývoj a rozvoj jeho osobnosti, tak na celospolečenské úrovni z hlediska „kolektivního“ zapomínání, resp. tedy ztráty informací z veřejně dostupných informací.

Zapomínání pro život a vývoj jednotlivce hraje stejnou roli jako paměť samotná.[468] Lidské vzpomínání není totiž jen pasivním procesem vyvolání původních informací v podobě, v jaké byly uloženy (jako je tomu v případě technologií), ale jedná se o aktivní, rekonstruktivní činností[469]; vzpomínky si totiž vybavujeme ovlivněné kontextem, v němž ke vzpomínání dochází, a minulost tak vnímáme optikou našeho současného já.[470] Efektivní fungování lidské mysli jednoznačně vyžaduje určité filtrování a očišťování již nepotřebných informací[471], aby nedošlo k zahlcení paměťové a mentální kapacity. Významu zapomínání a potenciálním důsledkům jeho absence v lidském životě se věnoval např. Jorge Luis Borge, který ve svém díle „Funes, muž se zázračnou pamětí“ popisuje příběh muže, který po pádu z koně ztratí schopnost zapomínání, tedy v zásadě trpí absolutním případem tzv. hyperthymesie[472]; v podání Borga tato schopnost zapomínat vede ke kompletní tělesné i myšlenkové paralýze: *„Myslit znamená*

[468] PAGALLO, Ugo a DURANTE, Massimo. Legal memories and the right to be forgotten. In: Luciano FLORIDI, ed. Protection of Information and the Right to Privacy-A New Equilibrium? B.m.: Springer, 2014, s. 17–30. ISBN 978-3-319-05719-4.

[469] SCHACTER, Daniel L. The seven sins of memory: Insights from psychology and cognitive neuroscience. American Psychologist [online]. 1999, 54(3), 182–203. ISSN 0003-066X. Dostupné z: doi:10.1037//0003066X.54.3.182. s. 194.

[470] SCHACTER, Daniel L., CHIAO, Joan Y. a MITCHELL, Jason P. The seven sins of memory: implications for self. Annals of the New York Academy of Sciences. 2003, 1001, 226–239. ISSN 0077-8923. s. 227.

[471] BANNON, Liam J. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign. 2006, 2(1), 3–15. ISSN 1571-0882, 1745-3755. s. 7.

[472] Popis případů hyperthymesie, kterými se zabývá např. PARKER, Elizabeth S., CAHILL, Larry a MCGAUGH, James L. a case of unusual autobiographical remembering. Neurocase. 2006, 12(1), 35–49.

zapomenout na rozdíly, generalizovat, abstrahovat. Ve Funesově napěchovaném světě existovaly jen detaily, téměř bezprostřední detaily".[473]

Zapomnění je přitom významné nejen pro konkrétní jednotlivce, ale pro vývoj celé společnosti a jejího fungování. Pokud by společnost nezapomínala, významně by se limitovaly možnosti jejího rozvoje: *„Pokud bychom se museli strachovat, že všechny naše soukromé informace budou uchovány po celý náš život, vyjadřovali bychom se stále k nepodstatným klevetám, sdíleli bychom své osobní zkušenosti, činili nejrůznější politická prohlášení, nebo bychom se uchýlili k autocenzuře? Tlumící efekt dokonalé paměti ovlivňuje naše chování.*[474] *[...] Bez možnosti retrospektivního vykoupení nám zůstává již jen prospektivní opatrnost."*[475]

V moderní technologické společnosti se však na zapomínání, které lze přirovnat ztrátě původně uložených dat, hledí jako na určité selhání, kterému je třeba se vyvarovat.[476] Tím v zásadě dochází k popírání smyslu a hlavní funkce zapomnění. Digitální paměť a permanence informací v digitálním světě[477] jsou přímým opakem této základní funkce a jednotlivci znemožňují, případně výrazně znesnadňují tzv. „čerstvý začátek"[478] v případech, kdy by je takové zapomnění výslovně žádoucí (jako např. zahlazení trestných činů), zejména pro přijetí ze strany ostatních lidí[479].

---

[473] BORGES, Jorge Luis. Funes, muž se zázračnou pamětí. In: Jorge Luis BORGES Spisy I. Praha: Argo, 2009. ISBN 978-80-257-0146-1.

[474] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 10.

[475] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 112.

[476] BANNON, Liam J. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign. 2006, 2(1), 3–15. ISSN 1571-0882, 1745-3755. s. 5.; COYNE, Nora H. Exploring the Notion of Forgetting. The Gettysburg College Student Publications [online]. 2017, (509). Dostupné z: http://cupola.gettysburg.edu/student_scholarship/509/.

[477] K tomu viz kapitola 4.1 této práce.

[478] BLANCHETTE, Jean-François a JOHNSON, Deborah G. Data retention and the panoptic society: The social benefits of forgetfulness. The Information Society. 2002, 18(1), 33–45. s. 35.

[479] MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5. s. 118.

O to významnější je, aby každý měl možnosti kontroly nad svým soukromím a zároveň mohl uplatňovat svá práva. Právě právo být zapomenut lze tedy považovat za jedno z vůdčích práv, které jednotlivcům umožňuje kontrolovat své soukromí, vnímání širokou veřejností i svou reputaci, a to zejména v digitálním světě, ve kterém se často nezapomíná.

5.2 Historický vývoj práva být zapomenut v rámci Evropské unie

5.2.1 Paralely práva být zapomenut

Účelové zapomínání není v právu žádným novým fenoménem, který by do formulace práva být zapomenut v právním světě neexistoval, avšak až se zakotvením tohoto práva se dostává skutečně do dispozice jednotlivce, jelikož do té doby se víceméně jednalo o systematizované přiznání důsledků plynutí času. Takto tomu je zejména ve dvou právních institutech, na kterých lze účel a význam zapomínání demonstrovat – částečně lze zvažovat promlčení (ať již v soukromoprávních vztazích, nebo promlčení deliktů v soukromém, správním i trestním právu) nebo zahlazení odsouzení v trestním právu. Zatímco tedy promlčení samo o sobě primárně reflektuje problémy spojené s plynutím času, jako je zhoršení dostupnosti a vypovídací hodnoty důkazů (což platí v soukromém[480] i trestním[481] právu), rovněž motivuje dlužníky k výkonu jejich práv[482], ale rovněž reflektuje společenský zájem[483] na trestání některých činů.

[480] Srov. např. BRIM in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 1950.

[481] Srov. např. PÚRY in ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012, 2 sv. (xvi, 1450, xiv s., s. 1451-3586). ISBN 978-80-7400-428-5, s. 454.

[482] Srov. např. BRIM in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 1950.

[483] *„Slábne, až docela zaniká potřeba trestněprávní reakce na trestný čin, a to jak z hlediska generální prevence (např. na trestný čin se zapomíná, negativní ovlivnění společenského vědomí mizí a škodlivost činu se snižuje), tak i z hlediska prevence individuální (u pachatele, jenž nespáchal další trestný čin, který je stejně nebo přísněji trestný, se předpokládá pozitivní změna jeho osoby, která rovněž přestala být nebezpečnou).“* in PÚRY in ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012, 2 sv. (xvi, 1450, xiv s., s. 1451-3586). ISBN 978-80-7400-428-5, s. 454.

Pokud budeme na zapomnění hledět jako na určitou formu úniku své vlastní minulosti, resocializaci či možnosti „začít znovu“ (rovněž spjatou s plynutím času), přicházejí v úvahu další instituty dlouhodobě zakotvené v právním řádu. Za nejvýznamnější považuji institut zahlazení odsouzení v trestním právu nebo pak rovněž úpadek a s ním spojené insolvenční důsledky.

Účelem institutu zahlazení odsouzení (v českém právním řádu zakotveném v § 105 a 106 trestního zákoníku) je umožnit pachateli, aby po splnění určitých podmínek byly odstraněny nepříznivé důsledky jeho odsouzení, které přetrvávají i po výkonu trestu či ochranného opatření a které by mu mohly ztěžovat uplatnění v dalším životě.[484] Řada autorů rovněž spatřuje konceptuální východiska práva být zapomenut ve francouzském *droit à l'oubli*, které se začalo v právní teorii objevovat v 70. letech minulého století.[485] Právo *droit à l'oubli* umožňovalo odsouzeným domáhat se toho, aby údaje o jejich kriminální minulosti nebyly nadále zveřejňovány[486], resp. aby nebyly spojování s již irelevantními aspekty své minulosti[487]. Obdobnou úpravu pak nabízel italský institut práva *diritto all'oblio*[488] a další paralely pak lze nalézt ve většině právních úprav členských států, kde mají pachatelé odsouzení za trestný čin právo ochrany svých trestních záznamů před nedovoleným přístupem či užitím těchto záznamů – a to zpravidla

[484] PÚRY in ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012, 2 sv. (xvi, 1450, xiv s., s. 1451-3586). ISBN 978-80-7400-428-5, s. 1123.

[485] XANTHOULIS, Napoleon. Conceptualising a Right to Oblivion in the Digital World: a Human Rights-Based Approach [online]. SSRN Scholarly Paper. ID 2064503. Rochester, NY: Social Science Research Network. 2012 [vid. 2022-04-01]. Dostupné z: https://papers.ssrn.com/abstract=2064503.

[486] ROSEN, Jeffrey. The Right to Be Forgotten. Stanford Law Review Online. 2011, 64, 88–92. s. 88.; TAMO, Aurelia a GEORGE, Damian. Oblivion, Erasure and Forgetting in the Digital Age. Journal of Intellectual Property, Information Technology and Electronic Commerce Law. 2014, 5, 71–87. s. 72.

[487] Např. PINO, Giorgio. The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights [online]. SSRN Scholarly Paper. ID 1737392. Rochester, NY: Social Science Research Network. 2000 [vid. 2022-04-02]. Dostupné z: https://papers.ssrn.com/abstract=1737392.

[488] MITROU, Lilian a Maria KARYDA. EU's Data Protection Reform and the right to be forgotten—A legal response to a technological challenge?. 5th International Conference of Information Law and Ethics. 2012, str. 29 - 30 [online]. [cit. 2022-04-02] Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245.

po uplynutí určité doby (po jejímž uplynutí dojde buď k úplnému odstranění či výmazu některých trestních záznamů).[489]

5.2.2 Rozsudek SDEU ve věci Google Spain[490]

Právo být zapomenut v podobě, ve které ho dnes známe, bylo poprvé formováno v rozsudku Soudního dvora ve věci Google Spain z roku 2014. Soudní dvůr se ve svém rozhodnutí zabýval podmínkami, za kterých musí internetový vyhledávač (zde Google) vymazat určité výsledky vyhledávání a za jakých okolností má tak subjekt údajů právo na to, aby daná informace týkající se jeho osoby již nebyla nadále spojena s jeho jménem. SDEU ve svém rozhodnutí dovodil, že čl. 12 písm. b) a čl. 14 první pododstavec písm. a) směrnice 95/46/ES musí být vykládány v tom smyslu, že za účelem respektování práv zakotvených v uvedených ustanoveních musí provozovatel vyhledávače vymazat ze zobrazovaného seznamu výsledků vyhledávání provedeného na základě jména osoby (v posuzovaném případě jméno španělského občana Mario Costeja González) odkazy na webové stránky zveřejněné třetími osobami a obsahující informace týkající se této osoby. Soudní dvůr v posuzovaném případě provedl test proporcionality mezi právem na ochranu soukromí subjektu údajů a veřejným zájmem společnosti nalézt uvedenou informaci na základě vyhledávání jména.

Případ se týkal španělského občana jménem Mario Costeja González, jehož nemovitosti byly koncem devadesátých let předmětem exekuce z důvodu dluhu na sociálním pojištění. Tato informace se objevila v deníku La Vanguardia, který je zveřejnil on-line, čímž se stala dostupná širokému okruhu veřejnosti prostřednictvím vyhledávače Google díky indexaci této informace ve výsledcích vyhledávání.

---

[489] CASTELLANO, Pere Simón. The Right to Be Forgotten under European Law: a Constitutional Debate. 2012, Lex Electronica, číslo 16.1 [online]. [cit. 2022-04-02] Dostupné z: www.lex-electronica.org/docs/articles_300.pdf.

[490] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 197 – 215.

SDEU s odkazem na svou předchozí judikaturu ve věci eDate Advertising[491] uvedl, že zpracování osobních údajů prováděné společností Google (jakožto provozovatelem vyhledávače) se může významně dotknout základního práva na soukromí a základního práva na ochranu osobních údajů, je-li vyhledávání pomocí tohoto vyhledávače uskutečněno na základě jména fyzické osoby, pokud uvedené zpracování umožní všem uživatelům internetu získat prostřednictvím seznamu výsledků vyhledávání strukturovaný přehled informací, které se týkají dotčené osoby a jsou dohledatelné na internetu, které se mohou týkat řady aspektů jejího soukromí a které by bez uvedeného vyhledávače nemohly – nebo jen velmi obtížně mohly – být vzájemně propojeny, a vytvořit tak víceméně podrobný profil subjektu údajů. Navíc účinek zásahu do uvedených práv subjektu údajů je znásoben z důvodu významné úlohy, kterou hrají v moderní společnosti internet a vyhledávače, jež činí informace obsažené v takovém seznamu všudypřítomnými.[492]

Soud zvažoval hospodářské zájmy společnosti Google, které shledal jako nedostatečné pro odůvodnění zásahu do soukromí stěžovatele. Dále zvažoval zájmy na ochraně soukromí stěžovatele oproti legitimním zájmům uživatelů internetu, kteří by mohli mít zájem na přístupu k této informaci a jejichž právo na informace by mohlo být výmazem informace o panu Gonzálezovi dotčeno. Soud konstatoval, že rovnováha těchto práv bude záviset v konkrétních případech na povaze dotčené informace a její citlivosti v souvislosti se soukromím subjektu údajů, jakož i na zájmu veřejnosti mít k této informaci přístup, jenž se může lišit zejména v závislosti na úloze, kterou má subjekt údajů ve veřejném životě.[493]

SDEU zde dovodil, že v případě, kdy neexistuje převažující legitimní zájem veřejnosti na existenci určité informace, má subjekt údajů právo, aby jeho osobní údaje byly smazány. Paradoxem toho rozhodnutí je, že po uplatnění – a v zásadě vytvoření práva být zapomenut Mario Costeja González již nikdy zapomenut nebude a stejně tak informace o jeho exekucích, které byly hlavním motivátorem

[491] Rozsudek SDEU ze dne 25. října 2011 ve věci C-509/09 eDate Advertising a další.

[492] Bod 80 rozsudku ve věci Google Spain.

[493] Bod 81 rozsudku ve věci Google Spain.

toho, proč se vůbec do soudního sporu a vymáhání svého práva na výmaz domáhal.[494] To však nemění nic na tom, že pro miliony lidí v nejen Evropě, ale vzhledem k dnešním dopadům GDPR po celém světě zajistil nezadatelné právo být zapomenut a kontrolu nad vlastní existenci v (zejména) kybernetickém světě.

Rozsudek ve věci Google Spain přitom nebyl průlomový jen ve formulaci a přiznání práva být zapomenut, ale rovněž v jeho aplikační rovině, kde, ač v rámci španělského soudního řízení, Soudní dvůr EU uznal (na základě výkladu pojmu provozovna, angl. *establishment*), že povinnosti vyplývající z evropských předpisů na ochranu osobních údajů lze – právě prostřednictvím španělské *provozovny* (Google Spain) – uplatňovat i vůči samotnému provozovateli sídlícímu v USA – americké společnosti Google Inc. Tento výklad tak přinesl zásadní posun pojetí internetu a možností ohledně domáhání se práva na internetu. Tento aplikační projev se pak propsal do rozsahu místní působnosti obecného nařízení o ochraně osobních údajů, které je blíže popsáno v kapitole 3.2.4 této práce.

Třetím významným bodem byla kvalifikace provozovatele vyhledávače jako správce osobních údajů, čímž se SDEU výslovně odchýlil od názoru generálního advokáta Jääskinsena[495]. Soud dospěl k závěru, že zpracování osobních údajů

[494] Tento efekt bývá také někdy označován jako tzv. Streisand efekt. Srov. např. PEGUERA, Miquel. No More right-to-be-forgotten for Mr. Costeja, Says Spanish Data Protection Authority. The Center for Internet and Society, Stanford Law School, 2015 [online]. [cit. 2022-01-24]. Dostupné z: http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority.

[495] Stanovisko generálního advokáta Niila Jääskinena přednesené dne 25. června 2013 ve věci C-131/12 Google Spain. Generální advokát poukazoval na široké pojetí pojmu správce *„[…] svědčí iracionalitě nekritického doslovného výkladu směrnice v kontextu internetu. Soudní dvůr by neměl přijmout výklad, podle kterého je správcem odpovědným za zpracování osobních údajů zveřejněných na internetu v podstatě každý, kdo vlastní chytrý telefon, tablet nebo laptop“*, a to proto, že *„poskytovatel služeb internetového vyhledávače nemůže právně nebo fakticky splnit povinnosti správce uvedené v článcích 6, 7 a 8 směrnice v souvislosti s osobními údaji uvedenými na zdrojových internetových stránkách umístněných na hostitelských serverech třetích osob.“* Podle generálního advokáta Jääskinena by pak platilo, že *„internetové vyhledávače jsou neslučitelné s unijním právem, což je závěr, který považuji za absurdní. Konkrétně, pokud by poskytovatelé služeb internetového vyhledávače byli považováni za správce osobních údajů uvedených na zdrojových internetových stránkách třetích osob, a pokud by některá z těchto stránek obsahovala „zvláštní kategorie údajů“ uvedené v článku 8 směrnice (například osobní údaje prozrazující politické názory nebo náboženské*

prováděné v rámci činnosti vyhledávače ovlivňuje základní práva subjektu údajů; proto provozovatel uvedeného vyhledávače musí, jako správce odpovědný za dané zpracování, v rámci své odpovědnosti, pravomoci a možností zajistit, aby toto zpracování splňovalo požadavky směrnice 95/46/ES, a aby směrnicí stanovené záruky mohly nabýt plného účinku.[496]

5.2.3 Další vývoj po rozsudku Google Spain

5.2.3.1 Rozhodovací praxe ESLP

Právo být zapomenut se (v určitých modifikacích, nicméně s podobnými důsledky) objevilo rovněž v rozhodovací praxi Evropského soudu pro lidská práva, a to dokonce před přijetím rozsudku ve věci Google Spain. Tyto případy sám ESLP označil za aplikaci práva být zapomenut.[497] Např. v roce 2006 ESLP uzavřel, že dlouhodobé uchovávání v archivech bezpečnostní služby již nenaplňuje požadavky nezbytnosti v demokratické společnosti a na základě toho rozhodl o právu stěžovatele na výmaz takových údajů.[498] V několika stížnostech se rovněž zabýval možností obviněných nebo pouze podezřelých ze spáchání trestného činu, aby došlo po určité době k odstranění jejich osobních údajů (profil DNA, fotografie totožnosti a otisky prstů) shromážděných orgány činnými v trestním řízení v databázích zaměřených na prevenci a boj proti zločinu.[499]

Za významné pak považuji rozhodnutí z r. 2018 ve věci M.L. a W.W. proti Německu[500], kde se soud zabýval možností stěžovatelů domáhat se výmazu

---

přesvědčení nebo údaje týkající se zdraví nebo sexuálního života jednotlivců), činnost poskytovatele služeb internetového vyhledávače by se automaticky stala nezákonnou, pokud by nebyly splněny přísné podmínky stanovené v tomto článku pro zpracování takových údajů."

[496] Bod 83 rozsudku ve věci Google Spain.

[497] EUROPEAN COURT OF HUMAN RIGHTS. Guide to the Case-Law of the of the European Court of Human Rights. Data Protecion. [online]. 31.12.2021. [cit- 2022-04-03]. Dostupné z https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

[498] Rozhodnutí ESLP ze dne 6. června 2006 ve věci 62332/00 Segerstedt-Wiberg a další proti Švédsku.

[499] Srov. např. rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 5335/06 B.B. proti Francii, rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 16248/05 Gardel proti Francii, nebo rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 18. dubna 2013 M.K. proti Francii.

[500] Rozhodnutí ESLP ze dne 28. června 2018 ve věci 60798/10 a 65599/10 M.L. a W.W. proti Německu.

informací o své osobě z médií – jednalo se pachatele vraždy, kteří byli po čtrnácti letech (po výkonu trestu) propuštěni na svobodu a následně se domáhali výmazu těchto informací zahrnující jejich identity a fotografie ve spojitosti se soudním procesem z médií. Soud zde uzavřel, že veřejnost má objektivní zájem na přístup k těmto informacím.

5.2.3.2 Soudní dvůr Evropské unie

5.2.3.2.1 Rozhodnutí ve věci Manni

Na rozhodnutí ve věci Google Spain SDEU poměrně plynule navázal v roce 2017 rozsudkem ve věci Manni[501]. V tomto případě Soudní dvůr konstatoval, že veřejný zájem na zachování údajů ve veřejných rejstřících (v tomto případě v obchodním rejstříku) je natolik silný, že právo být zapomenut je zde vyloučeno. Stížnost se týkala vedení osobních údajů jednotlivce ve veřejném obchodním rejstříku.

Pan Manni požádal obchodní komoru v Lecce, aby vymazala jeho osobní údaje z rejstříku poté, co zjistil, že případní zákazníci mohou nahlížet do rejstříku a zjistit, že byl jednatelem společnosti, která před více než deseti lety vyhlásila úpadek. Tato informace odrazovala případné zákazníky a mohla mít nepříznivý dopad na jeho obchodní zájmy. SDEU zvažoval práva ochrany údajů EU a obchodní zájem pana Manniho na odstranění informací o úpadku jeho někdejší společnosti na jedné straně a veřejný zájem na přístup k informacím na straně druhé. Soudní dvůr připomněl skutečnost, že takové zveřejnění informace ve veřejném rejstříku obchodních společností je zakotvené v zákoně implementující směrnici EU. Cílem těchto předpisů je přitom usnadnit třetím osobám přístup k informacím o společnostech. Zveřejnění je důležité pro ochranu zájmů třetích osob, které mohou chtít obchodovat s danou společností, protože jediné záruky, které třetím osobám nabízí akciová společnost a společnost s ručením omezeným, jsou její aktiva.[502]

[501] Rozsudek Soudního dvora Evropské unie ze dne 9. března 2017 ve věci C-398/15 Manni.

[502] Příručka evropského práva v oblasti ochrany osobních údajů. [online]. [cit. 2022-02-12]. Dostupná z https://www.echr.coe.int/Documents/Handbook_data_protection_CES.PDF.

Vzhledem k významu legitimního cíle, který rejstřík sleduje, SDEU rozhodl, že pan Manni nemá právo dosáhnout výmazu svých osobních údajů, protože nad jeho právy podle právních předpisů o ochraně osobních údajů převažuje nezbytnost chránit zájmy třetích osob ve vztahu k akciovým společnostem a ke společnostem s ručením omezeným a zajistit právní jistotu, poctivost obchodních transakcí, a tedy i řádné fungování vnitřního trhu. Toto zveřejnění tedy nevede k nepřiměřenému zásahu do základních práv dotyčných osob, a zejména do jejich práva na respektování soukromého života, jakož i jejich práva na ochranu osobních údajů, která jsou zaručena články 7 a 8 Listiny EU.[503]

5.2.3.2.2 Rozhodnutí ve věci GC a další

Další rozsudek aplikující a interpretující právo být zapomenut bylo rozhodnutí SDEU ve věci CG a další[504] z roku 2019, ve kterém se SDEU zabýval problematikou citlivých osobních údajů ve smyslu čl. 8 Směrnice 95/46/ES, a dále otázkou, jaký význam by měly mít výjimky pro zpracování osobních údajů výlučně pro účely novinářské činnosti (nebo uměleckého či literárního projevu) dle čl. 9 Směrnice 95/46/ES z hlediska provozovatelů internetových vyhledávačů.

Paní G. C. a pánové A. F., B. H. a E. D. žádali každý jednotlivě společnost Google Inc., aby odstranila z výsledků vyhledávání, které se zobrazí při zadání jejich jména do vyhledávače provozovaného touto společností, různé odkazy vedoucí na webové stránky zveřejněné třetími osobami, což společnost Google odmítla. Paní G. C. požádala o odstranění odkazu na satirickou fotomontáž zveřejněnou pod pseudonymem dne 18. února 2011 na kanále YouTube, na níž je vyobrazena vedle starosty obce, kde vykonávala funkci vedoucí kanceláře starosty, a která jasně naznačuje, že spolu mají intimní poměr, a také rozebírá vliv tohoto intimního poměru na její politickou kariéru. Další stěžovatel, pan A. F., usiloval o odstranění odkazů vedoucích na článek v deníku Libération ze dne 9. září 2008, který byl zveřejněn rovněž na internetových stránkách Centre contre les manipulations mentales (Centrum proti mentální manipulaci, dále jen „CCMM“),

[503] Bod 57 rozsudku Soudního dvora Evropské unie ze dne 9. března 2017 ve věci C-398/15 Manni.

[504] Rozsudek SDEU ze dne 24. září 2019 ve věci C-136/17 - GC a další.

a týkal se sebevraždy člena scientologické církve. Pan B. H. požadoval odstranění odkazů, které vedly na články, zejména na články, které vyšly v tisku, o soudním řízení zahájeném v červnu 1995, týkajícím se financování Republikánské strany, v rámci kterého bylo vůči němu a několika dalším podnikatelům a politikům vzneseno obvinění. Pan E. D. požadoval odstranění odkazů vedoucích na články publikované v denících Nice Matin a le Figaro, které informují o jednání v rámci trestního řízení, v němž byl odsouzen k trestu odnětí svobody v délce trvání sedmi let a dále k trestu soudního ochranného dohledu v délce deseti let za sexuální násilí vůči nezletilým osobám mladším patnácti let.[505]

V posuzovaném případě se tak jednalo o zpracování různých kategorií údajů, a to včetně údajů o trestné činnosti (dle čl. 8 odst. 5 směrnice 95/46/ES, dnes upravené v čl. 10 GDPR) a zvláštních kategorií osobních údajů (dle čl. 8 odst. 1 směrnice 95/46/ES, dnes upravené v čl. 9 odst. 1 GDPR). Proto může být zásah do základního práva subjektu údajů na soukromí a na ochranu osobních údajů zvláště závažný vzhledem k citlivosti těchto údajů.[506]

Ve vztahu k údajům o „protiprávním jednání“ a „odsouzení za trestné činy“ ve smyslu čl. 8 odst. 5 směrnice 95/46/ES (a tedy dnes v rámci čl. 10 GDPR) je provozovatel vyhledávače povinen vyhovět žádosti o odstranění odkazů, pokud se tyto informace týkají dřívější fáze dotčeného soudního řízení a s ohledem na jeho průběh již neodpovídají současnému stavu a jestliže s ohledem na všechny okolnosti konkrétního případu převažují základní práva subjektu údajů zaručená články 7 a 8 Listiny EU nad zájmy potenciálně interesovaných uživatelů internetu chráněnými článkem 11 Listiny EU.[507] Stejný závěr pak soud konstatoval ve vztahu ke zvláštním kategoriím osobních údajů (ve smyslu čl. 8 odst. 1 směrnice 95/46/ES, dnes tedy čl. 9 odst. 1 GDPR).[508]

[505] Body 25-29 stanoviska generálního advokáta Macieje Szpunara ze dne 10. ledna 2019 ve věci C-136/17 - GC a další.

[506] Bod 44 a 67 rozsudku SDEU ze dne 24. září 2019 ve věci C-136/17 - GC a další.

[507] Bod 79 rozsudku SDEU ze dne 24. září 2019 ve věci C-136/17 - GC a další.

[508] Bod 69 rozsudku SDEU ze dne 24. září 2019 ve věci C-136/17 - GC a další.

Soudní dvůr tak rovněž na tyto senzitivní informace aplikoval test proporcionality a zvažoval, do jaké míry má veřejnost právo na přístup k těmto informacím. Senzitivní povaha informací musí být zvážena v rámci testu proporcionality, avšak sama o sobě bez dalšího neodůvodňuje automatický výmaz.

5.2.3.3 Rozhodovací praxe v členských státech

Konkrétní aplikace práva být zapomenut se již objevila i rozhodovací praxi dalších členských států EU (bez toho, aniž by doputovaly k SDEU). Jako jeden příklad za všechny si dovolím poukázat na příklad německého Spolkového ústavního soudu z roku 2019[509]. Televizní kanál Norddeutscher Rundfunk odvysílal v lednu r. 2010 díl pořadu Panorama s názvem „Výpověď: Odporné triky zaměstnavatelů." V tomto pořadu bylo zmíněno i jméno pozdější stěžovatelky, která byla obviněna z nespravedlivého chování vůči zaměstnanci. Stěžovatelka pořadu poskytla rozhovor, ve kterém se k případu vyjádřila. Díl byl dostupný v online archivu tohoto televizního kanálu a zobrazoval se ve výsledcích vyhledávání Google při vyhledání jména stěžovatelky.[510]

Soud se věnoval porovnání jednotlivých konkurujících si práv a zájmů, kde tedy na straně stěžovatelky došlo k zásahu do práva na respektování soukromého a rodinného života (čl. 7 Listiny EU) a práva na ochranu osobních údajů (čl. 8 Listiny EU). Oproti tomu soud porovnával právo spol. Google na svobodu podnikání (ve smyslu čl. 16 Listiny EU). Svobodu projevu (čl. 11 Listiny EU) soud zvažoval jako obecný princip. Soud zároveň zvažoval oprávněná práva tvůrců. Stěžejním východiskem vážení zájmů pak je, že se nevychází z domněnky přednosti osobnostních práv[511].

[509] Rozhodnutí Spolkového ústavního soudu ze dne 6. listopadu 2019, sp. zn. 1 BvR 276/17.

[510] FRONC, Jaromír. Google, právo být zapomenut a Listina základních práv EU. Revue pro právo a technologie [online]. 2020, 11(21) [cit. 2022-03-14]. ISSN 1805-2797. Dostupné z: doi:https://doi.org/10.5817/RPT2020-1-7.

[511] Bod 28 rozhodnutí Spolkového ústavního soudu ze dne 6. listopadu 2019, sp. zn. 1 BvR 276/17.

Rozhodnutí Spolkového ústavního soudu bylo považováno za poměrně kontroverzní[512], jelikož bez dalšího přistoupil k aplikaci Listiny EU, aniž by položil předběžnou otázku SDEU a rovněž částečně ignoroval rozhodnutí SDEU ve věci Google Spain, které naopak vyzdvihují význam ochrany osobnosti a osobních práv ve smyslu čl. 7 a 8 Listiny EU nad ekonomickými zájmy. Zároveň nově zvážil 11 a 16 Listiny EU a stejně tak nezbytné zohledňování práv tvůrce obsahu.

Spolkový ústavní soud tedy aplikaci práva být zapomenut podmínil proporcionálním zvažováním dalších zájmů – základními právy příslušných tvůrců obsahu a informačními zájmy uživatelů internetu, a to v rámci svobody podnikání provozovatelů vyhledávání.

5.3 Funkce a povaha práva být zapomenut

Funkce práva být zapomenut, resp. tedy práva domáhat se výmazu svých osobních údajů a jiných informací, úzce souvisí s problematikou zapomnění jednotlivců i společnosti jako celku.

Zveřejňováním informací může docházet k podstatnému zásahu do cti, důstojnosti či soukromí konkrétní osoby, a i když jde o zásah, který lze v době, kdy k němu došlo, označit za legitimní, jeho negativní důsledky pro osobní sféru jednotlivce mohou přetrvávat ještě dlouho po takovém zveřejnění nebo dokonce mohou být trvalé povahy. Čím jsou tyto informace senzitivnější, o to větší zásah se může jednat – takový efekt mohou mít zejména informace o trestné činnosti, zejména pokud se následně ukáží jako nepravdivá a je vydáno zprošťující rozhodnutí. Zveřejnění a permanentní přístupnost takových informací může představovat trvající protiprávní zásah do důstojnosti, cti či soukromí dotčené osoby.[513]

O to zásadnější může být zveřejnění (či neustálá dostupnost) zavádějících, neúplných, útržkovitých anebo zastaralých informací. Jejich přístupnost (ať už

[512] Srov. FRONC, Jaromír. Google, právo být zapomenut a Listina základních práv EU. Revue pro právo a technologie [online]. 2020, 11(21) [cit. 2022-03-14]. ISSN 1805-2797. Dostupné z: doi:https://doi.org/10.5817/RPT2020-1-7.

[513] Srov. např. nález Ústavního soudu ze dne 23. června 2020, sp. zn. IV. ÚS 2257/18.

veřejnosti nebo i jen úzce vymezenému okruhu osob) může být nežádoucí i v době jejich vzniku, a tím spíše pak při dalším plynutí času, kdy se navíc zcela vytratí kontext původní informace. V době internetové jsme si navíc zvykli nakládat s dostupnými informacemi jako jakýmsi „komplexním profilem“ osoby, na který se často spoléháme i při zásadních událostech, jako jsou např. pohovory do zaměstnání (jakkoliv by takové využívání informací ze strany zaměstnavatelů mělo být omezené).

Právo být zapomenut je tak projevem práva na informační sebeurčení, které dává jednotlivci možnosti kontrolovat informace, které o něm existují, resp. pak data, do kterých se tyto informace propisují. Zájem na existenci těchto informací může existovat jak vůči úzce vymezenému okruhu osob (rodina, zaměstnavatel, poskytovatel sociální sítě, ale rovněž i státu aj.) ale i obecně veřejnosti.

Veřejnou dostupnost informací je přitom vždy nezbytné zvažovat v kontextu dané situace, protože ne vždy musí existovat zájem na tom, abychom „byli zapomenuti“, resp. aby negativní informace o nás nemohla být více připomínána, ale naopak aby příslušná informace byla připomenuta spolu s vyjasněním takové situace. Tak tomu může být např. v případě zveřejnění informací týkající se potenciální trestné činnosti nebo obžaloby konkrétní osoby, která může mít následně imanentní zájem na tom, aby taková informace byla vždy přístupná, avšak s dodatkem, jaký byl výsledek daného řízení.[514] O to významnější je, aby právo být zapomenut bylo v dispoziční sféře jedince, který tak může plně kontrolovat informace o své osobě.

Ačkoliv je tedy (dosavadní) aplikace práva být zapomenut skloňována zejména v souvislosti s veřejně dostupnými informacemi, nesmíme zapomínat na jejich význam i ve vztahu k mnohem užšímu okruhu příjemců, vůči kterému mohou mít určité informace srovnatelně ničivé účinky, a vůči kterým by tak měly rovněž existovat prostředky k výmazu.

Funkcí práva být zapomenut je tak ochrana jednotlivce, který by (obdobně, jako je tomu např. u zahlazení odsouzení) měl mít možnost „čerstvého začátku“, resp.

[514] Srov. bod 44 nálezu Ústavního soudu ze dne 23. června 2020, sp. zn. IV. ÚS 2257/18.

aby byl plně chráněn nejen vůči veřejnosti, ale i vůči státu a jiným (konkrétním) osobám soukromého práva, kteří přinejmenším plynutím času ztrácejí legitimní zájmy na dispozici s takovými informacemi, které by mohly opodstatnit přístup k okruhu těmto informacím.

5.4 Závěr

Zapomnění je důležitou součástí lidské společnosti a člověka – ať už pro samostatného jedince, jeho vývoj a rozvoj jeho osobnosti, tak na celospolečenské úrovni z hlediska „kolektivního“ zapomínání, resp. tedy ztráty informací z veřejně dostupných zdrojů. Zapomínání pro život a vývoj jednotlivce hraje stejnou roli jako paměť samotná. V moderní technologické společnosti však dochází k popírání smyslu a hlavní funkce zapomnění, jelikož digitální paměť a permanence informací v digitálním světě tuto základní funkci znemožňují, případně výrazně znesnadňují tzv. „čerstvý začátek“ v případech, kdy je takové zapomnění výslovně žádoucí (jako např. zahlazení trestných činů nebo odstranění informací o trestním stíhání).

Význam zapomnění je tedy ještě posílen v prostředí internetu a obecně v kybernetickém světě, ve kterém data a informace existují permanentně a propojeně. V tomto prostředí by měl mít jednotlivec vždy právo kontrolovat informace o sobě přístupné, ledaže existuje jednoznačně převažující zájem jiné osoby či celé společnosti na tom, aby takové informace existovaly a byly dostupné. Tímto způsobem jsou váženy zájmy a práva jednotlivců i společnosti v dosavadní praxi Soudního dvora EU, který rozhodl, že plynutím času již společnost nemá nárok na přístup o bývalých exekucích (SDEU v případu Google Spain), zatímco v případech, kdy jsou informace (o úpadku) zveřejňované ve veřejném rejstříku v rozsahu a smyslu vyžadovaném takovým předpisem, je takové zveřejnění legitimní, i když může ovlivňovat další podnikatelskou činnost takové osoby (SDEU v případu Manni). Test proporcionality je navíc nezbytné provádět vždy, i když se jedná např. o zvláštní kategorie osobních údajů, nebo údaje o trestné činnosti (SDEU v případu GC a další). Německý Spolkový ústavní soud rovněž připomíná, že soukromí přitom nelze poměřovat jen se svobodou projevu, ale rovněž např. s oprávněnými zájmy tvůrce obsahu a právem na

podnikatelskou činnost. Právo být zapomenut tedy není absolutním právem a jeho aplikaci je vždy nezbytné poměřovat s dalšími základními lidskými právy – primárně tedy svobodou projevu, právem na informace, ale rovněž s právem na podnikatelskou činnost, případně dalšími možnými dotčenými zájmy (vlastnická práva či práva tvůrce obsahu).

Funkcí práva být zapomenut je tak ochrana jednotlivce, který by (obdobně, jako je tomu např. u zahlazení odsouzení) měl mít možnost „čerstvého začátku“, resp. aby byl plně chráněn nejen vůči veřejnosti, ale i vůči státu a jiným (konkrétním) osobám soukromého práva, kteří přinejmenším plynutím času ztrácejí až na výjimky legitimní zájmy na dispozici s takovými informacemi, které by mohly opodstatnit přístup k okruhu těmto informacím.

V souladu se závěry v kapitole 2 výše zároveň platí, že právo být zapomenut může náležet i právnickým osobám, nikoliv pouze jednotlivcům; zde naopak může být posílen význam jiných (ekonomických) zájmů na úkor ochrany soukromí.

6 Právo být zapomenut z hlediska ochrany osobních údajů[515]

6.1 Právo být zapomenut v legislativní úpravě

Právo na výmaz navazuje na dosavadní úpravu zakotvenou v čl. 12 písm. b) směrnice 95/46/ES. Český zákon o ochraně osobních údajů byl v tomto ohledu značně podrobnější než unijní úprava, kdy tato úprava byla do českého právního řádu zavedena v podobě povinnosti správce osobní údaje zlikvidovat ve smyslu § 4 odst. 1 písm. i) ZOOÚ a ve spojení s § 20 ZOOÚ v případě, že (i) pomine účel, pro který byly osobní údaje zpracovány, nebo (ii) na základě žádosti subjektu údajů.

---

[515] Text v této kapitole byl publikován jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 197 – 215.

Další použité literární zdroje v této kapitole:

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

MALDOFF, G., CIPP/US, Top 10 operational impacts of the GDPR, part 6 – RTFB and data portability, iapp.org, 25. 1. 2016.

WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European

NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3.

USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

Vodítka WP29 č. 225 ze dne 16. listopadu 2016 k implementaci rozsudku Soudního dvora Evropské unie ve věci Google Spain a Inc v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja Gonzáles

Ke zpracování osobních údajů bývalých zaměstnanců, ÚOOÚ dne 21. března 2013, https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=1585&n=ke-zpracovani-osobnich-udaju-byvalych-zamestnancu.

Právo na výmaz bylo zprofanované díky rozsudku SDEU ve věci Google Spain, díky kterému toto právo nabylo populární označení právo být zapomenut (angl. *right to be forgotten* nebo také *right to oblivion*). Ten se zabýval otázkou smazání veřejně dostupných údajů, které dále podroboval testu proporcionality mezi právem na ochranu soukromí a veřejným zájmem společnosti na přístup k určitému okruhu informací (k tomu viz kapitola 5.2.2 výše).

Právo na výmaz ve smyslu tohoto čl. 17 GDPR plynule navazuje na dosavadní úpravu a dále ještě posiluje postavení subjektů údajů, a to v návaznosti na ostatní povinnosti správce, které by měl plnit i bez ohledu na to, zda se subjekt údajů bude tohoto práva domáhat. Právo na výmaz tak v zásadě pouze pomáhá subjektu údajů, který se může domáhat, aby správce plnil své povinnosti – tedy aby v souladu se zásadou zákonnosti a zásadou minimalizace zpracovával vždy jen údaje nezbytné ke splnění určitého účelu, po dobu nezbytnou ke splnění tohoto účelu a vždy na základě platného právního základu (v souvislosti s ochranou osobních údajů často rovněž označovaného jako „právní titul"). V případě, kdy neplní tyto podmínky, je povinen se zdržet zpracování osobních údajů a tyto údaje vymazat (tj. „povinný výmaz"). Výmaz osobních údajů je tak často přímo zákonnou povinností správce, bez toho aniž by subjekt údajů uplatňoval žádost o výmaz svých údajů („výmaz na žádost"); ta je naopak spíše až sekundárním nástrojem toho, kdy by měl správce osobní údaje vymazávat. Subjekt údajů se tak prostřednictvím uplatnění práva na výmaz často domáhá již existujících povinností správce – resp. se domáhá toho, aby se správce zdržel takového zpracování, ke kterému již nemá žádný právní základ, a tyto údaje vymazal.

Vznik povinnosti vymazat osobní údaje, popř. uplatnění práva na výmaz, na druhou stranu může být i právním důsledkem uplatnění jiných práv dle nařízení. Povinnost vymazat osobní údaje tak zejména vzniká v případě, kdy subjekt údajů uplatní své právo na odvolání souhlasu[516] nebo pokud vznese námitky proti zpracování svých údajů[517], kde v případě, že neexistují jiné právní nebo převažující důvody, vzniká správci údajů povinnost osobní údaje bez dalšího

[516] Srov. čl. 17 odst. 1 písm. b) a písm. f) GDPR.

[517] Srov. čl. 17 odst. 1 písm. c) GDPR.

vymazat. Úzká souvislost rovněž existuje mezi uplatněním práva na omezení zpracování, kde se subjekt údajů může v případě nezákonného zpracování namísto výmazu domáhat právě omezení zpracování[518], a to zejména v případě, kdy subjekt údajů bude chtít napadat nezákonnost takového zpracování a od správce tak v zásadě žádá zachování důkazů nebo obecně požaduje zachování těchto údajů pro určení, výkon nebo obhajobu právních nároků[519]. Na druhou stranu rovněž v případě, kdy správci údajů vzniká povinnost aplikovat povinný výmaz, může přistoupit pouze k omezení zpracování osobních údajů namísto jejich výmazu, pokud tyto údaje potřebuje pro určení, výkon nebo ochranu vlastních nároků[520].

Obecně lze očekávat, že uplatňování práva na výmaz bude logickým důsledkem uplatnění práva na přístup, na základě kterého se subjekt údajů dozví, jaké údaje o něm správce zpracovává, a následně se bude domáhat jejich výmazu.

V každém případě má každý subjekt údajů v souladu s čl. 17 GDPR a ve spojení s čl. 12 právo po správci požadovat, aby vymazal jeho osobní údaje, resp. aby splnil své povinnosti a za splnění podmínek tyto osobní údaje vymazal[521], tj. může se dožadovat, aby správce přistoupil k výmazu na žádost, ovšem za předpokladu, že se neuplatní některá z výjimek dle čl. 17 odst. 3 GDPR. V případě, že správce některé osobní údaje zveřejnil a subjekt se dožaduje jejich výmazu, je správce navíc povinen o uplatnění tohoto práva informovat ostatní správce[522].

V případě, že dojde k výmazu (ať již povinnému nebo na žádost), je správce povinen o této skutečnosti informovat jednotlivé příjemce, jimž byly osobní údaje zpřístupněny, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí[523]. Ustanovení § 9 ZZOÚ navíc výslovně zakotvuje možnost tuto povinnost splnit úpravou údajů v evidenci, jejíž obsah je zveřejňován. Pokud

[518] Srov. čl. 18 odst. 1 písm. b) GDPR.

[519] Srov. čl. 18 odst. 1 písm. c). GDPR.

[520] Srov. čl. 18 odst. 2 GDPR.

[521] Srov. Čl. 17 odst. 1 GDPR.

[522] Srov. čl. 17 odst. 2 GDPR.

[523] Srov. čl. 19 GDPR.

tak správce např. zpřístupňuje data prostřednictvím API, postačí úprava v původní databázi bez dalších nezbytných notifikací.

Členské státy jsou v souladu s čl. 6 odst. 2 a 3 oprávněné stanovit konkrétní pravidla pro zpracování osobních údajů, které probíhá na základě právního základu plnění právní povinnosti [čl. 6 odst. 1 písm. c)] nebo plnění úkolu ve veřejném zájmu [čl. 6 odst. 1 písm. e)]. Taková specifická úprava může zahrnovat, kromě jiného, pravidla pro jednotlivé operace zpracování a postupy zpracování, jakož i další opatření k zajištění zákonného a spravedlivého zpracování. Český zákonodárce však této možnosti nevyužil.

Další specifická pravidla mohou být stanovena pro konkrétní oblasti v souladu s čl. 23 či čl. 85 a násl. Stanovení specifických pravidel v těchto oblastech pak může zahrnovat i konkrétní vymezení pravidel pro uplatnění práva na výmaz. Český zákonodárce však v ZZOÚ této možnosti nevyužil, a i v těchto specifických případech se tak postupuje zcela v režimu čl. 17.

6.2 Kdy vzniká povinnost vymazat údaje dle GDPR

6.2.1 Rozsah právní úpravy

V případě, že (i) je splněna alespoň jedna z podmínek stanovená v čl. 17 odst. 1 GDPR a zároveň (ii) není splněna některá z výjimek dle čl. 17 odst. 3 GDPR, je správce povinen bez zbytečného odkladu vymazat veškeré osobní údaje týkající se konkrétního subjektu údajů, a to bez ohledu na to, zda subjekt údajů uplatnil žádost o výmaz (dále také jen „***výmaz na žádost***“) nebo zda se jedná o případ výmazu z důvodu plnění zákonné povinnosti, resp. neexistence právního základu zpracování (dále také jen „***povinný výmaz***“).

V případě, že dojde k uplatnění práva na výmaz, je správce povinen žadatele identifikovat, a zjistit tak, že se skutečně jedná o subjekt údajů, jehož údaje mají být vymazány. Pokud nebude správce schopen subjekt údajů identifikovat, v souladu s čl. 11 jej o tom informuje, popř. jej informuje, že aby jej mohl prokazatelně identifikovat a přistoupit tak k výmazu, potřebuje od něj získat další údaje (srov. čl. 11 GDPR). Správce v takovém případě může v souladu s čl. 12 odst. 6 požádat o dodatečné údaje nezbytné k takové identifikaci.

Příklad:

Správci přijde žádost, ve které se bude Jan Novák dožadovat výmazu veškerých údajů, které o něm má společnost k dispozici. Vzhledem k tomu, že společnost má tři zaměstnance a další čtyři zákazníky s tímto jménem, není schopna bez dalšího subjekt údajů identifikovat a spolehlivě tak zajistit, že smaže jen jeho osobní údaje. V takovém případě si může požádat o poskytnutí více informací (nikoliv však nad rámec toho, co již sám zpracovává), aby mohl identitu subjektu dostatečně ověřit (ve smyslu čl. 12 odst. 6 GDPR). Pokud ani v takovém případě nebude celý rozsah informací dostatečný, lze žádost o výmaz odmítnout s poukazem na tuto skutečnost (ve smyslu čl. 11 odst. 2).

6.2.2 K pojmu „bez zbytečného odkladu“

Obecné nařízení o ochraně osobních údajů pro výmaz osobních údajů stanoví speciální lhůtu „bez zbytečného odkladu“. Ta se tedy uplatní jako lex specialis oproti obecné jednoměsíční lhůtě poskytované pro vyřízení ostatních práv, které nemají vymezenou žádnou zvláštní lhůtu. Správce by tak měl vyvinout v případě uplatnění žádosti o výmaz zvláštní úsilí k tomu, aby zajistil co nejdřívější výmaz. Obecná lhůta jednoho měsíce, která může být navíc v odůvodněných případech prodloužena až na tři měsíce (srov. čl. 12 odst. 3), se pak uplatní subsidiárně jako maximální časový rámec, během kterého je správce povinen žádost vyřídit.

Druhým rozměrem této lhůty je povinný výmaz. Jelikož se nejedná o výmaz na žádost, nelze aplikovat obecnou jednoměsíční lhůtu. Naopak – v případě, že vznikne událost, která správci zakládá povinnost údaje vymazat, musí tento povinný výmaz provést bez zbytečného odkladu. Pokud tak neučiní a bude údaje i nadále zpracovávat, bude jednat v rozporu s GDPR, jelikož nebude mít právní základ pro takové zpracování (naopak, pokud by měl, nejednalo by se o případ povinného výmazu).

6.2.3 Výmaz osobních údajů, včetně jejich anonymizace

GDPR jakožto technologicky neutrální předpis nevymezuje, co přesně znamená výmaz a jakým způsobem má probíhat. Částečně návodné tak může být dosavadní vymezení likvidace osobních údajů ve smyslu § 4 písm. i) ZOOÚ, kterou se

rozumí fyzické zničení nosiče osobních údajů, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování. Likvidací osobních údajů se tak podle stávajícího výkladu rozumí nezvratná operace směřující k vyloučení osobních údajů z aktivního zpracování.

Použitá metoda výmazu by neměla být rozhodující, rozhodující je jen výsledek – tedy že osobní údaje již nebudou nadále použitelné, resp. nebudou naplňovat definici osobního údaje – nebudou ani potenciálně způsobilé k identifikaci fyzické osoby. Aby bylo možné osobní údaje považovat za vymazané, nemělo by být možné je obnovit bez vynaložení nadměrného úsilí. Na jedné straně tak zajisté nepostačí pouhé „přesunutí do koše“ na ploše počítače (ze kterého lze data bez dalšího obnovit), ale zároveň by se nemělo bez dalšího dovozovat porušení povinnosti správce vymazat data, pokud je tato data možné obnovit pouze za vynaložení nadměrného úsilí a např. při použití specializovaného softwaru. Je tak zjevné, že existují rizika spojená s možností obnovy nedůsledně smazaných dat z prostředků výpočetní techniky, neboť takto provedené smazání dat neznamená jejich faktickou likvidaci. Domnívám se však, že by bylo nepřiměřené na každého správce bez dalšího aplikovat povinnost zajistit absolutní nemožnost obnovy takových údajů, a způsob likvidace dat nebo jejich nosičů by tedy měl být vždy dovozován a prováděn s ohledem na technologické možnosti povinného subjektu.

Opačný výklad takového zpracování by byl pro některé správce zjevně nepřiměřený a rovněž by popíral obecné principy, ze kterých jinak GDPR vychází – tedy přístupu vycházejícího z hrozícího rizika (v angl. *risk-based approach*), který GDPR výslovně uplatňuje např. na povinnost dostatečného zabezpečení údajů dle čl. 32. Pro výběr a zavedení určitých technických a organizačních opatření tak nařízení stanoví, že se mají zavádět *„s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům.“* Domníváme se, že tento přístup lze analogicky aplikovat i při výmazu osobních údajů. V případě, kdy správce neprovádí žádné extenzivní zpracovatelské operace, by bylo zjevně nepřiměřené a v rozporu s ostatními povinnostmi GDPR, pokud by si měl správce pro jinak standardní agendu zajistit specializované softwarové nástroje, které by zajistily definitivní a nijak nevratný výmaz a které by v kontextu jiných

povinností, např. zavádění technických a organizačních opatření dle čl. 32 GDPR, vůči správci působily zcela neadekvátně.

S problematikou toho, co znamená finální výmaz, velmi úzce rovněž souvisí otázka, odkud je nezbytné údaje mazat, zda se má výmaz promítnout jen do aktivně používaných databází, nebo zda je nutné mazat např. i zálohy osobních údajů na nepřepisovatelných nosičích, aj. Nařízení k tomu nenabízí žádnou odpověď a povinností správce je tak v zásadě vymazat veškeré osobní údaje, které má o subjektu údajů k dispozici.

Výmazem údajů se tak rozumí učinění osobních údajů nepoužitelnými, a to takovým způsobem, který správci, zpracovateli nebo jakékoliv jiné osobě znemožní přístup, nakládání či jiné zpracování těchto osobních údajů bez ohledu na to, zda takový úkon technicky spočívá ve výmazu dat z jejich nosiče nebo ve fyzické likvidaci dat či jejich nosiče.

Domnívám se, že za výmaz osobních údajů lze přiměřeně považovat i jejich anonymizaci, popř. výmaz identifikátorů u pseudonymizovaných údajů (a tím pádem jejich anonymizaci – tento krok bude pro správce technologicky snazší, jelikož k oddělení identifikátorů došlo již před žádostí o výmaz/vzniku povinnosti vymazat osobní údaje). Správce v takovém případě musí vymazat všechny informace umožňující přímou i nepřímou identifikaci subjektu údajů a musí zajistit, že údaje budou natolik anonymizované, že subjekt údajů nebude moci být skutečně identifikovatelný[524]. Prostředky anonymizace musí být zvoleny s přihlédnutím k významu uchovávaných údajů a rizikům plynoucím z jejich případného zneužití.[525] Jakmile správce osobní údaje anonymizuje, přestane se jednat o zpracování osobních údajů ve smyslu GDPR a nakládání s nimi tak nadále nebude podléhat pravidlům GDPR. I anonymizace je sama o sobě (obdobně jako výmaz) samotnou zpracovatelskou operací – byť konečnou, která tedy bez dalšího vede k znehodnocení/likvidaci dat ve smyslu osobních údajů;

[524] K pojmu anonymizace srov. kapitolu 3.1.5 této práce.

[525] RÁMIŠ, V. in UŘIČAŘ, Miroslav a Vladan RÁMIŠ. Obecné nařízení o ochraně osobních údajů: komentář. Praha: C. H. Beck, 2021, xxvii, 1386. ISBN 978-80-7400-815-3, s. 512-537.

správce by se tak měl anonymizace zdržet např. v případě, že se uplatní podmínky pro omezení zpracování dle čl. 18 GDPR.

Obdobný výklad pojmu „výmaz“ se uplatní i na povinnosti zpracovatele vymazat osobní data v případě ukončení zpracovatelského vztahu (tj. v případě ukončení zpracovatelské smlouvy) ve smyslu čl. 28 odst. 2 písm. g) GDPR.

6.2.4 Důvody pro výmaz

V případě, že se neuplatní některá výjimka dle odst. 3, je správce povinen osobní údaje vymazat v následujících případech:

6.2.4.1 Naplnění účelu zpracování osobních údajů

Podle čl. 17 odst. 1 písm. a) GDPR platí, že správce je povinen vymazat údaje, pokud *„osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány“*.

Jedním z hlavních důvodů, které jsou základní podmínkou pro uplatnění práva na výmaz, je splnění účelu, pro který byly osobní údaje shromážděny nebo jinak zpracovávány. Tato povinnost tak vyplývá z obecné zásady zákonnosti zpracování a minimalizace osobních údajů. Časový okamžik naplnění původního účelu zpracování často bude shodný s okamžikem ukončení právního titulu zpracování – např. splnění smlouvy, uběhnutí doby, na kterou byl získán souhlas, splnění zákonné povinnosti aj. V takovém případě se aplikuje povinný výmaz a správce je povinen vymazat osobní údaje bez dalšího (ledaže vznikne jiný účel, který je slučitelný s účelem původním, a správce zároveň bude mít právní titul pro takové zpracování – může se tak jednat např. o zpracování nezbytné pro obhajobu a výkon vlastních nároků na základě oprávněného zájmu nebo o zpracování osobních údajů na daňových dokladech na základě plnění zákonných povinností správce dle zákona o účetnictví či zákona o DPH).

Ustanovení čl. 17 GDPR se však nevztahuje pouze na případy povinného výmazu – tj. na případy, kdy správce již nadále nedisponuje s právním základem zpracování ve smyslu čl. 6 odst. 1 GDPR. Dopady ustanovení čl. 17 GDPR jsou širší, když stanoví, že k výmazu osobních údajů dojde, pokud tyto již nejsou potřebné pro účely. Nařízení tím otevírá možnost pro subjekty údajů dožadovat se

výmazu na žádost, a to i v případě, kdy správce údajů i nadále formálně disponuje právním titulem ke zpracování. I v takovém případě má však subjekt údajů možnost prokázat, že již došlo k naplnění účelu a samotný právní titul tak nadále neopodstatňuje to, aby správce nadále disponoval s osobními údaji. I v takovém případě správci na základě uplatněné žádosti vznikne povinnost údaje vymazat. Faktické možnosti takového uplatnění práva na výmaz jsou však spíše omezené, a pro výmaz na žádost se tak uplatní zejména důvody dle dalších ustanovení tohoto čl. 17 odst. 1 GDPR.

6.2.4.2 Odvolání souhlasu

Podle čl. 17 odst. 1 písm. b) GDPR platí, že správce je povinen vymazat údaje, pokud subjekt údajů odvolá svůj souhlas, na jehož základě byly v souladu s ostatními podmínkami GDPR zpracovávány jeho osobní údaje; a pokud neexistuje žádný další právní důvod pro zpracování.

V případě, že subjekt údajů odvolá svůj souhlas se zpracováním osobních údajů, automaticky tím správci vzniká povinnost vymazat osobní údaje, které na základě tohoto právního titulu dosud zpracovával. V zásadě se tak jedná o další případ povinného výmazu, jelikož v okamžiku, kdy subjekt údajů odvolá svůj souhlas, správce je povinen – aniž o to subjekt údajů výslovně žádá – bez dalšího jeho osobní údaje vymazat. Pokud by tyto údaje nevymazal, jednal by v rozporu s nařízením, jelikož by údaje zpracovával bez validního právního titulu.

Povinnost vymazat údaje se však uplatní pouze za předpokladu, že správce nemá jiný právní titul pro zpracování osobních údajů tohoto subjektu údajů – může se tak jednat o jiný souhlas (pro jiný účel), smlouvu, zákonnou povinnost či jiný titul dle čl. 6 odst. 1 GDPR.

Povinnost vymazat údaje se uplatní bez ohledu na to, zda subjekt údajů odvolá svůj souhlas se zpracováním „běžných“ osobních údajů [dle čl. 6 odst. 1 písm. a) GDPR] nebo souhlas se zpracováním zvláštních kategorií osobních údajů [dle čl. 9 odst. 1 písm. a) GDPR]. Pokud jsou splněny ostatní podmínky, správce bude povinen vymazat veškeré takové údaje, pro které nemá jiný titul zpracování.

Příklad:

Subjekt údajů odvolá souhlas se zasíláním marketingových sdělení ohledně novinek na e-shopu na svou e-mailovou adresu. Subjekt údajů je však pravidelným zákazníkem tohoto e-shopu, a proto si zde vytvořil uživatelský účet. Ačkoliv subjekt údajů odvolá svůj souhlas se zasíláním marketingových novinek, provozovatel e-shopu tuto e-mailovou adresu (a popř. další údaje) i nadále potřebuje pro udržení uživatelského konta a tuto e-mailovou adresu proto nesmaže – pouze ji vyřadí (tedy vymaže) z databáze příjemců marketingových sdělení.

Rovněž připomínáme, že odvolání souhlasu by vždy mělo být v zásadě stejně snadné jako jeho udělení, jak vyplývá z čl. 7 odst. 3 GDPR.

6.2.4.3 Neexistující převažující právní důvody po vznesení námitek

V případě, kdy je zpracování založeno na právním titulu oprávněného zájmu [čl. 6 odst. 1 písm. f) GDPR] nebo veřejného zájmu [čl. 6 odst. 1 písm. e) GDPR], má subjekt údajů právo podat námitky podle čl. 21 odst. 1. Subjekt údajů by měl při uplatnění námitek předložit okolnosti, které odůvodňují, že jeho oprávněný zájem převažuje nad oprávněným/veřejným zájmem správce; přesto důkazní břemeno o tom, že stále existují převažující oprávněné zájmy, nese správce. Pokud jsou námitky úspěšné, tj. správce neprokáže, že původní oprávněný zájem stále trvá, tedy že správce nemá nadále právní titul pro takové zpracování, je správce povinen bez dalšího provést povinný výmaz takto zpracovávaných osobních údajů.

Správce má však možnost prokázat, že i nadále existují oprávněné důvody/zájmy, které převažují nad zájmy tohoto subjektu údajů, a tedy že i nadále má dostatečný právní titul pro zpracování příslušných osobních údajů tohoto subjektu.

Posuzování správce, zda i nadále existují jeho převažující zájmy, může být časově náročné. Proto se od okamžiku vznesení námitky [resp. uplatnění žádosti na výmaz dle tohoto čl. 17 odst. 1 písm. c)], automaticky uplatní povinnost omezit zpracování [podle čl. 18 odst. 1 písm. d)]. Správce po dobu, po kterou bude posuzovat oprávněnost tohoto zpracování, nebude oprávněn s namítanými údaji nakládat (k tomu srov. čl. 18 GDPR). Nařízení tak pro případy zpracování na základě oprávněného/veřejného zájmu v zásadě přináší presumpci nezákonnosti

takového zpracování, kde přenáší důkazní břemeno na správce. Pokud správce takové důkazní břemeno neunese, je povinen osobní údaje vymazat.

Správce však nemá možnost argumentovat převažujícím zájmem v případě, že údaje na základě oprávněného zájmu zpracovával pouze za účelem přímého marketingu. V takovém případě se jedná o námitky dle čl. 21 odst. 2 a správce je v souladu s čl. 17 GDPR ustanovením spolu s čl. 21 odst. 3 povinen údaje bez zbytečného odkladu vymazat, aniž by měl možnost jakkoliv dále obhajovat oprávněnost takového zpracování.

6.2.4.4 Protiprávní zpracování osobních údajů

Podle čl. 17 odst. 1 písm. d) GDPR se subjekty údajů mohou dovolávat práva na výmaz v případě, kdy osobní údaje tohoto subjektu údajů byly zpracovány protiprávně.

GDPR přitom nestanovuje další podmínky toho, co znamená, že údaje byly *„zpracovávány protiprávně“* (angl. *unlawfully processed*, něm. *unrechtmäßig verarbeitet*).

V zásadě se tak nabízí dva možné výklady: (i) protiprávním zpracováním se rozumí takové zpracování, které není zákonné, tj. správce zpracovává osobní údaje bez právního titulu – v rozporu s podmínkami čl. 6, nebo (ii) protiprávním zpracováním se rozumí jakékoliv porušení GDPR (nebo jiných předpisů) ze strany správce při zpracování osobních údajů.

Gramatický výklad českého znění tohoto ustanovení a pojmu „protiprávně“ indikuje, že právo na výmaz vzniká v okamžiku jakéhokoliv porušení GDPR a/nebo jiného právního předpisu při zpracování osobních údajů. Tomuto nasvědčuje i bod 65 odůvodnění, podle kterého má subjekt údajů právo na výmaz, „pokud uchovávání těchto údajů porušuje toto nařízení nebo právo Unie či členského státu, které se na správce vztahuje.“ Obdobný závěr bez dalšího přijali někteří zahraniční i tuzemští autoři.

Např. P. Voigt se domnívá, že čl. 17 odst. 1 písm. d) GDPR ustanovení lze považovat za všezahrnující klauzuli, která zaručuje subjektu údajů právo na výmaz v případě, kdy je zpracování osobních údajů protiprávní mj. z důvodu

rozporu s GDPR, jako je např. nezavedení dostatečných organizačních a technických opatření.[526]

V souladu s bodem 65 odůvodnění rovněž vykládají čl. 17 odst. 1 písm. d) GDPR ustanovení tuzemští autoři, podle kterých protiprávní zpracování znamená, že osobní údaje jsou zpracovány v rozporu s nařízením, ale případně i s jakýmkoliv právním předpisem EU nebo předpisem členského státu, který se na správce vztahuje.[527]

Na základě gramatického výkladu ustanovení 17 odst. 1 písm. d) GDPR se domnívám, že se takto široký výklad neuplatní. Ačkoliv česká jazyková verze GDPR používá výraz protiprávně, ostatní jazykové verze nařízení hovoří o nezákonném zpracování. Nařízení přitom v čl. 6 odst. 1 jednoznačně definuje, co se rozumí zákonným zpracováním, tedy pokud je zpracování založeno na validním právním titulu (čl. 6 odst. 1 stanoví, že „zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu“). Výkladem a contrario pak platí, že zpracování je nezákonné, pokud není splněna ani jedna z podmínek stanovených v čl. 6 odst. 1.

K tomu srov. jednotlivé jazykové verze:

	Čl. 17 odst. 1 písm. d)	**Čl. 6 odst. 1**
česky	osobní údaje byly zpracovány **protiprávně**	Zpracování je **zákonné**
slovensky	osobné údaje sa spracúvali **nezákonne**	Spracúvanie je **zákonné**
anglicky	the personal data have been	Processing shall be **lawful**

[526] Srov. VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7, s. 158.

[527] Srov. NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3, s. 231.

	unlawfully processed	
německy	die personenbezogenen Daten wurden **unrechtmäßig** verarbeitet	Die Verarbeitung ist nur **rechtmäßig**
francouzsky	les données à caractère personnel ont fait l'objet d'un traitement **illicite**	Le traitement n'est **licite** que si

Vzhledem ke gramatickému výkladu ostatních jazykových verzí GDPR by pak mělo platit, že ustanovení čl. 17 odst. 1 písm. d) GDPR se vztahuje především na takové zpracování, které není zákonné, tedy na případy, kdy správce údajů nedisponuje žádným právním titulem pro zpracování osobních údajů a měl by bez dalšího uplatnit povinný výmaz.

Na druhou stranu je třeba připustit, že omezovat výklad podmínky výmazu pouze na případy zpracování bez právního titulu může být příliš restriktivní – tyto případy jsou zároveň pokryty písm. a), b) a c). S přihlédnutím k bodu 65 odůvodnění, který však pojednává pouze o uchovávání údajů, nikoliv o jakémkoliv zpracování, se domníváme, že ustanovení čl. 17 odst. 1 písm. d) GDPR slouží jako určitý korektiv jednání správce. Pokud by tedy zpracovatelské operace prováděné správcem dosáhly takové intenzity, že by byly v rozporu se všemi ostatními principy nařízení dle čl. 5, lze připustit, že by se subjekt údajů mohl domáhat výmazu osobních údajů na základě tohoto ustanovení. Takové porušování podmínek obecného nařízení o ochraně osobních údajů, které může být podmínkou výmazu osobních údajů dle čl. 17 odst. 1 písm. d) GDPR, je však nezbytné vykládat restriktivně a musí dosahovat značné intenzity.

V opačném případě, kdybychom dovozovali, že jakékoliv porušení pravidel pro zpracování osobních údajů dle GDPR může znamenat porušení ochrany osobních údajů, by tak ad absurdum znamenalo, že správce je např. povinen smazat veškeré údaje subjektu údajů jen z toho důvodu, že jej nedostatečně informoval dle čl. 13 a/nebo pouze z toho důvodu, že nejmenoval pověřence pro ochranu osobních údajů, ač byla naplněna některá z podmínek dle čl. 37. Domnívám se, že taková

podmínka by byla pro správce zjevně nepřiměřená a není v souladu s úmyslem zákonodárce.

6.2.4.5 Výmaz údajů pro splnění právní povinnosti

Podle čl. 17 odst. 1 písm. e) GDPR platí, že osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje.

Správce je rovněž povinný vymazat osobní údaje týkající se subjektu údajů, pokud mu to přikazují národní předpisy nebo ustanovení práva EU.

V souvislosti s tímto ustanovením není zcela jasné, zda je cílem tohoto ustanovení umožnit členským státům, aby přijaly speciální ustanovení týkající se práva na výmaz.

Vzhledem k systematice nařízení, které možnosti derogace obvykle doprovází výslovným zmocněním pro úpravu ze strany členských států (členské státy mohou, členské státy uvedou apod.), se domníváme, že se nejedná o blanketní zmocnění členských států přijmout libovolnou úpravu povinností, které by směřovaly k výmazu dat. Jedná se tak spíše o okrajové ustanovení, které předpokládá existenci jiných povinností, které mohou zahrnovat, kromě jiného, i povinnost vymazat osobní údaje.

6.2.4.6 Zpracování osobních údajů nezletilých

Správce osobních údajů má dále podle čl. 17 odst. 1 písm. f) GDPR povinnost osobních údaje vymazat, pokud byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 GDPR. Pokud byly údaje shromážděny od subjektu, který byl v době získání těchto údajů dítětem ve smyslu GDPR (tj. mladistvým do věku 13–16 let v závislosti na národní úpravě ve smyslu čl. 8), má takový subjekt údajů právo požádat výmaz těchto údajů, a to i pokud (resp. zejména i pokud) již přesáhl tuto věkovou hranici – 13–16 let dle národní úpravy (v ČR tedy dovršením 15 let ve smyslu § 7 ZZOÚ).

Zákonodárce tak míří na případy, kdy dochází ke zpracování osobních údajů dítěte na základě souhlasu (dle čl. 8 odst. 1). Takové dítě si však nemuselo (vzhledem ke své rozumové vyspělosti) být vědomo důsledků udělení souhlasu,

resp. takový souhlas za něj mohli udělit jeho rodiče, a to dokonce bez vědomí tohoto dítěte. Je proto v souladu s jeho právy na ochranu soukromí a ochranu osobních údajů, aby se mohlo bez dalšího domáhat výmazu svých osobních údajů.

Tím samozřejmě nejsou dotčeny povinnosti správce, který měl vždy postupovat se zvýšenou obezřetností, pokud se jedná o zpracování osobních údajů dítěte (tím spíše v online prostředí). Ustanovením čl. 17 odst. 1 písm. f) GDPR zároveň není dotčeno právo subjektu údajů odvolat souhlas. V takovém případě se bude jednat o povinný výmaz a správce tak bude postupovat dle čl. 17 odst. 1 písm. b) GDPR.

6.3 Pozitivní vymezení práva být zapomenut (pro zveřejněné údaje)

6.3.1 Vymezení aplikační roviny práva být zapomenut

Podle čl. 17 odst. 2 GDPR platí: *„Jestliže správce osobní údaje zveřejnil a je povinen je podle odstavce 1 vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.“*

Ustanovení čl. 17 odst. 2 GDPR je tak v zásadě konsekvencí povinností vymezených v čl. 17 odst. 1 GDPR, přičemž v zásadě posiluje ochranu osobních údajů v online prostředí.[528] Povinnosti stanovené v čl. 17 odst. 2 GDPR jednoznačně navazují na rozhodnutí SDEU ve věci Google Spain, který je blíže analyzován v kapitole 5.2.2 této práce. Nicméně obecné nařízení o ochraně osobních údajů v zásadě přesahuje dosavadní úpravu, kterou původně formuloval SDEU v tomto rozsudku Google Spain. Ustanovení čl. 17 odst. 2 GDPR totiž navíc ukládá správci povinnosti týkající se informování dalších osob (obdobná obecná povinnost informovat příjemce je zakotvena v čl. 19 GDPR). Ačkoliv se tak původní rozhodnutí SDEU se věci Google Spain zaobíralo primárně vyhledávacími nástroji (search engine), GDPR nad rámec původní úpravy stanoví,

[528] VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7, s. 351.

že je možné dožadovat se uplatnění práva na výmaz u všech správců, kteří nakládají s osobními údaji tohoto subjektu údajů – tím GDPR rozšiřuje výklad nad rámec dosavadních vyhledávacích nástrojů. Podmínkou zůstává, že se jedná o zveřejněné osobní údaje.

Jedná se o specifický dopad práva na výmaz zejména ve vztahu k online prostředí. Aby se uplatnila povinnost správce, musí subjekt alespoň implicitně naznačit, že si přeje úplné vymazání daného osobního údaje ze všech zdrojů. Takový požadavek pak zahrnuje všechny správce tohoto údaje.

6.3.2 K pojmu „zveřejnil“

Podmínkou povinnosti správce přijmout tyto dodatečné kroky (nad rámec čl. 19) je zveřejnění osobních údajů ze strany správce. Za zveřejnění se tak považuje zpřístupnění osobních údajů předem nedefinovanému počtu osob. Typickým příkladem takového zveřejnění je umístění osobních údajů na webové stránky, jako tomu bylo např. v případě Google Spain nebo rozhodnutí Krajského soudu v Brně[529].

Podmínkou výmazu je stále, že tyto osobní údaje byly zveřejněny správcem (popř. jeho zpracovatelem, pokud tak učinil na základě pokynů správce). Správci povinnost jednat v souladu s čl. 17 odst. 2 GDPR nevzniká, pokud zpracovává údaje, které byly zveřejněné jinou osobou.

6.3.3 Přiměřené kroky k výmazu odkazů na osobní údaje, jejich kopie či replikace

V případě uplatnění čl. 17 odst. 2 správci vzniká povinnost přijmout přiměřené kroky k informování dalších správců, kteří tyto zveřejněné údaje zpracovávají, a to s ohledem na dostupnou technologii a náklady na provedení, včetně technických opatření.

Nařízení nestanoví přesnou formu, jak by měl správce údajů v takové situaci postupovat. Stanoví však subjektivní podmínku, že musí přijmout takové kroky, které pro něj budou přiměřené – tj. nebudou pro daného správce představovat

[529] Usnesení Krajského soudu v Brně ze dne 7. října 2015, sp. zn. 70 Co 228/2015 – 38.

příliš velkou zátěž, resp. nevyžadují od správce implementace speciálních technologií, které by zabránily jakémukoliv dalšímu zpracování.

Naopak, pokud správcem, který údaje zveřejnil, bude technologická společnost, zřejmě se očekává, že přijme dostačující kroky (tj. technická opatření), které zabrání dalšímu zpracování ze strany dalších správců, kteří mohli dosud osobní údaje tohoto subjektu údajů také zpracovávat (např. je informuje, zablokuje jejich přístup k takovým údajům v systému či např. znepřístupní svoje API, prostřednictvím kterých docházelo k přístupu do databáze údaje či systémů správce).

Musí se tedy jednat o výmaz „odkazů na tyto osobní údaje, jejich kopie či replikace“ Obecné nařízení tuto povinnost nijak dále nespecifikuje. Např. německé doktrína pak dovozuje, že se musí jednat o výmazy všech odkazů na jakékoliv myslitelé úložiště, kde jsou uloženy osobní údaje, které mají být vymazány. Zároveň by se mělo jednat i o odkazy, které odkazují na jiné úložiště než to, kde byla data původně publikována. Vymazat je rovněž třeba všechny „kopie“ a „replikace“, čímž zákonodárce dává jasně najevo, že mají být vymazány nejen přesné kopie předmětných dat, ale také snímky, které přesně neodpovídají originálu, ale z nichž data v příslušných datech lze extrahovat informace obsažené v datech nebo dokonce jejich část.[530]

6.4 Negativní vymezení aplikačního dopadu práva být zapomenut

6.4.1 Vymezení podmínek stanovených v GDPR

I v případě, že je splněna některá z podmínek pro uplatnění práva na výmaz dle odst. 1 (bez ohledu na to, zda se jedná o povinný výmaz nebo výmaz na žádost), nařízení poskytuje výjimky, kdy se právo na výmaz neuplatní. V případě, že subjekt zažádá o výmaz svých osobních údajů a správce vyhodnotí, že se na něj vztahuje některá z výjimek dle tohoto odst. 3, informuje o této skutečnosti subjekt

[530] HERBST. Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“). KÜHLING a BUCHNER. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. 2. vydání. 2018. ISBN 978-3-406-74994-0, s. 89-94.

údajů (srov. čl. 12 GDPR). Pokud by subjekt údajů s uplatněním takové výjimky nesouhlasil, má možnost se obrátit se stížností na dozorový úřad.

6.4.2 Výkon práva na svobodu projevu a informace

Na správce osobních údajů se nevztahuje povinnost vymazat údaje, pokud je zveřejnil v souvislosti s právem na svobodu projevu (např. tedy v oblasti žurnalistiky) nebo jako projev práva na informace (např. veřejné rejstříky či v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím).

Ani uplatnění této výjimky však není absolutní – správce by měl provést proporční test mezi právem na soukromí subjektu údajů a těmito právy. Některé údaje mohou rovněž stárnout v čase a, i přes původní uplatnění této výjimky, tak mohou být údaje po určité době neaktuální a nepřesné. V takovém případě se výjimka v čase neuplatní a správce bude muset osobní údaje subjektu rovněž vymazat, i když původně byly zveřejněné např. v rámci svobody projevu (tedy např. v rámci novinového článku). V zásadě tak platí, že čím starší údaje jsou, tím menší je uplatnitelnost této výjimky.

Uplatnění této výjimky se rovněž může lišit mezi členskými státy, a to v závislosti na tom, zda a jakou přijmou národní úpravu dle čl. 85; ZZOÚ v souladu s tímto článkem obsahuje úpravu pro zpracování osobních údajů prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu (srov. čl. 85 GDPR).

V určitých případech tak platí, že nad právem na ochranu soukromí a osobních údajů může převážit právo veřejnosti na informace – a to zejména v případě veřejných rejstříků. SDEU se otázkou proporcionality pro takové případy zabýval v rozsudku Manni, ve kterém stanovil, že legitimní zájem třetích osob na informace z veřejného (obchodního či insolvenčního) rejstříku a úmysl zajistit právní jistotu, poctivost v obchodních vztazích a řádné fungování vnitřního trhu obvykle převáží nad individuálním zájmem dotčené osoby na ochranu soukromí. Nevyloučil však, že v konkrétní situaci mohou existovat závažné důvody, které mohou výjimečně odůvodnit výmaz daných osobních údajů po uplynutí přiměřené doby. SDEU tak potvrdil, že i v případě, že určitý set údajů naplní výjimku pro právo na informace a svobodu projevu, tato ochrana může slábnout v čase a netrvá

tak absolutně po neomezeně dlouhou dobu. Správci by tak měli po určité době při uplatnění práva na výmaz při aplikaci této výjimky provádět test proporcionality mezi právem na ochranu soukromí a osobních údajů a právem na informace a svobodu projevu.

Dle stanoviska WP29 k rozsudku Google Spain je i v případě zájmu veřejnosti na informace v souvislosti s vyhledáváním informací na internetu třeba uplatnit test proporcionality a zajistit tak rovnováhu mezi právem na informace a právem na soukromí. Výsledek proporčního testu tak bude záviset zejména na charakteru a citlivosti zpracovávaných údajů, což může být ovlivněno také postavením subjektů údajů ve veřejném životě.

Za subjekty, které plní roli ve veřejném životě, lze považovat např. politiky, vedoucí úředníky, významné podnikatele či členy regulovaných profesí. Ve vztahu k těmto osobám lze předpokládat zájem veřejnosti na možnosti vyhledat relevantní informace související s jejich uplatněním ve veřejném životě. Užitečným pravidlem ke stanovení rovnováhy mezi právem společnosti na informace a právem veřejně činné osoby na soukromí je posouzení, zda zveřejnění daných informací může pomoci předejít nevhodnému profesnímu chování těchto veřejně činných osob, tedy zda zveřejnění informací usnadňuje jakousi kontrolu veřejnosti. Obdobné posouzení bude třeba provést také v případě veřejně známých osobností, u nichž lze předpokládat míru mediální známosti, a tedy zvýšeného zájmu veřejnosti z důvodu jejich postavení ve společnosti. Obecným korektivem v takovém případě vždy bude úprava ochrany osobnosti ve smyslu § 81 a násl. občanského zákoníku.

6.4.3 Plnění právní povinnosti

pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen

Účelem této výjimky je zajistit, aby správce nemusel osobní údaje vymazat, pokud se na něj uplatní zákonná povinnost údaje po určitou dobu uchovávat, tedy zejména v případech, kdy jsou tyto retenční lhůty stanovené právním předpisem. Typicky jsou tyto povinnosti (často vč. retenčních lhůt) stanoveny daňovými,

účetními nebo pracovněprávními předpisy či zákonem o archivnictví. Speciální lhůty jsou ale také často stanoveny sektorovými regulacemi (včetně zdravotnického a finančního sektoru).

Tato výjimka se uplatní i v případě, že správce původně údaje zpracovával na základě jiného právního titulu, než je plnění právní povinnosti, avšak tato povinnost mu vznikla později.

Typickým příkladem tak může být situace, kdy správce získal a zpracovával údaje subjektu údajů za účelem splnění (kupní) smlouvy. Správci však zároveň vznikne povinnost dle daňových a účetních předpisů uchovat daňový doklad (např. retenční doba uchování daňových dokladů dle zákona o DPH[531] je 10 let od konce zdaňovacího období – a to včetně povinně uváděných osobních údajů) i s osobními údaji tohoto subjektu údajů. Uchování těchto daňových dokladů tak bude probíhat na základě zákonné povinnosti a na správce se nevztahuje povinnost po zákonem stanovenou dobu tyto údaje vymazat. Na druhou stranu je však správce povinen zajistit výmaz těchto údajů po uplynutí zákonné retenční lhůty, jelikož pro další zpracování již nebude mít žádný právní titul.

6.4.4 Důvody veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3

Výjimka je určena pro některá zpracování založená na veřejných zájmech státu či EU souvisejících se zdravotnictvím a veřejným zdravím. Konkrétními účely zpracování jsou dle odkazovaného článku 9 preventivní či pracovní lékařství, poskytování zdravotní nebo sociální péče nebo léčby, ochrana před přeshraničními zdravotními hrozbami atd.

Dle GDPR se v této oblasti předpokládá zajištění odpovídající ochrany osobních údajů subjektů zákonnými předpisy, včetně např. povinnosti mlčenlivosti lékařů a dalšího personálu. V českém právním řádu jsou zvláštní povinnosti, zejména v souvislosti s vedením zdravotnické dokumentace, stanoveny zákonem o

[531] Podle § 35 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“), platí, že daňové doklady se uchovávají po dobu 10 let od konce zdaňovacího období, ve kterém se plnění uskutečnilo. Ustanovení § 29 zákona o DPH dále stanovuje taxativní výčet náležitostí, které daňový doklad musí obsahovat.

zdravotních službách, vyhláškou o zdravotnické dokumentaci a dalšími prováděcími předpisy.

Tato výjimka se v českém právním prostředí velmi překrývá s výjimkou pro plnění zákonné povinnosti dle písm. b) výše. V případě, kdy správce zpracovává osobní údaje na základě některých povinností dle sektorových předpisů pro oblast zdravotnictví, není povinen (a mnohdy tedy ani oprávněn) po dobu trvání těchto povinností osobní údaje mazat.

6.4.5 Archivace ve veřejném zájmu a výzkum

pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování

Právo na výmaz se neuplatní v případě, že jsou kumulativně splněny dvě podmínky:

a) Zpracování osobních údajů probíhá za účelem archivace pro vymezené zájmy nebo pro statistické účely v souladu s čl. 89 odst. 1. Může se tak jednat např. o zpracování na základě zákona č. 499/2004 Sb., o archivnictví a spisové službě, zákona č. 89/1995 Sb., o státní statistické službě, nebo případně na základě některých zákonů o sčítání lidu.

b) V případě, že by byly osobní údaje vymazány, je pravděpodobné, že by takový výmaz znemožnil nebo vážně ohrozil splnění primárních cílů archivace nebo statistických záměrů.

Toto ustanovení tak komplementárně souvisí s čl. 89 a zároveň s principy ochrany osobních údajů dle čl. 5 odst. 1 písm. b), který předpokládá, že lze osobní údaje za účelem archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely zpracovávat vždy bez ohledu na původní účel zpracování těchto údajů.

V případě, že správce uplatní vůči výmazu osobních údajů tuto výjimku, bude muset především obhájit, že v případě, že by údaje vymazal, bylo by vážně ohroženo nebo zcela znemožněno dosažení původního cíle tohoto zpracování. Je

však dostačující, že správce dokáže, že je takové ohrožení nebo znemožnění pravděpodobné.

6.4.6 Určení, výkon nebo obhajobu právních nároků

Správce není povinen osobní údaje vymazat, pokud je jejich zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků (a de facto tak existuje oprávněný zájem na takovém uchování).

Subjekty údajů se tak nemohou dožadovat výmazu osobních údajů, které by mohly být nezbytné pro uplatnění (budoucích) právních nároků správce a bez jejichž uplatnění by správce nebyl schopen prokázat tyto nároky. Pokud by se mělo uplatnit právo na výmaz i vůči takovým údajům, jednalo by se o zjevný nepřiměřený zásah do práv správce.

Podle stávající výkladové praxe však nesmí správce shromažďovat údaje jen z toho důvodu, že by je mohl v budoucnu potenciálně využít v soudním řízení. Správce by měl mít vždy důvodnou obavu, že může dojít k soudnímu řízení, kde tyto údaje bude nezbytné předložit – aby se domohl svých nároků nebo mohl prokázat či obhájit svou pozici. ÚOOÚ v této souvislosti navíc uvedl, že „dobu uchování osobních údajů zpracovávaných za účelem ochrany práv a právem chráněných zájmů správce osobních údajů [tedy podle § 5 odst. 2 písm. e) ZOOÚ] však nelze stanovit pouze s odkazem na obecné promlčecí či prekluzívní lhůty, pokud již neprobíhá např. soudní či jiné řízení, anebo pokud není důvodné takové řízení předpokládat.

Uplatnění této výjimky rovněž slábne v čase a správce se tak obhajoby svých právních nároků nemůže dovolávat neomezeně. Základním vodítkem pro nastavení doby uchování údajů pro učení, výkon nebo obhajobu právních nároků by tak měly být (zejména subjektivní) promlčecí lhůty spojené s takovým nárokem. Po uběhnutí promlčecích lhůt obvykle není další uchování těchto údajů opodstatněné a správce by měl údaje vymazat, tj. tato podmínka se po uběhnutí promlčecích lhůt ve většině případů nadále neuplatní.

6.5 Právo být zapomenut ve vztahu k osobním údajům v trestních věcech ve smyslu směrnice 680/2019

Analogicky[532] s úpravou v obecném nařízení o ochraně osobních údajů má subjekt údajů právo na výmaz osobních údajů. Toto právo je zakotvené v čl. 16 odst. 2 směrnice 2016/680 a do českého právního řádu je transponováno prostřednictvím § 29 zákona o zpracování osobních údajů.

Fyzická osoba má a právo na výmaz, pokud je zpracování těchto údajů v rozporu s touto směrnicí.[533] Právo na výmaz lze tedy uplatnit, pokud ke zpracování dochází v rozporu s právními předpisy, pokud došlo k omezení zpracování některých kategorií osobních údajů nebo pokud má spravující orgán z jiných důvodů povinnost tyto údaje vymazat. Právě rozsah zákonné úpravy bude mít v trestněprávní oblasti přitom zásadní dotaz, jak vyplývá rovněž např. z rozhodnutí Nejvyššího soudu, ve kterém aproboval uchování vzorků (profilu) DNA pachatele úmyslné trestné činnosti Policií ČR, která podle závěrů Nejvyššího soudu tak činila zcela v souladu s platnou právní úpravou, a tudíž nebylo možné se dožadovat výmazu takových osobních údajů.[534]

Právo na výmaz ve smyslu směrnice 2016/680, resp. pak ve smyslu zákona o zpracování osobních údajů, se tak obsahově neliší od práva být zapomenut vymezeného v obecném nařízení o ochraně osobních údajů a blíže analyzoaném v kapitolách výše. Nakládání s osobními údaji ze strany orgánů činných v trestním řízení a jiných tzv. spravujících orgánů[535] pak podléhá zvláštním právním

[532] VLACHOVÁ, Barbora a Martin MAISNER. Zákon o zpracování osobních údajů: komentář. V Praze: C.H. Beck, 2019, xviii, 145. ISBN 978-80-7400-760-6, s. 67 – 70.

[533] Bod č. 46 úvodních ustanovení směrnice 2016/680.

[534] Rozsudek Nejvyššího soudu ze dne 17. ledna 2020, 30 Cdo 2003/2018.

[535] Těmi se ve smyslu § 24 odst. 3 ZZOÚ rozumí toliko orgán veřejné moci příslušný k plnění úkolu výkonu veřejné moci při odhalování a potírání trestné činnosti (za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti včetně pátrání po osobách a věcech); k tomu srov. RŮŽIČKA M., in in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 612.

předpisům. V případě, že bude zpracování osobních údajů podle těchto právních předpisů nezákonné (resp. bude v rozporu se zásadami zpracování ve smyslu § 25 ZZOÚ), subjekt údajů se může domáhat výmazu svých osobních údajů.

Pro účely této práce již nejsou blíže analyzovány konkrétní trestněprávní předpisy (vymezující tak účely zpracování, které nemohou být přesáhnuty a pro které mohou spravující orgány s osobními údaji nakládat), kterými se může takové zpracování osobních údajů řídit.

6.6 Závěr

Po formulaci práva být zapomenut (angl. *right to be forgotten* nebo také *right to oblivion*) v podobě rozsudku Soudního dvora EU ve věci Google Spain v roce 2014 došlo k výslovnému legislativnímu zakotvení tohoto práva v čl. 17 obecného nařízení o ochraně osobních údajů aplikovatelném od 25. května 2018 na území EU i EHP.

Právo na výmaz ve smyslu tohoto čl. 17 GDPR plynule navazuje na dosavadní úpravu a dále ještě posiluje postavení subjektů údajů, a to v návaznosti na ostatní povinnosti správce, které by měl plnit i bez ohledu na to, zda se subjekt údajů bude tohoto práva domáhat. Právo na výmaz tak v zásadě pouze pomáhá subjektu údajů, který se může domáhat, aby správce plnil své povinnosti – tedy aby v souladu se zásadou zákonnosti a zásadou minimalizace zpracovával vždy jen údaje nezbytné ke splnění určitého účelu, po dobu nezbytnou ke splnění tohoto účelu a vždy na základě platného právního základu. V případě, kdy neplní tyto podmínky, je povinen se zdržet zpracování osobních údajů a tyto údaje vymazat (tj. „povinný výmaz“). Výmaz osobních údajů je tak často přímo zákonnou povinností správce, bez toho aniž by subjekt údajů uplatňoval žádost o výmaz svých údajů („výmaz na žádost“); ta je naopak spíše až sekundárním nástrojem toho, kdy by měl správce osobní údaje vymazávat. Subjekt údajů se tak prostřednictvím uplatnění práva na výmaz často domáhá již existujících

Jedná se tak např. o Generální inspekce bezpečnostních sborů, Policie České republiky nebo Vojenské policie České republiky – k tomu srov. VLACHOVÁ, Barbora a Martin MAISNER. Zákon o zpracování osobních údajů: komentář. V Praze: C.H. Beck, 2019, xviii, 145. ISBN 978-80-7400-760-6, s. 54 – 58.

povinností správce – resp. se domáhá toho, aby se správce zdržel takového zpracování, ke kterému již nemá žádný právní základ, a tyto údaje vymazal.

V případě, že dojde k výmazu (ať již povinnému nebo na žádost), je správce povinen o této skutečnosti informovat jednotlivé příjemce, jimž byly osobní údaje zpřístupněny, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí[536]. Ustanovení § 9 ZZOÚ navíc výslovně zakotvuje možnost tuto povinnost splnit úpravou údajů v evidenci, jejíž obsah je zveřejňován. Pokud tak správce např. zpřístupňuje data prostřednictvím API, postačí úprava v původní databázi bez dalších nezbytných notifikací. Domnívám se, že tato možnost je jen logickým aplikačním projevem této povinnosti a lze s její aplikací počítat i na území jiných členských států.

Použitá metoda výmazu by neměla být rozhodující, rozhodující je jen výsledek, tedy že osobní údaje již nebudou nadále použitelné, resp. nebudou naplňovat definici osobního údaje, a nebudou ani potenciálně způsobilé k identifikaci fyzické osoby. Domnívám se, že by bylo nepřiměřené na každého správce bez dalšího aplikovat povinnost zajistit absolutní nemožnost obnovy takových údajů, a způsob likvidace dat nebo jejich nosičů by tedy měl být vždy dovozován a prováděn s ohledem na technologické možnosti povinného subjektu.

Stejně tak lze provést výmaz osobních údajů prostřednictvím anonymizace, avšak i v takovém případě je nezbytné zajistit, že dojde k *absolutní* anonymizaci, a tedy nebude existovat možnost takový dataset zpětně de-anonymizovat. V takovém případě by nebyly splněny podmínky práva na výmaz.

S problematikou toho, co znamená finální výmaz, rovněž velmi úzce souvisí otázka, odkud je nezbytné údaje mazat, zda se má výmaz promítnout jen do aktivně používaných databází, nebo zda je nutné mazat např. i zálohy osobních údajů na nepřepisovatelných nosičích, aj. Nařízení k tomu nenabízí žádnou odpověď a povinností správce je tak v zásadě vymazat veškeré osobní údaje, které má o subjektu údajů k dispozici.

[536] Srov. čl. 19 GDPR.

Konkrétní podmínky, za kterých vzniká povinnost data vymazat jsou stanoveny v čl. 17 odst. 1 GDPR a pro zveřejněné údaje pak v čl. 17 odst. 2 GDPR, přičemž platí, že nesmí být naplněna žádná výjimka v čl. 17 odst. 3 GDPR (jako jsou svoboda projevu a přístup k informacím či plnění povinností ve veřejném zájmu), která by opodstatňovala další zpracování takových osobních údajů a která by proporcionálně převážila nad právy subjektu údajů. Tyto výjimky, ač mohou v praktické aplikaci způsobovat problémy, jsou logickým vyústěním relativní povahy práva být zapomenut, které nemůže absolutně a bez dalšího převážit nad zájmy celé společnosti ani konkrétního správce.

Za nejspornější předpoklad výmazu pak považuji povinnost data vymazat v případě, kdy osobní údaje tohoto subjektu údajů byly zpracovány protiprávně (dle čl. 17 odst. 1 písm. d) GDPR). Na základě jazykového, komparativního a teleologického výkladu jsem dospěl k závěru, že tato podmínka musí být vykládána restriktivně a musí se jednat především o porušení jiných právních povinností než těch vyplývajících z GDPR (v opačném případě by bylo nezbytné dovozovat, že předpokladem vzniku výmazu je jakékoliv porušení ochrany osobních údajů a správce by byl bez dalšího povinen smazat veškeré osobní údaje subjektu údajů např. jen z toho důvodu, že jej nedostatečně informoval dle čl. 13 GDPR). Nicméně i tak lze předvídat, že v případě, že by zpracovatelské operace prováděné správcem dosáhly takové intenzity, že by byly v rozporu se všemi ostatními principy nařízení dle čl. 5, lze připustit, že by se subjekt údajů mohl domáhat výmazu osobních údajů na základě tohoto ustanovení.

Ve zbylých částech této kapitoly jsou podrobně analyzovány požadavky práva být zapomenut (práva na výmaz) ve smyslu čl. 17 GDPR a podrobně vysvětluje jednotlivé požadavky v systematice toho ustanovení.

7 Důsledky porušení práva být zapomenut

7.1 Možné důsledky porušení práva být zapomenut

7.1.1 Vymezení důsledků porušení práva být zapomenut

Porušení práva být zapomenut, resp. tedy odmítnutí vymazat konkrétní informace či osobní údaje, popř. neúplné (nedokonalé) vymazání může mít několikeré důsledky. V případě osobnostních práv jednotlivce obecně nemusí dojít k samotnému zásahu, ale postačí i pouhé ohrožení chráněného zájmu.[537] Domnívám se však, že ohrožení práva být zapomenut není prakticky možné, jelikož tím v zásadě vždy dojde k ohrožení, či dokonce porušení jiného osobnostního práva. Proto dále uvažuji pouze s konkrétními zásahy do tohoto práva.

Porušení práva být zapomenut má soukromoprávní i veřejnoprávní konsekvence. Z hlediska soukromoprávní se bude jednat zejména o standardní nástroje ochrany osobnosti, popř. specifikovaných pro oblast osobních údajů, a případné soukromoprávní delikty (zejména tedy náhradu újmy), jak jsou detailněji analyzovány níže. Ty tak zajišťují standardní reparační, satisfakční a případně i kompenzační funkci[538].

Z hlediska veřejnoprávního jsou pro případy porušení práva být zapomenut zejména veřejnoprávní sankce vymezené v čl. 83 a 84 GDPR. Soukromí je pak chráněné rovněž trestním právem, kde Hlava II, díl 2 trestního zákoníku vymezuje trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství (§ 180 a násl.). Specifická skutková podstata trestného činu neoprávněného nakládání s osobními údaji dle § 180 t.z. chrání osobní údaje shromážděné v souvislosti s výkonem veřejné moci a chráněné státem uloženou nebo uznanou povinností mlčenlivosti. Všech těchto trestných činů se navíc může dopustit i

[537] Srov. např. KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6, s. 150 – 153.

[538] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 524.

právnická osoba (ve smyslu zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim), nikoliv však stát či samosprávný celek.

7.1.2 Občanskoprávní nároky

Občanskoprávní nároky vyplývají z obecných pravidel ochrany osobnosti a soukromí. Ty jsou navíc doplněny, resp. specifikovány, pro oblast ochrany osobních údajů. Nejširší možné důsledky tak mohou nastat v případě, že se se jedná o zpracování osobních údajů a jednotlivec se bude domáhat výmazu svých osobních údajů ve smyslu obecného nařízení osobních údajů. V případě, že správce, popř. zpracovatel, takovému nároku nevyhoví, přicházejí v úvahu různé instrumenty práva soukromého i veřejného.

Právo být zapomenut, ač integrální součást osobnosti, samo o sobě reprezentuje spíše „prvek ochrany“ spočívající v odstranění (výmazu) nežádoucích informací, resp. dat či osobních údajů a některé nároky tak mohou být fakticky omezené, resp. jsou inherentně zahrnuté v samostatné podstatě tohoto práva.

Jak již bylo dovozeno v kapitole 2.6, právo být zapomenut, coby integrální součást osobnosti, má svou pozitivní a negativní složku – nejen že tedy člověk disponuje možností své právo být zapomenut užívat a v mezích právního řádu s ní i disponovat (pozitivní složka), ale v případě jeho porušení se domáhat právních ochrany (negativní složka), která tedy představuje ochranu proti zásahům, tj. proti soukromoprávním deliktům.[539] Vzhledem k povaze tohoto práva se však z praktického hlediska tyto dvě roviny velmi překrývají. Již samotná podstata tohoto práva totiž v sobě zahrnuje určitou negativní složku – tedy právo domáhat se určitého konání (výmazu) daného setu informací, resp. osobních údajů.

Z pozitivního hlediska se v zásadě jedná o „samostatné právo“, kterého se lze domáhat jakožto součást volné dispozice s vlastními právy a možností vymezovat své vlastní soukromí a osobnost, což odpovídá lidskoprávní povaze tohoto práva. Z negativního hlediska pak právo být zapomenut působí spíše jako sekundární

[539] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 524.

právo, resp. jako prvek ochrany (či nárok), jehož plnění se může jednotlivec domáhat – tedy může požadovat výmaz.

Z hlediska praktické aplikovatelnosti pak lze zvažovat rozsah a překryvy těchto složek. Domnívám se, že zejména v oblasti zpracování osobních údajů je pozitivní složka do značné míry potlačena, resp. se natolik překrývá s negativní složkou, že při praktické aplikaci bude obtížné tyto dvě složky odlišovat. Právo být zapomenut ve smyslu čl. 17 GDPR totiž v zásadě nastává až jako sekundární právo v případě, že je vyčerpán účel[540] nebo dochází k protiprávnímu zpracování[541]. Přesto má pozitivní složka svůj význam, jelikož působí primárně jako povinnost povinných subjektů (zejména tedy správců/zpracovatelů osobních údajů) vymazat osobní údaje podle čl. 17 GDPR. Zároveň to znamená, že právo být zapomenut je vždy plně v dispozici jednotlivce a může se pak domáhat i např. toho, aby se naopak povinný subjekt (správce/zpracovatel) výmazu naopak zdržel[542]. Domnívám se, že tyto závěry lze obecně aplikovat na právo být zapomenut v celém jeho souhrnu (bez ohledu na to, zda se jedná o obecná osobnostní práva nebo specifikou ochranu osobních údajů). Praktické dopady mohou vznikat zejména z hlediska pozitivní složky, která dává každému jednotlivci možnost plně chránit svou osobnost a uplatňovat právo být zapomenut i v oblastech, které nespadají do působnosti obecného nařízení o ochraně osobních údajů, popř. pak zákona o zpracování osobních údajů.

Fakticky tak bude možné vždy uplatňovat právo být zapomenut jako pozitivní povinnost správce/zpracovatele osobních údajů či jiných subjektů nakládajícími s informacemi.

V případě, že takový povinný subjekt žádosti o výmaz nevyhoví, a tedy dojde k narušení práva být zapomenut (které však standardně již půjde ruku v ruce se zásahem do osobních údajů, soukromí, či jiných složek osobnosti), mají

[540] Zejména tedy ve smyslu čl. 17 odst. 1 písm. a) GDPR.

[541] Zejména tedy ve smyslu čl. 17 odst. 1 písm. b) a c) (chybějící právní základ) a dále čl. 17 odst. 1 písm. d) (zpracování bylo a priori nezákonné) GDPR.

[542] Z hlediska zpracování osobních údajů je však i toto právo v zásadě poměrně marginální, jelikož je samostatným způsobem pokryto v čl. 18 odst. 1 písm. b) GDPR, podle kterého se subjektu údajů může domáhat tzv. omezení zpracování

jednotlivci nástroje ochrany obecně poskytované pro porušení práva na ochranu osobnosti, jak jsou popsané níže. Vzhledem ke specifické povaze práva být zapomenut, které v sobě již nese určitou povinnost k výmazu (resp. právo oprávněného se takového výmazu dožadovat) dále uvažuji nad reálnými možnostmi jednotlivých nároků:

- nárok odstraňovací (restituční) směřuje k odstranění závadného stavu a obnovení stavu *quo ante*, tj. stavu, který byl před tím, než bylo ohroženo nebo zasaženo osobnostní právo.[543] Žaloba na odstranění bude pravděpodobně představovat jeden z hlavních potenciálních nároků, kterých se subjekty údajů mohou domáhat, jelikož vystihuje samotnou podstatu práva být zapomenut, které slouží k odstranění nežádoucího stavu. V tomto případě bude docházet k uplatnění samotného práva na výmaz, kterého se daný jednotlivec bude domáhat, aby došlo k výmazu jeho údajů. Tento nárok bude zpravidla spojený s narušením jiných složek ochrany osobnosti, resp. porušení některých pravidel ochrany osobních údajů.

- nárok zápůrčí (negatorní, zdržovací či zakazovací) spočívají v možnosti požadovat, aby se narušitel zdržel protiprávního jednání, jímž porušuje osobnostností právo dotčeného.[544] Zdržovací nárok bude nicméně vždy podmíněn tím, aby protiprávní zásah trval anebo aby alespoň hrozil, což rovněž připomněl Krajský soud v Brně v případě uplatňování předběžného opatření k výmazu údajů z internetového portálu.[545]

- nárok na náhradu újmy směřující ke kompenzaci újmy[546], která nastala v důsledku porušení práva na výmaz. Pro újmu při zpracování osobních údajů nabízí specifikou úpravu čl. 82 GDPR, jinak se bude postupovat

[543] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 533.

[544] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 533.

[545] Usnesení Krajského soudu v Brně ze dne 7. října 201, sp. zn. 70 Co 228/2015 – 38.

[546] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 533.

podle obecných pravidel občanského zákoníku. K tomu viz kapitola 7.2 níže.

- nárok určovací, který směřuje k určení, že určitým skutkem bylo ohroženo nebo porušeno osobnostní právo dotčeného člověka[547] za předpokladu, že žalobce osvědčí existenci naléhavého právního zájmu na nárokovaném určení. Využití určovacího nároku ve vztahu jen k právu být zapomenut považuji za velmi marginální, jelikož by v zásadě docházelo k určení toho, zda v daném případě má stěžoval práv být zapomenut (a inherentně tedy k posouzení toho, zda zároveň dochází k narušení jeho osobnostních práv). Proto se domnívám, že praktická využitelnost takového nároku je velmi limitovaná.
- další zvláštní nároky, což mohou být zejména nároky založené mimo režim občanského zákoníku. Podle Tůmy se může jednat např. o nároky založené ustanoveními tiskového zákona nebo zákona o provozování rozhlasového vysílání.[548] Ty však nejsou předmětem zkoumání této práce; nicméně se domnívám, že jejich relevance ve vztahu k pravidlům ochrany osobních údajů je minimální, ne-li žádná.

Vedle těchto nároků lze rovněž zvažovat nároky vzniklé z bezdůvodného obohacení (srov. § 3004 o.z.) anebo zákaz dotěrného obtěžování v rámci deliktů z nekalé soutěže (srov. § 2989 o. z.). Rozbor těchto dopadů by však vyžadoval samostatnou analýzu, která přesahuje cíle této práce.

7.1.3 Nároky podle obecného nařízení o ochraně osobních údajů

7.1.3.1 Možnosti ochrany subjektů údajů

Obecné nařízení o ochraně osobních údajů rovněž specificky upravuje postup pro náhradu újmy – majetkové i nemajetkové – která vznikne v souvislosti se zpracováním osobních údajů, které probíhalo v rozporu s pravidly tohoto nařízení.

[547] DOLEŽAL T. in MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1, s 533.

[548] TŮMA, P. in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 289.

Tato úprava je koncentrována v ustanovení čl. 82 GDPR, podle kterého právo na náhradu újmy vzniká bez ohledu na to, ve které fázi zpracování nebo při jaké zpracovatelské operaci ke vzniku újmy dojde. Ke vzniku újmy při zpracování osobních údajů navíc nemusí dojít jen z důvodu porušení GDPR, ale rovněž dalších (národních) předpisů upravujících ochranu osobních údajů – zejména tedy prováděcích národních předpisů[549].

Článek 82 tak vymezuje náhradu újmy jako jeden z nároků, který lze vůči správci/zpracovateli uplatit, a to i souběžně s ostatními nároky, které GDPR nabízí: je tedy možné vůči správci/zpracovateli zároveň požadovat nápravu závadného stavu (podle čl. 79 GDPR), podat stížnost u dozorového úřadu (podle čl. 77 GDPR) a zároveň požadovat náhradu způsobené újmy podle tohoto článku 82 (k tomu viz kapitola 7.2.2 níže). Rovněž probíhající správní řízení vedené vůči tomuto správci/zpracovateli pro stejné porušení není překážkou domáhání se náhrady újmy podle čl. 82 GDPR. Na druhou stranu pro subjekt údajů může být výhodné vyčkat na ukončení řízení ze strany dozorového úřadu, a to zejména z hlediska důkazního břemene, které subjekt údajů nemusí být bez výsledného rozhodnutí dozorového úřadu schopen unést.

7.1.3.2 Právo na soudní ochranu proti správci/zpracovateli[550]

Ustanovení čl. 79 výslovně garantuje subjektům údajů právo na soudní ochranu. Tato úprava navazuje na úpravu čl. 22 směrnice 95/46/ES implementovanou do § 21 odst. 3 ZOOÚ. GDPR tak výslovně zakotvuje právo každého subjektu obrátit se na soud v případě, že zjistí nebo se domnívá, že správce nebo zpracovatel

[549] Srov. zejména bod 146 úvodních ustanovení GDPR.

[550] Části textu v této kapitole byl publikován jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 439 – 444.

Další použité literární zdroje v této kapitole:

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

provádí zpracování jeho osobních údajů v rozporu s ochranou soukromého a osobního života tohoto subjektu údajů nebo v rozporu s pravidly GDPR. Tato úprava rovněž plynule navazuje na čl. 78 GDPR, který poskytuje subjektům údajů ochranu proti postupu či proti nečinnosti dozorového úřadu – v České republice tedy proti rozhodnutí či nečinnosti ÚOOÚ. Obě ustanovení tak dohromady (a ve spojitosti s článkem 82 GDPR přiznávajícím právo na náhradu újmy) vytvářejí systém soudních opravných prostředků. Tato dvě ustanovení se navzájem nevylučují a nevytvářejí vzájemné podmínky přístupu k soudu. Subjekt údajů tak může napadat ne/činnost dozorového úřadu a zároveň podat žalobu na správce či zpracovatele, kteří porušili jeho práva na ochranu osobních údajů dle GDPR.

V souladu s čl. 78 odst. 1 GDPR může subjekt údajů podat žalobu na správce či zpracovatele bez ohledu na to, zda předtím podal stížnost podle čl. 77 GDPR. Podání žaloby na správce/zpracovatele tak není podmíněné předchozím podáním stížnosti na tohoto správce či zpracovatele dozorovému úřadu.

Na druhou stranu nařízení zcela jednoznačně nevysvětluje vztah mezi článkem 79 GDPR a zbytkem tohoto předpisu – zejména pak kapitolou III (práva subjektů údajů). Ze znění čl. 79 GDPR není zcela jasné, zda se v případě článku 79 odst. 1 jedná o samostatné hmotněprávní právo, které zakládá subjektům údajů za všech okolností právo na přístup k soudu, nebo zda se jedná o pouhé utvrzení (konstatování) práva na přístup k soudu za předpokladu, že došlo k porušení práv subjektů údajů ze strany správce či zpracovatele.

Domnívám se, že komentované ustanovení samo o sobě nezakládá právo k podání žaloby, a bez dalšího tak neopravňuje subjekt údajů k podání žaloby na správce či zpracovatele. Aby se tak subjekt údajů mohl domáhat soudní ochrany proti správci či zpracovateli, měl by tvrdit porušení některého ze svých práv dle kapitoly III GDPR. Pokud bychom přijali opačnou interpretaci – tedy, že článek 79 odst. 1 zakládá právo na přístup k soudu subjektu údajů v případě jakéhokoliv porušení podmínek GDPR ze strany správce či zpracovatele, došlo by k zavedení dvojkolejné ochrany, kde by subjekt údajů mohl podávat „stížnost“ buď postupem dle čl. 77 dozorovému úřadu, nebo postupem dle čl. 79 odst. 1 GDPR, kdy by

takovou stížnost ve formě žaloby mohl podat z důvodu jakéhokoli porušení povinností GDPR správcem/zpracovatelem.

Taková dvojkolejnost by byla v rozporu s cílem zaváděné úpravy a celkovým konceptem oddělených stížností a přístupu k soudu. Proto je třeba komentované ustanovení vykládat jako procesní ustanovení konstatující právo na soudní ochranu v případě porušení práv subjektů údajů ze strany správce či zpracovatele. Tomuto zároveň odpovídá čl. 12 odst. 4 GDPR, podle kterého, pokud správce nepřijme opatření, o něž subjekt údajů požádá, jej informuje nejpozději do jednoho měsíce o důvodech nepřijetí tohoto opatření a zároveň jej informuje, kromě jiného, o možnosti žádat o soudní ochranu – tj. podat žalobu proti správci. To bude relevantní pro uplatňování práva na výmaz.

Subjekty údajů jsou oprávněny k podání žaloby proti konkrétnímu správci nebo zpracovateli, pokud se tento subjekt údajů domnívá, že správce či zpracovatel porušil jeho práva dle GDPR, zpracovává jeho osobní údaje neoprávněně a/nebo pokud mu porušováním nařízení ze strany tohoto správce či zpracovatele vzniká újma. Žalovaným by tedy v daném případě byl konkrétní správce nebo zpracovatel.

Podle nařízení není podmínkou podání žaloby předcházející uplatnění stížnosti ze strany subjektu údajů u správce či zpracovatele. Taková podmínka by naopak byla velmi restriktivní a vedla by k znevýhodnění postavení subjektů údajů, kdy by na ně byly kladeny nežádoucí podmínky přístupu k soudu, a navíc by tím správci/zpracovateli ještě poskytovaly další prostor k porušování jejich práv.[551]

[551] Subjekt údajů tak může podat žalobu na správce či zpracovatele bez dalšího, aniž by předtím správce/zpracovatele kontaktoval. Ačkoliv tak nejsou kladeny žádné hmotněprávní požadavky na podání žaloby, v případě, že subjekt údajů (žalobce) se nebude domáhat svých práv nejdříve u správce/zpracovatele – tedy nekontaktuje žalovaného předem (7 dnů před podáním návrhu) – může přijít o nárok na soudní náklady spojené s tímto soudním řízením (k tomu srov. § 142a občanského soudního řádu), navzdory tomu, že bude ve sporu úspěšný. Vzhledem k mnohdy slabému postavení subjektu údajů v porovnání s postavením správce/zpracovatele však nelze zcela vyloučit, že by soud přiznal subjektu údajů nárok na náhradu soudních nákladů i v případě, že by před podáním žaloby nebyl se žalovaným v žádném kontaktu – tedy považoval by tuto skutečnost za hodnou zvláštního zřetele (v souladu s § 142a odst. 2 občanského soudního řádu).

7.2 Náhrada újmy

7.2.1 Náhrada újmy podle občanského zákoníku[552]

Vznik újmy a povinnost k její náhradě považuji za jeden z hlavních důsledků porušení práva být zapomenut, resp. obecně zásahu do osobnostních práv.

Podle pravidel občanského zákoníku platí, že povinnost nahradit jinému újmu zahrnuje vždy povinnost k náhradě újmy na jmění, přičemž povinnost odčinit nemajetkovou újmu se uplatní jen, pokud byla ujednána nebo pokud tak stanoví zákon.[553] Jak bylo dovozeno výše v této práci, právo být zapomenut je součástí ochrany osobnosti, a jeho porušení tedy povede k narušení přirozených práv chráněných podle části první občanského zákoníku. Z tohoto důvodu se domnívám, že v případě porušení tohoto práva vznikne škůdci vždy povinnost nahradit škodu i nemajetkovou újmu, kterou tím způsobil, a to včetně způsobených duševních útrap ve smyslu § 2956 o.z. Nicméně jsem toho názoru, že psychické útrapy budou při samotném porušení práva být zapomenut v praxi spíše omezenou relevanci, jelikož zásah v takovém případě musí vždy dosáhnout alespoň určité kvalifikované intenzity – míry útrap, a to sice dle objektivní pohledu *běžného člověka*.[554] Nezáleží na tom, zda je do tohoto práva zasaženo zaviněným protiprávním činem (nedbalostním či úmyslným), anebo újma vznikla v důsledku škodní události přičítané škůdci bez ohledu na jeho zavinění.[555]

Zdrojem protiprávnosti, která je předpokladem pro vznik újmy, může přitom být porušení povinnosti stanovené zákonem, porušení smluvních povinností nebo

[552] ELISCHER, David. Protiprávnost – co je jejím zdrojem v soukromém právu?. Časopis pro právní vědu a praxi [online]. Masaryk University Press, 2016, 24(4), 501-526 [cit. 2022-03-23]. ISSN 1210-9126. Dostupné z: doi:10.5817/CPVP2016-4-1.

[553] Srov. ustanovení § 2984 o.z.

[554] RYŠKA in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2902.

[555] BEZOUŠKA in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, Milan HULMÁK, Roman FIALA a Ljubomír DRÁPAL. Občanský zákoník ..: komentář. V Praze: C.H. Beck, 2013, ^^^sv. ISBN 978-80-7400-287-8, s. 1506.

porušení dobrých mravů.[556] Vedle toho samozřejmě platí standardní předpoklady vzniku civilní odpovědnosti – vznik újmy a příčinná souvislost.

Jak bylo dovozeno v kapitole 2, právo být zapomenut je součástí ochrany osobnosti, a jeho porušení tak bude porušením zákonné povinnosti (zejména § 81 o.z.), za kterou bude škůdce odpovědný pouze v případě, že se bude jednat o jeho zaviněné porušení[557], tedy k takovému porušení musí směřovat jeho úmysl nebo nedbalost[558], a bude se jednat o subjektivní odpovědnost. V takovém případě vždy budou platit právní domněnky nedbalosti ve smyslu § 2911 a § 2912 o.z.

Výjimku budou tvořit případy, kdy se bude jednat o zpracování osobních údajů, pro které je právo být zapomenut zakotveno jako zákonná povinnost a jeho porušení bude rovněž porušení zákonné povinnosti. GDPR nicméně upravuje tuto problematiku samostatně, jak je blíže analyzována v kapitole 7.2.2 níže.

Porušením práva být zapomenut (kterékoliv z jeho složek) by rovněž mohlo dojít k porušení obecné prevenční povinnosti, podle které je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.[559] Jedná se o principy, které slouží k udržení požadovaného standardu náležité péče (jako měřítko chování rozumného jednotlivce). Interpretace generální prevenční povinnosti má být v praxi vedena snahou především reprobovat ta jednání, jež jsou zaviněně nerozumná, nepozorná či neohleduplná, vzejde-li z nich újma, avšak nikoli ztotožnit její účinky s přísnou

[556] ELISCHER, David. Protiprávnost – co je jejím zdrojem v soukromém právu?. Časopis pro právní vědu a praxi [online]. Masaryk University Press, 2016, 24(4), 501-526 [cit. 2022-03-23]. ISSN 1210-9126. Dostupné z: doi:10.5817/CPVP2016-4-1, s. 520.

[557] Srov. ustanovení § 2910 o.z.

[558] Srov. např. PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2816 nebo BEZOUŠKA in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, Milan HULMÁK, Roman FIALA a Ljubomír DRÁPAL. Občanský zákoník ..: komentář. V Praze: C.H. Beck, 2013, ^^^sv. ISBN 978-80-7400-287-8, s. 1567.

[559] Srov. ustanovení § 2900 o.z.

odpovědností za výsledek. [560] Porušení prevenční povinnosti přitom znamená porušení zákona[561] a může se promítnout do výše obecných povinností.

Vedle obecných pravidel ochrany osobnosti však může právo být zapomenut součástí plnění smluvních povinností. V takovém případě může vznikat otázka, do jaké míry může být právo být zapomenut skutečně součástí plnění právních povinností. Zde se domnívám, že obdobná povinnost nemusí být výslovně zakotvena (což lze předpokládat, jelikož takové ustanovení by ve smlouvě – s výjimkou specifických případů – bylo velmi nestandardní[562]). Povinností ze smlouvy je třeba ve smyslu § 545 o.z. rozumět nejen povinnost výslovně ve smlouvě uvedenou, nýbrž i takovou, která pro smluvní stranu plyne ze zákona.[563] I v případě, kdy povinnost vymazat data nebude výslovně ve smlouvě zakotvena, a přesto by docházelo k uplatňování (a následnému porušení) práva být zapomenut, bude se jednat o porušení smluvních povinností. V takovém případě bude odpovědnost za způsobenou újmu objektivní[564] bez nutnosti zkoumat zavinění[565].

Vzhledem k charakteru práva být zapomenut coby přirozeného práva, rovněž nebude možné předem smluvně omezit nebo se vzdát újmy způsobené člověku na těchto právech.[566] Toto ustanovení je v takovém případě kogentní a nelze jej

[560] ELISCHER, David a kol. Náhrada majetkové a nemajetkové újmy podle občanského zákoníku, zákoníku práce, v oblasti průmyslového vlastnictví a podle autorského zákona. 1. vyd. Praha: Leges, 2020, 381 s. ISBN 978-80-7502-382-7, s. 14 a násl.

[561] Srov. PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2823 nebo ELISCHER , David a kol. Náhrada majetkové a nemajetkové újmy podle občanského zákoníku, zákoníku práce, v oblasti průmyslového vlastnictví a podle autorského zákona. 1. vyd. Praha: Leges, 2020, 381 s. ISBN 978-80-7502-382-7, s. 14 a násl.

[562] Navíc platí, že strany při uzavírání smlouvy nemohou domýšlet všechny možné situace nebo naopak počítají se zákonnými pravidly. Srov. BEZOUŠKA in LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, Milan HULMÁK, Roman FIALA a Ljubomír DRÁPAL. Občanský zákoník ..: komentář. V Praze: C.H. Beck, 2013, ^^^sv. ISBN 978-80-7400-287-8, s. 1567.

[563] PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2837.

[564] Srov. § 2913 o.z.

[565] Srov. např. PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2837.

[566] Srov. ustanovení § 2898 o.z.

žádným způsobem mezi stranami derogovat.[567] Nicméně platí, že omezení se vztahují pouze na člověka, na újmu způsobenou v této souvislosti právnické osobě se neuplatní.[568]

7.2.2 Náhrada újmy podle obecného nařízení o ochraně osobních údajů[569]

7.2.2.1 Vývoj právní úpravy v GDPR

Povinnosti k náhradě škody jsou v obecném nařízení o ochraně osobních údajů specificky upraveny v čl. 82. Toto ustanovení navazuje na předcházející úpravu čl. 23 směrnice 95/46/ES, podle kterého měly členské státy stanovit, že jakákoliv osoba poškozená neoprávněným zpracováním má právo na náhradu utrpěné škody od správce. Směrnice zároveň poskytovala správcům možnost prokázat, že za vznik škody neodpovídají. Úprava byla implementována v podobě § 21 odst. 3 a 4 a § 25 ZOOÚ, které shodně stanoví, že pokud v důsledku zpracování osobních

[567] PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2819.

[568] PAŠEK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2820.

[569] Části textu v této kapitole byly publikovány jako VÍTEK, D. in PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 457 - 463.

Další použité literární zdroje v této kapitole:

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016, xi, 338. ISBN 978-80-7400-610-4.

GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0.

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

údajů dojde ke vzniku majetkové či jiné újmy, postupuje se podle občanského zákoníku. Zákon o zpracování osobních údajů tuto implementaci sice nepřevzal, na subsidiárním použití občanského zákoníku ve vztahu k náhradě újmy to však nic nemění.

Navzdory znění směrnice 95/46/ES český zákonodárce automaticky předvídal, že se subjekty údajů mohou domáhat nejen majetkové, ale i nemajetkové újmy, která jim vznikne v důsledku zpracování jejich osobních údajů. Obdobný výklad se postupně prosazoval na celoevropské úrovni, kdy podle výkladu WP29 bylo pod pojem škoda třeba zahrnout i nemajetkovou újmu, která mohla subjektu údajů vzniknout. Naopak např. ve Velké Británii se dlouho prosazoval výklad, že škoda (angl. *damage*) ve smyslu směrnice 95/46/ES znamená pouze finanční ztrátu. Tento výklad se uplatňoval až do nedávného rozsudku Vrchního soudu Spojeného království (High Court) ve věci Vidal-Hall v Google Inc[570], ve které soud rozhodl, že právo na náhradu škody za porušení pravidel na ochranu osobních údajů nezbytně musí zahrnovat i náhradu nemajetkové újmy (*non-pecuniary damage*).

7.2.2.2 Rozsah odškodnění

GDPR tyto nejasnosti odstraňuje a jednoznačně stanoví, že právo na náhradu újmy vzniká v důsledku vzniku újmy hmotné i nehmotné (tj. majetkové i nemajetkové, angl. *material* nebo *non-material damage*). Vzhledem k tomu, že je právo na ochranu osobních údajů základním lidským právem[571], je zcela přirozené, že by jakékoliv porušení tohoto práva mělo zahrnovat majetkovou i nemajetkovou újmu; opačný výklad by zcela popíral celý koncept ochrany osobních údajů a soukromí. Navíc, jak bylo dovozeno výše, zásahem do osobnostních práv (a tedy i do práv na ochranu osobních údajů) dochází k zásahu do nepřirozených práv člověka. Proto subjektu údajů náleží nemajetková újma ve smyslu § 2956 o.z.

[570] Rozsudek High Court, Queen's Bench Division ze dne 16. 1. 2014, [2014] EWHC 13 (QB), Vidal-Hall v Google Inc.

[571] K tomu viz kapitola 1.3 této práce.

Obecné nařízení o ochraně osobních údajů navíc zdůrazňuje, že náhrada způsobené újmy má být úplná – podle bodu 146 úvodních ustanovení se má jednat o veškerou újmu, která může osobám vzniknout v důsledku zpracování, které porušuje GDPR. Důsledky porušení GDPR mohou být velmi široké a velmi často nemajetkové povahy. Např. nedostatečné zabezpečení zdravotnické dokumentace (jakožto dokumentace obsahující rovněž zvláštní kategorie osobních údajů) a jejich únik tak mohou poškozeným ve svém důsledku způsobit diskriminaci ve společnosti, psychický stres či překážky v dalším rozvoji osobnosti.

7.2.2.3 Objektivní odpovědnost

Odpovědnost správce či zpracovatele za způsobenou újmu je objektivní[572], tj. není potřeba prokazovat jejich zavinění.[573] Jakmile dojde k porušení pravidel nařízení, které způsobí jiné osobě újmu, vzniká odpovědnost tohoto správce/zpracovatele za způsobenou újmu (v rozsahu vymezené v čl. 82 odst. 2 GDPR), ledaže prokáže, že není žádným způsobem za tuto újmu odpovědný, tj. prokáže existenci liberačního důvodu.[574] Úprava tak přímo navazuje na dosavadní znění čl. 23 odst. 2 směrnice 95/46/ES a rozšiřuje úpravu i na zpracovatele. Zároveň se úprava v obecném nařízení o ochraně osobních údajů odchyluje od obecného civilněprávního režimu, který obecně pro porušení zákonných povinností vychází z principů subjektivní odpovědnosti.

V případě vzniku majetkové i nemajetkové újmy vzniklé v důsledku porušení GDPR se uplatní pravidla na náhradu újmy podle § 2894 a násl. o. z. Článek 82 ve vztahu k občanskému zákoníku působí jako speciální skutková podstata (nad rámec speciální úpravy zavedené pro některé skutky v § 2920–2950 o. z.), pro

[572] K tomu obdobně např. SEDLÁČEK in RÁMIŠ, V. in UŘIČAŘ, Miroslav a Vladan RÁMIŠ. Obecné nařízení o ochraně osobních údajů: komentář. Praha: C. H. Beck, 2021, xxvii, 1386. ISBN 978-80-7400-815-3, s. 1190 – 1196, nebo NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3, s. 472.

[573] K tomu srov. zejména čl. 82 odst. 1 GDPR, podle kterého *„[k]dokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy“* ve spojení s čl. 82 odst. 3 GDPR, stanovující možnost liberace: *„Správce nebo zpracovatel jsou odpovědnosti podle odstavce 2 zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.“*

[574] Srov. čl. 82 odst. 3 GDPR.

kterou se tak zavádí režim objektivní odpovědnosti se samostatným liberačním důvodem.

Jedná se tak o vymezení případů, kdy správci či zpracovateli vzniká objektivní odpovědnost za vzniklou újmu. Bez ohledu na toto omezení (relevantní zejména ve vztahu ke zpracovateli), může správce či zpracovatel vlastním zaviněním rovněž způsobit jinou škodu (újmu), než je předvídána v čl. 82 GDPR. V takovém případě bude žalobce nucen navíc, nad rámec vzniku újmy a příčinné souvislosti, prokázat zavinění správce/zpracovatele ve vztahu k této újmě. Obecně se pak bude postupovat podle § 2910 an. o. z., ledaže se bude jednat o porušení smluvní povinnosti, u které by se bez dalších ujednání mohlo jednat rovněž o objektivní újmu (srov. § 2913 o. z.).

Možnosti liberace jsou poměrně úzce vymezené, když obecné nařízení o ochraně osobních údajů stanoví, že správce/zpracovatel musí prokázat, že žádným způsobem nemohou nést odpovědnost za újmu vzniklou poškozenému. Správce/zpracovatel má tak jen velmi úzkou možnost, jak se odpovědnosti zprostit. I v případech, kdy občanský zákoník zavádí režim objektivní odpovědnosti, obvykle poskytuje liberační důvod v podobě vynaložené rozumně očekávatelné péče (srov. např. § 2924 o. z., podle kterého se škůdce může odpovědnosti zprostit, pokud prokáže, že „*vynaložil veškerou péči, kterou lze rozumně požadovat, aby ke škodě nedošlo.“*). GDPR takovou možnost správci/zpracovateli neposkytuje a omezuje se jen na úzké „žádným způsobem“.

Správce/zpracovatel se tak odpovědnosti za újmu bude v zásadě schopen zprostit pouze v případě mimořádné události (vis maior), jejíž existenci bude muset prokázat a zároveň bude muset prokázat, že jí nemohl žádný způsobem zabránit.

Objektivní odpovědnost ve vztahu k soukromoprávním nárokům za způsobenou újmu je tak vymezena velmi široce, a to i v porovnání s odpovědností za správní delikty, resp. přestupky, přičitatelné správci/zpracovateli. V zásadě tak platí, že i v případě, že dozorový úřad shledá, že správce/zpracovatel není odpovědný za konkrétní porušení nařízení z hlediska správního práva (a nepřistoupí tedy k udělení sankce podle čl. 83 GDPR), neznamená to automaticky, že se subjekt údajů či jiná poškozená osoba nemohou domáhat náhrady újmy, která jim vznikla.

I pokud tedy prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat (srov. § 21 zák. o odpovědnosti za přestupky), neznamená to automaticky, že skutečně nenese žádnou odpovědnost za událost, která ke vzniku újmy vedla.

Příklad:

Správce v souladu s čl. 32 (a tedy s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům) zavede technická a organizační opatření pro své zpracovatelské aktivity. Přes tato důsledně dodržovaná opatření se třetí straně (v rámci hackerského útoku) podaří získat přístup k těmto údajům a data ukradne. Správci se navíc nepodaří tento útok vůbec detekovat a hacker ukradené údaje následně zveřejní. Tímto zveřejněním dojde ke vzniku újmy subjektu údajů. Navzdory zavedeným opatřením, správce nebyl schopen útok včas identifikovat a ani mu zabránit. Správce nebude schopen prokázat, že za umožnění přístupu nenese žádným způsobem odpovědnost (ačkoliv je prokázána jednoznačná příčinná souvislost mezi vzniklou újmou a tímto hackerským útokem), a může mu vzniknout povinnost způsobenou újmu subjektu údajů uhradit. Subjekt údajů však bude muset prokázat výši újmy mezi vznikem újmy a touto krádeží údajů.

V případě, že je do zpracování zapojeno více správců, správce a zpracovatel a/nebo více zpracovatelů, je každá z těchto osob – pokud lze v souladu s čl. 82 odst. 2 a 3 GDPR dovodit jejich samostatnou odpovědnost za vzniklou újmu – odpovědná společně a nerozdílně. V případě, že je tedy v souladu s pravidly uvedenými výše za způsobenou újmu odpovědných více osob zapojených do zpracovatelského řetězce, vzniká mezi nimi solidární odpovědnost. Koncept solidární odpovědnosti je pro poškozeného (zejména tedy pro dotčený subjekt údajů) velmi výhodný, a to především proto, že je v takovém případě pouze na něm, na kterém ze škůdců se bude náhrady vzniklé újmy domáhat. Z hlediska škůdců pak platí, že pokud újmu nahradí jeden ze škůdců, závazek všech ostatních vůči poškozenému zaniká. Škůdce, který splnil více (popř. nahradil celou

vzniklou újmu i za ostatní škůdce), než na něj připadá, má proti ostatním právo na následné vypořádání, a to podle výše jejich účasti na způsobené újmě[575].

7.2.2.4 Aktivní legitimace k náhradě újmy dle GDPR

Aktivní legitimace na náhradu újmy vzniká každému, komu byla způsobená majetková nebo nemajetková újma v důsledku porušení GDPR s možností domáhat se po správci nebo zpracovateli osobních údajů její náhrady. Nemusí se tak nutně jednat pouze o subjekt údajů, jehož údaje správce/zpracovatel zpracovává, ale jakoukoliv jinou osobu, které vznikne v důsledku porušení taková újma. Je však pravděpodobné, že taková osoba bude mít obtížnější postavení při prokazování příčinné souvislosti mezi (prokázaným) porušením GDPR a vznikem újmy. Pokud se takovéto třetí osobě podaří příčinnou souvislost mezi porušením povinností dle GDPR a vznikem její újmy prokázat, bude mít rovněž právo na náhradu vzniklé (majetkové i nemajetkové) újmy. Újma tak může potenciálně vzniknout např. rodinným příslušníkům subjektů údajů, popř. zaměstnancům správce/zpracovatele.

Újma může rovněž vzniknout správci, jehož zpracovatel porušuje pravidla. GDPR (např. vzniklá újma v důsledku poškození reputace a/nebo ušlého zisku). Postavení správce při prokazování újmy však může být ztíženo jeho speciální povinností kontrolovat zpracování prováděné zpracovatelem (*culpa in inspiciendo)*, stejně jako jeho odpovědnost za výběr zodpovědné osoby (*culpa in eligendo*), jak mu to ukládá čl. 28 odst. 1 GDPR. Navíc se uplatní omezení podle odst. 2, podle kterého zpracovatel odpovídá za újmu pouze, pokud nesplnil povinnosti stanovené nařízením konkrétně pro zpracovatele nebo jednal nad rámec zákonných pokynů správce či v rozporu s nimi.

Stejně tak může újma vzniknout zpracovateli. Postavení zpracovatele při vzniku újmy bude ovšem rovněž podmíněno splněním ostatních povinností z GDPR. Aby se zpracovatel mohl domáhat újmy, měl by být zároveň schopen prokázat, že nedošlo k porušení jeho povinnosti informovat správce o nevhodnosti některých pokynů dle čl. 28 odst. 3 GDPR poslední ustanovení – tj. povinnost zpracovatele

[575] Dle čl. 82 odst. 5 GDPR.

upozornit správce na protiprávnost jeho pokynů. Bude se tak jednat zejména o případy, kdy zpracovatel není z objektivních důvodů schopen pokyny správce přezkoumávat ani ověřovat jejich protiprávnost – typicky se může jednat o poskytovatele softwarových prostředků nebo cloudových řešení, které správce využívá dle svých potřeb (v mezích, které mu takové řešení umožňuje) a zpracovatel tak nemá další kontrolu nad obsahem ani operacemi.

7.3 Závěr

Porušení práva být zapomenut má soukromoprávní i veřejnoprávní konsekvence. Z hlediska soukromoprávní se bude jednat zejména o standardní nástroje ochrany osobnosti, popř. specifikovaných pro oblast osobních údajů, a případné soukromoprávní delikty (zejména tedy náhradu újmy). Ty tak zajišťují standardní reparační, satisfakční a případně i kompenzační funkci.

Právo být zapomenut, ač integrální součást osobnosti, samo o sobě reprezentuje spíše „prvek ochrany“ spočívající v odstranění (výmazu) nežádoucích informací, resp. dat či osobních údajů a některé nároky tak mohou být fakticky omezené, resp. jsou inherentně zahrnuté v samostatné podstatě tohoto práva. Fakticky tak bude možné vždy uplatňovat právo být zapomenut jako pozitivní povinnost správce/zpracovatele osobních údajů či jiných subjektů nakládajícími s informacemi. Právní ochranu přitom nabízí jak obecné principy ochrany osobnosti (zejména odstraňovací, zdržovací a kompenzační nároky), ale rovněž obecné nařízení o ochraně osobních údajů, které specificky upravuje možnost veřejnoprávní ochrany (prostřednictvím kontrol a případných sankcí dozorových orgánů), ale rovněž soukromoprávní ochrany garantující soudní ochranu proti správci i zpracovateli a specificky pak upravující právo na náhradu újmy.

Potenciální náhradu újmy přitom v práci zvažuji jako jeden z hlavních potenciálních důsledků. Vzhledem k přirozenoprávní povaze tohoto práva se domnívám, že v případě, že dojde k narušení práva být zapomenut (coby inherentní součást osobnosti), vznikne poškozeným právo dožadovat se rovněž nemajetkové újmy.

V oblasti zpracování ochrany osobních údajů se tak případné nároky k náhradě újmy budou primárně řídit režimem obecného nařízení ochrany osobních údajů, které předvídá, že se bude jednat vždy o objektivní odpovědnost s poměrně limitovanými možnostmi liberace – správce/zpracovatel musí prokázat, že žádným způsobem nemůže nést odpovědnost za újmu vzniklou poškozenému.

V případě, kdyby se nejednalo o zpracování osobních údajů (např. v případě zemřelých, právnických osob nebo protože dané nakládání spadá mimo působnost GDPR), vždy subsidiárně bude působit zákonná ochrana poskytovaná občanským zákoníkem. Ochrana osobnosti a s tím spojené právo být zapomenut (a související povinnosti povinných subjektů) tedy působí jako zákonná povinnost, jejíž porušení tak zakládá subjektivní odpovědnost pachatele se všemi spojenými domněnkami zavinění, které občanský zákoník předvídá. Nicméně i v těchto případech může k porušení tohoto práva dojít v souvislosti s plněním smluvních povinností, a bude se tak jednat o odpovědnost objektivní.

Vedle těchto nároků lze rovněž zvažovat nároky vzniklé z bezdůvodného obohacení anebo zákaz dotěrného obtěžování v rámci deliktů z nekalé soutěže.

8 Právo být zapomenut v rámci moderních technologií a limity jeho vymahatelnosti

Právo být zapomenut a ochrana osobnosti a soukromí (a specificky pak především oblast ochrany osobních údajů) prodělaly značný rozmach v posledních třech dekádách. Tento vývoj byl (alespoň prozatím) legislativně uzavřen přijetím obecného nařízení o ochraně osobních údajů – ambiciózního právního předpisu s přímo aplikační předností, a navíc s extrateritoriálními ambicemi. Ačkoliv se mnozí autoři a politici obávali, že přijetí GDPR může vytvořit z Evropské unie skanzen, ve kterém dojde k zastavení nebo přinejmenším úplnému zastavení rozvoje nových technologií (obvykle tedy založených na práci s daty a osobními údaji), z GDPR se v zásadě stal nový celosvětový standard ochrany osobních údajů (k tomu srov. kapitolu 3.4 výše).

Ačkoliv se tak nestalo, oblast ochrany soukromí a jeho jednotlivé instituty, včetně práva být zapomenut, stále představují při praktické aplikaci v konkrétních informačních systémech značné výzvy a je často problematické tyto instituty v praxi implementovat a právně vymáhat.[576] Často tak dochází k odtržení právních požadavků od technické reality[577], což je zjevně nežádoucí status. Používání dvou různých jazyků (právního a technického) v přístupu k těmto základním konceptům, jako je vymazání dat, vede k problematické komunikaci, která může mít při praktické aplikaci neblahé důsledky. Proto je nezbytné překlenout tento rozdíl v jazycích a chápání pojmů, jako je „paměť“ či „zapomínání“, jejichž pojetí by mělo být co nejbližší v technickém i právním pojetí.[578] S tím souvisí rovněž výklad samotného „výmazu“, jak byl z právního hlediska popsán např. v kapitole

[576] Srov. např. KOOPS, Bert-Jaap Koops a Ronald LEENES. Privacy regulation cannot be hardcoded. a critical comment on the ‘privacy by design’ provision in data-protection law. International Review of Law. 2014. Computers & Technology, 28:2, 159-17.

[577] FOSCH VILLARONGA, Eduard, KIESEBERG, Peter and LI, Tiffany, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten (August 13, 2017). Computer Security & Law Review (Forthcoming). Dostupné z: https://ssrn.com/abstract=3018186.

[578] FOSCH VILLARONGA, Eduard, KIESEBERG, Peter and LI, Tiffany, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten (August 13, 2017). Computer Security & Law Review (Forthcoming). Dostupné z: https://ssrn.com/abstract=3018186.

6.2.3 této práce. Ten však vždy může narážet na technologické možnosti skutečného výmazu celé stopy daného data setu a případné možnosti jejich zpětné rekonstrukce.

Např. Fosch, Kieseberg a Li označují za hlavní nedostatek stávajícího aplikační přístupu (ať už ze strany zákonodárce, regulátorů či soudů) to, že právo být zapomenut se dnes aplikuje na základě principů zapomínání lidské mysli a společnosti (jak bylo rovněž popsáno v kapitole 5.1 výše). Volají přitom po nutnosti vedení dialogu mezi zákonodárci a technickými experty. Nicméně zároveň upozorňují, že u některých technologií, jako je např. umělá inteligence, nemusí být ani tato spolupráce dostačující a při nastavování dalších pravidel bude s velkou mírou pravděpodobnosti nezbytné vyžadovat multidisciplinární spolupráci, a to včetně zapojení odborníků z oblasti neurologie, kognitivních věd, antropologie, psychologie či sociologie. [579]

Domnívám se, že právě oblast umělé inteligence (která, jak je mým pochopením, je z technologického hlediska stále v naprostých počátcích svého vývoje) bude ukázkovým příkladem, který uplatnitelnost a vymahatelnost práva být zapomenut (ale rovněž další legislativní vývoj) přinese a který rovněž může přinést zásadní zásahy do soukromí bez většího pochopení ze strany subjektů údajů (jednotlivců), ale rovněž i samotných vývojářů a „vlastníků" nástrojů umělé inteligence, kteří často nemusejí rozumět způsobům rozhodování vlastních nástrojů, které budou spočívat právě primárně ve schopnosti sebe-učení a dalšího vývoje.[580]

---

[579] FOSCH VILLARONGA, Eduard, KIESEBERG, Peter and LI, Tiffany, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten (August 13, 2017). Computer Security & Law Review (Forthcoming). Dostupné z: https://ssrn.com/abstract=3018186.

[580] Evropský zákonodárce si obecně uvědomuje problematiku nových technologií a již přinesl první konkrétní návrh další regulace těchto systémů (v podobě tzv. AI Act, citovaném dále), ve kterém se však výmazu dat věnuje jen v jednom krátkém ustanovením týkajícím se vymazávání dat z tzv. sandboxů bez toho, aniž by dále zvažoval jakékoliv dopady vyplývající z existující právní úpravy práva být zapomenut (ani tedy jiných institutů ochrany soukromí) a pro jejich úpravu pouze existuje na existující legislativní rámec v podobě GDPR. I zde by tedy byl žádoucí další interdisciplinární dialog zvažující veškeré aspekty ochrany soukromí, a specificky rovněž práva být zapomenut. Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. [online]. 21.4.2021. [cit. 2022-03-18]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN#:~:text=It%20proposes%20a%20single%20future,the%20purpose%20of%20law%20enforcement.

Aby totiž byly tyto AI (z anglického *artificial intellgence)* systémy schopné dalšího vývoje, je nezbytné, aby (při nejmenším v počátečních fázích) získaly dostatečné množství data setů. I kdyby došlo k výmazu původního data setu, tyto systémy si již navždy budou pamatovat své vstupní veličiny, a je tak velmi pravděpodobné, že budou schopné rovněž (např. za předpokladu další interakce) opětovně rozpoznat konkrétní osoby či zkrátka budou její údaje již *navždy* zpracovávány. Takové principy jsou přitom ve zjevném rozporu se zájmy na zapomnění takových osob, a tedy v nesouladu s jejich právem být zapomenut. Jak totiž trefně shrnují Fosch, Kieseberg a Li: *„Humans forget, but machines remember."*[581]

V těchto intencích není vyloučené, že nebude nadále možné uplatňování práva být zapomenut v podobě, ve které jej vnímáme dnes – tedy jako nástroj *absolutního* zapomnění konkrétní skutečnosti, informací či setu dat, o kterých nadále nechceme, aby byly přístupné širší veřejnosti či konkrétním subjektům. Není tak vyloučené, že v rámci širšího rozvoje a nasazení těchto systémů dojde k limitaci jednotlivců při kontrole jejich soukromí, které např. bude redukováno pouze na otázku, zda stojí o využívání takových technologií (a tedy jsou ochotni přistoupit na zásahy do svého soukromí bez jeho další kontroly, včetně možnosti domáhat se budoucího zapomnění), anebo zda takovou technologii využívat nechtějí (a tedy si chtějí zachovat kontrolu nad svým soukromím). Takové pojetí technologií a ochrany soukromí však zjevně není žádoucí – nejenže bude dávat technologickým společnostem (gigantům) absolutní *monopol* nad soukromím jednotlivců (což může samo o sobě přinejmenším vyvolávat další právní otázky, ale především mít neblahé následky pro ochranu soukromí), ale může vést k vytvoření *velkého bratra* a kontrolujícího každodenní počínání. Právě proto je nezbytná interdisciplinární spolupráce napříč jednotlivými obory, které umožní vytvoření takové právní regulace, která bude odpovídat reálným možnostem technologií a vytvoří tedy takové právní podmínky, které budou skutečně účinné a vymahatelné a nebudou vytvářet zdání informačního sebeurčení coby určité

[581] FOSCH VILLARONGA, Eduard, KIESEBERG, Peter and LI, Tiffany, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten (August 13, 2017). Computer Security & Law Review (Forthcoming). Dostupné z: https://ssrn.com/abstract=3018186.

Potěmkinovy vesnice dávající zdání ochrany a kontroly nad vlastním soukromím *pouze na papíře*.

Limity práva být zapomenut ale zjevně nesouvisí jen s technologiemi *budoucnosti,* jako je právě umělá inteligence. Jak upozorňuje např. Vint Cerf, *„nelze jít a vymazat data z počítače všech lidí jen kvůli tomu, že se někdo rozhodl, že chce, aby na něj svět zapomněl.“*[582] Ačkoliv tedy teoreticky právo na výmaz v takovém případě bude existovat, jeho praktická vymahatelnost se může limitně blížit nule. V prostředí internetu (a tím spíše sociálních médií), kde se informace šíří v řádu (mili-)sekund[583], je představa kontroly nad vlastním soukromím poměrně lichá, a tím spíš možnosti uplatňování práva být zapomenut.

Představme si například situaci, kdy dojde k publikaci videa na sociální síti Twitter. Během několik minut se dané video stane virálním hitem, které ne že je jen sdílené napříč Twitterem („retweetované“), ale rovněž si jej uživatelé postupně ukládají do svých telefonů, vytvářet *printscreeny* z tohoto videa, různé *memes* či toto video dále sdílí prostřednictvím jiných sítí – Youtube, Facebook a Snapchat – a zároveň si jej přeposílat prostřednictvím soukromých zpráv na Messengeru, WhatsAppu a Instagramu. Předjímejme, že neexistuje jiný zájem a takové video již samo o sobě (bez ohledu na jeho virální šíření) bude významně narušovat soukromí poškozeného. V takové situaci bude mít zajisté poškozený možnost domáhat se výmazu tohoto videa. Ale bude skutečně úspěšný a dojde k plném vymahatelnosti tohoto práva? Pravděpodobně se mu podaří smazání videa z Twitteru, předpokládejme i ze všech ostatních sociálních sítích, nicméně vymahatelnost vůči jednotlivcům bude fakticky téměř neproveditelná (bez ohledu na to, že v takovém případě pravděpodobně nebude na základě „domácí výjimky“ možné aplikovat GDPR a bude nezbytné postupovat civilně-právní cestou) a videa

[582] WARMAN, M. (2012) Vint Cerf attacks European internet policy. Telegraph. [online]. 29.3.2012.[cit. 2022-02-18]. Dostupné z www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html

[583] Srov. např. DIZIKES, Peter. Study: On Twitter, false news travels faster than true stories. [online]. 8.3.2018. [cit. 2022-02-18]. Dostupné z https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

(a jeho odvozeniny, obrázky na něm založené aj.) již navždy budou žít v telefonech, počítačích a jiných zařízeních po celém světě.

Takové případy se přitom dějí téměř na každodenní bázi a neexistuje účinný právní nástroj, který by vedl k ochraně takových poškozených. V úvahu může přicházet např. dohledání prvotního pořizovatele takového videa a domáhat se proti němu náhrady újmy (popř. se vůči němu domáhat, aby zajistil uplatnění výmazu napříč internetem, kde se však pravděpodobně setká se stejným výsledkem jako samotný poškozený).

Vzhledem ke globální povaze internetu a vzhledem k množství zapojených subjektů mohou být faktické možnosti uplatnitelnosti práva být zapomenut velmi limitované a bude záležet na dalším legislativním i technologickém vývoji, zda dojde k naplnění existujících právních možností. Takovou situací by byla existence veškerých dat v prostředí blockchain, který by byl schopen jim vždy přiřadit konkrétní identifikátor a kompletní dohledatelnost v případech, kdy by se konkrétní poškozený chtěl domáhat výmazu takových dat.

Závěr

Právo být zapomenut, které bylo poprvé formulováno v rámci rozsudku Soudního dvora EU ve věci Google Spain v roce 2014, tvoří jeden z právních instrumentů práva na ochranu soukromí. Právní ochrana soukromí se přitom začala v právní nauce poprvé objevovat ke konci 19. století, když Samuel D. Waren a Louis D. Brandeis formulovali *right to be alone.* Širší pozornosti se ochraně soukromí začalo dostávat ve 30. letech 20. století, přičemž význam ochrany soukromí a jednotlivce vůči státu se ukázal jako nezbytný zejména po zkušenostech s totalitními režimy – fašistickými i komunistickými – které se snažily zneužívat informace o soukromí svých občanů ve svůj prospěch a k posílení vlastní moci.

Pojem soukromí není v českém ani evropském právním řádu nijak vymezen a blíže jej nedefinují ani jednotlivé mezinárodní dohody. Absence vymezení soukromí však není na škodu, a naopak pomáhá jeho ochraně. Pojem soukromí (a práva na soukromí) v sobě totiž zahrnuje nemalé množství aspektů týkajících se psychické a fyzické integrity jednotlivce a jeho soukromého života a uplatňuje se napříč jednotlivými vrstvami života jednotlivce – soukromou, společenskou, občanskou a profesionální, přičemž do každé z nich lze v určitém (diferenciovaném) rozsahu za určitých okolností zasahovat. Bližší definice soukromí by tak mohla vést k nežádoucímu zužování tohoto pojmu a omezování jeho ochrany.

Vnímání soukromí se rovněž významně vyvíjí v čase, a především v souvislosti s rozvojem nových technologií. Pravděpodobně největší rozvoj vnímání soukromí a potřeby jeho ochrany přinesl v posledních dvou dekádách rozvoj internetu a kyberprostoru, ve kterém může docházet k zásahům do soukromí na každodenní bázi, a to často bez většího uvědomění ze strany jednotlivců. Judikatura evropských i českých nejvyšších soudů se pak musí vypořádávat se střetem soukromí a dalšími lidskými právy, kde vždy záleží na konkrétní situaci a složce a vrstvě soukromí, která může být dotčena – nejčastěji tedy s právem na svobodu projevu a informace, ale přicházejí v úvahu i další základní lidská práva, jako je právo na svobodu podnikání či vlastnictví.

Pro účely aplikace práva být zapomenut, na něž se zaměřuje tato práce a které je dnes již inherentní součástí ochrany soukromí, pak za nejvýznamnější považuji vymezení práva na informační sebeurčení, které dává jednotlivcům možnost rozhodnout podle vlastního uvážení zda, popřípadě v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jejich osobního soukromí zpřístupněny jiným subjektům.

V této práci jsem dospěl k závěru, že právo být zapomenut je nedílnou součástí ochrany osobnosti a osobnostních práv, a to vzhledem k jejím přirozenoprávní povaze. Jednotlivé osobnostní atributy (dílčí práva) osobnosti a osobnostních práv jsou součástí jediného práva a vytvářejí monistickou koncepci lidské osobnosti; nelze tak hovořit o několika osobnostních právech, ale jen o celku této ochrany. Tato dílčí práva se navíc stále rozvíjejí spolu s rozvojem společnosti a jejích potřeb. Proto se součástí osobnosti stalo i právo být zapomenut, které představuje jedno z dílčích práv inherentně spojených s osobností. I právo být zapomenut tak bude působit *erga omnes*, ale vždy jen v rozsahu, ve kterém lze poskytovat ochranu osobnosti jako celku. Z tohoto hlediska se tedy jedná o relativní právo, jehož uplatnění není neomezené a je vždy nezbytné jej v souladu s principy proporcionality poměřovat a balancovat s jinými chráněnými zájmy. Tato ochrana přitom náleží nejen po celou dobu života člověka, ale je poskytována i nasciturovi a zemřelým.

Z této přirozenoprávní podstaty právo být zapomenut nenáleží pouze fyzickým osobám (lidem), ale rovněž osobám právnickým. Ochrana „osobnosti“ právnické osoby zahrnuje zejména ochranu dobrého jména, pověsti a soukromí právnické osoby, která má zároveň ústavně-právní garance v podobě práva na soukromí ve smyslu čl. 10 LZPS. Ačkoliv se nejedná o „standardní“ ochranu všeobecných osobnostních práv, která český právní řád přiznává fyzickým osobám, tyto jednotlivé složky jsou specificky chráněny dle § 135 o.z. Proto jsem dospěl k závěru, že právo být zapomenut náleží i právnickým osobám, ačkoliv rozsah poskytované ochrany bude z podstaty jejich ochrany obecně užší než u lidí.

Právní oblast ochrany osobnosti a soukromí je širokou množinou zahrnující rovněž kromě jiného poměrně novou ochranu osobních údajů, která je od roku

1995 specificky chráněná i na úrovni Evropské unie (ve smyslu směrnice 95/46/ES) a od roku 2009 díky přijetí Lisabonské smlouvy a zakotvení Listiny EU coby součástí primárního práva EU je rovněž chráněna jako jedna ze základních „ústavních" hodnot Evropské unie. Roku 2016 byla tato ochrana rozvinuta v podobě nového právního předpisu – obecného nařízení o ochraně osobních údajů (GDPR), které je jakožto *nařízení EU* přímo aplikovatelným právním předpisem napříč všemi členskými státy EU (a EHP). GDPR má navíc extrateritoriální ambice a předvídá za splnění podmínek čl. 3 GDPR aplikovatelnost rovněž na subjekty mimo území EU, a tedy mimo standardní působnost evropských právních předpisů. Jakkoliv ambiciózní a v mnoha případech i nevymahatelná taková aplikovatelnost může být, GDPR se stalo předobrazem mnoha právních předpisů na ochranu soukromí okolo celého světa, a to včetně institutu práva být zapomenut. Díky tomu se z práva být zapomenut (spolu s dalšími základními principy a instituty soukromí a ochrany osobních údajů) stává celosvětově uplatnitelné právo, což je zejména v oblasti internetu velmi významný posun.

Právo být zapomenut tak bude – bez dalšího – uplatnitelné na území Evropské unie a Evropského hospodářského prostoru na základě pravidel GDPR (tj. v rámci ochrany osobních údajů); díky vlivu GDPR i na zahraniční právní řády a díky postupné adopci předpisů na ochranu osobních údajů v těchto právních řádech bude možné toto právo rovněž uplatňovat ve státech, kde již došlo k uzákonění těchto předpisů na ochranu soukromí a osobních údajů; nicméně v takovém případě bude nezbytné postupovat prostřednictvím standardních kolizních pravidel mezinárodního práva soukromého. Podobně tomu bude v oblastech nespadajících do oblasti ochrany osobních údajů (jako bude např. ochrana právnických osob nebo zemřelých), kdy lze nicméně právo být zapomenut uplatňovat jako součást ochrany osobnosti (v rámci standardních civilněprávních nástrojů ochrany osobnosti). I tato pravidla bude (díky jejich přirozenoprávní a lidskoprávní povaze) dovozovat i mimo území působnosti evropského práva, avšak bude nezbytné postupovat podle aplikovatelných kolizních norem.

Funkcí práva být zapomenut je ochrana jednotlivce, který by (obdobně, jako je tomu např. u zahlazení odsouzení) měl mít možnost „čerstvého začátku", resp.

aby byl plně chráněn nejen vůči veřejnosti, ale i vůči státu a jiným (konkrétním) osobám soukromého práva, kteří přinejmenším plynutím času ztrácejí až na výjimky legitimní zájmy na dispozici s takovými informacemi, které by mohly opodstatnit přístup k těmto informacím.

Oblast ochrany osobních údajů, osobnosti, soukromí i konkrétně práva být zapomenut úzce souvisí s rozvojem nových technologií, zejména tedy internetu, ale v zásadě celého kyberprostoru. Základem nových technologií je přitom práce s daty, jejichž právní povahu tato práce také zkoumá a dospívá k závěru, že vzhledem k širokému pojetí věci v českém právním řádu se data kvalifikují jako věc a je nezbytné s nimi jako s věcí nakládat. Nicméně povaha dat jako věci otevírá významné výkladové problémy, jako jsou otázky možnosti vlastnictví dat a výkonu (různých) majetkových práv. Bližší analýza této oblasti významně přesahuje cíle této práce; nicméně se zdá, že bez další legislativní úpravy nebude možné tyto fundamentální problémy překlenout; jako inspirace se přitom nabízí např. koncepty autorského práva (zejména dělení subjektivních a majetkových práv). Minimálně při uplatňování práva být zapomenut však nemusejí tyto otázky hrát zásadní roli – uplatnění práva být zapomenut je totiž vždy nezbytné poměřovat s ostatními základními právy a principy a přiznání vlastnických práv k datům (nesoucí osobnostní prvky, tedy včetně osobních údajů) by tak jen posílalo případnou argumentaci pro vyvážení práva na vlastnictví či podnikatelskou činnost.

V digitálním světě jsou data (včetně osobních údajů) neustále přítomná a permanentně existující. Tato neustálá permanence dat přináší značná rizika ohledně způsobu jejich využívání a spolehlivosti. Internet totiž vytváří prostředí pro neustálou kumulaci dat a informací, které vytvářejí propletenou pavučinu různých střípků poskytující „komplexní profil“ jednotlivců. Tento komplexní profil je často jen pouhým zdáním, které může vést k nebezpečným předsudkům a ukvapeným závěrům. Přinejmenším srovnatelné nebezpečí tak vzniká i v souvislosti s nedostupností dat, resp. v souvislosti s jejich zastaráváním, roztříštěností nebo vytrháváním z kontextu (které mohou budovat zcela zavádějící online obraz jednotlivce). Takto (ne)přístupné (dis-)informace, navíc ještě veřejně dostupné na internetu, tak mohou vést ke značně zavádějícím výsledkům

a značným zásahům do soukromí. Oba tyto jevy tak posilují význam práva být zapomenut coby jednoho z projevů práva na informační sebeurčení, které dává jednotlivci kontrolu nad svými osobními údaji a dalšími informacemi a daty souvisejícími s jeho osobou a potenciálně tak ohrožující jeho soukromí a další osobnostní práva. Pokud tedy nepřevládne jiný společenský zájem (zejména právo veřejnosti na informace), každý by měl mít možnost plné kontroly nad rozsahem informací, které jsou o něm veřejně přístupné, a stejně tak o těch, které přístupné nejsou. Obě situace totiž mohou vyvolat značné zásahy do soukromí a zneužitelnost těchto informací.

Permanence a objem existujících informací na internetu přitom neohrožuje jen osobní sféru konkrétního jednotlivce, ale může ohrozit fungování celé demokratické společnosti. To bylo prezentováno na příkladu Facebook Cambridge Analytica, ve kterém docházelo k masivnímu zneužívání osobních údajů a informací osobní povahy k vytvoření osobních profilů a následnému ovlivňování voličských preferencí (v rámci prezidentských voleb v USA i v rámci referenda o Brexitu). Druhým příkladem je povinná *data retention*, u které státní moc opakovaně argumentuje zájmem na ochraně bezpečnosti, která má převážit nad ochranou soukromí jednotlivců; nicméně tato funkce je přinejmenším zpochybnitelná a, jak dokládá opakovaná judikatura SDEU v této věci, jen výjimečně odůvodnitelná.

Tyto otázky rovněž souvisí s možnostmi dalšího zpracovávání zveřejněných osobních údajů, které sice není vyloučené, nicméně správce bude muset splnit veškeré podmínky takového zpracování, včetně provedení balančního testu, informování subjektů a zejména pak zajištění uplatnění práv subjektů údajů, včetně práva být zapomenut, které mohou být fakticky jen obtížně splnitelné.

Obdobné limity byly identifikovány při uplatnění práva být zapomenut v rámci obsahu ukládaného na individuálních úložištích (jako jsou mobilní telefony, počítače aj.), kde je faktická vymahatelnost práva být zapomenut limitně se blížící nule. Tyto otázky se však obecně propisují do oblasti nových technologií, jako je umělá inteligence (zpracovávající osobní údaje či jiná data osobní povahy, ať už v rámci svého fungování nebo v rámci vstupního datasetu). Uplatnění práva být

zapomenut v rámci těchto nových technologií může být na hraně technických i faktických možností. Nastavování dalších pravidel tak bude vyžadovat multidisciplinární spolupráci, a to včetně zapojení odborníků z oblasti neurologie, kognitivních věd, antropologie, psychologie či sociologie, které mohou významně modifikovat funkci zapomínání, jak ji vnímáme dnes a na které jsou vystavěny stávající principy práva být zapomenut (ale v zásadě i celé ochrany soukromí).

Porušení práva být zapomenut přitom může mít zásadní důsledky – ať již veřejnoprávní (sankce podle GDPR nebo dokonce trestněprávní následky), nebo soukromoprávní. Z hlediska soukromoprávních důsledků se práce blíže zaměřuje na náhradu újmy jako jeden z hlavních možných následků, který je navíc rovněž specificky upraven na úrovni GDPR jakožto objektivní odpovědnost s velmi úzce vymezenými případy liberace. V případě, kdyby se nejednalo o zpracování osobních údajů (např. v případě zemřelých, právnických osob nebo protože dané nakládání spadá mimo působnost GDPR), vždy bude subsidiárně působit obecná ochrana osobnosti (ať již na ústavní úrovni nebo pak specificky prováděná v občanském zákoníku). Ochrana osobnosti a s ní spojené právo být zapomenut (a související povinnosti povinných subjektů) tedy působí jako zákonná povinnost, jejíž porušení tak zakládá subjektivní odpovědnost pachatele se všemi spojenými domněnkami zavinění, které občanský zákoník předvídá. Nicméně i v těchto případech může k porušení tohoto práva dojít v souvislosti s plněním smluvních povinností, a bude se tak jednat o odpovědnost objektivní.

Vedle těchto nároků lze rovněž zvažovat nároky vzniklé z bezdůvodného obohacení anebo zákaz dotěrného obtěžování v rámci deliktů z nekalé soutěže.

Seznam zdrojů literatury

Používané právní předpisy

1. Listina základních práv Evropské unie (2012/C 326/02)
2. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
3. Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.
4. Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 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) (Text s významem pro EHP).
5. Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad "bezpečného přístavu" a s tím souvisejících "často kladených otázek" vydaných Ministerstvem obchodu Spojených států.
6. Sdělení č. 104/2013 Sb. m. s., Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě.
7. Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
8. Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

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

10. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), ve znění pozdějších předpisů.

11. Smlouva o Evropské unii (2016/C 202/01)

12. Smlouva o fungování Evropské unie (2016/C 202/01)

13. Úmluva o kybernetické bezpečnosti.

14. Úmluva o ochraně lidských práv a základních svobod (Evropská úmluva o lidských právech).

15. Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981).

16. Zákon 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů.

17. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

18. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

19. Zákon č. 110/2019 Sb., o zpracování osobních údajů.

20. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

21. Zákon č. 141/1950 Sb., občanský zákoník.

22. Zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

23. Zákon č. 269/2021 Sb., o občanských průkazech, ve znění pozdějších předpisů.

24. Zákon č. 361/2000 Sb., o silničním provoz, ve znění pozdějších předpisů.

25. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

26. Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

27. Zákon č. 100/1960 Sb., Ústava Československé socialistické republiky

28. Zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů.

29. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých souvisejících zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

30. Ústavní zákon č. 1/1993 Sb., Ústava České republiky.

31. Ústavní zákon č. 2/1993 Sb., usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení LISTINY ZÁKLADNÍCH PRÁV a SVOBOD jako součásti ústavního pořádku České republiky.

32. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.

33. Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad "bezpečného přístavu" a s tím souvisejících "často kladených otázek" vydaných Ministerstvem obchodu Spojených států.

Judikatura Evropského soudu pro lidská práva

34. Rozhodnutí ESLP ze dne 22. května 1990 ve věci 12726/87 - Autronic AG proti Švýcarsku.

35. Rozhodnutí ESLP ze dne 28. září 1990 ve věci 10890/84 - Groppera Radio AG a další proti Švýcarsku.

36. Rozhodnutí ESLP ze dne 16. 12. 1992, stížnost č. 13710/88 (Niemietz proti Německu).

37. Rozhodnutí ESLP ze dne 16. 12. 1997 ve věci Camenzind proti Švýcarsku č. 21353/93.

38. Rozhodnutí ESLP ze dne 4. května 2000 ve věci č. 28341/95 - Rotaru proti Rumunsku.

39. Rozhodnutí ESLP ze dne 24. června 2004 ve věci 59320/00 - Von Hannover proti Německu.

40. Rozhodnutí ESLP ze dne 6. června 2006 ve věci 62332/00 Segerstedt-Wiberg a další proti Švédsku.

41. Rozhodnutí ESLP ze dne 29. června 2006 ve věci Weber a Saravia proti Německu č. 54934/00.

42. Rozhodnutí ESLP ze dne 10. července 2006 ve věci 19101/03 - Sdružení Jihočeské matky proti České republice.

43. Rozhodnutí ESLP ze dne 3. dubna 2007 ve věci 62617/00 - Copland proti Velké Británii.

44. Rozhodnutí ESLP ze dne 1. července 2008 ve věci Liberty a další proti Spojenému království č. 58243/00.

45. Rozhodnutí ESLP ze dne 4. prosince 2008 ve věci 30562/04 - S. a Marper proti Spojenému království.

46. Rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 16248/05 Gardel proti Francii.

47. Rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 18. dubna 2013 M.K. proti Francii.

48. Rozhodnutí ESLP ze dne 17. prosince 2009 ve věci 5335/06 B.B. proti Francii.

49. Rozhodnutí ESLP ze dne 12. října 2010, ve věci 184/06 - Saaristo a ostatní proti Finsku.

50. Rozhodnutí ESLP ze dne 8. listopadu 2011 ve věci 18968/07 - Glass proti Spojenému království.

51. Rozhodnutí ESLP ze dne 7. února 2012 ve věci 39954/08 - Axel Springer proti Německu.

52. Rozhodnutí ESLP ze dne 7. února 2012 ve věci 40660/08 a 60641/08 – Von Hannover proti Německu.

53. Rozhodnutí ESLP ze dne 8. listopadu 2016 ve věci 18030/11 - Magyar Helsinki Bizottság.

54. Rozhodnutí ESLP ze dne 27. června 2017 ve věci č. 931/13 - Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku.

55. Rozhodnutí ESLP ze dne 5. září 2017 ve věci 61496/08 - Bărbulescu v. Romania.

56. Rozhodnutí ESLP ze dne 28. června 2018 ve věci 60798/10 a 65599/10 M.L. a W.W. proti Německu.

Judikatura Soudního dvora Evropské unie

57. Rozhodnutí SDEU ze dne 5. února 1963, ve věci C-26/62, Van Gend en Loos proti Nederlandse Administratis der Belastigen.

58. Rozhodnutí SDEU ze dne 15. července 1964, ve věci C-6/64, Costa proti ENEL.

59. Rozhodnutí SDEU ze dne 12. listopadu 1969 ve věci C-29/69 Erich Stauder proti Stadt Ulm - Sozialamt.

60. Rozhodnutí SDEU ze dne 10. října 1973 ve věci C-34/73, Fratelli Variola S.p.A. proti Amministrazione italiana delle Finanze.

61. Rozhodnutí SDEU ze dne 13. prosince 1979 ve věci C-44/79 Hauer.

62. Rozhodnutí SDEU ze dne 17. ledna 1984, VBVB proti Komisi Evropských společenství, Spojené věci 43/82 a 63/82.

63. Rozhodnutí SDEU ze dne 26. února 1986 ve věci 152/84, M. H. Marshall v. Southampton and South-West.

64. Rozhodnutí SDEU ze dne 18. června 1991, Elliniki Radiophonia Tiléorassi AE, C-260/89.

65. Rozhodnutí SDEU ze dne 4. října 1991 ve věci C-159/90 The Society for the Protection of Unborn Children Ireland Ltd.

66. Rozhodnutí SDEU ze dne 20. května 2003 ve věci C-465/00 Österreichischer Rundfunk.

67. Rozhodnutí SDEU ze dne 6. listopadu 2003, ve věci C-101/01 Bodil Lindqvist.

68. Rozhodnutí SDEU ze dne 29. ledna 2008 ve věci C-275/06 Promusicae.

69. Rozhodnutí SDEU ze dne 7. prosince 2010 ve spojených věcech C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) a Hotel Alpenhof GesmbH v Oliver Heller (C-144/09).

70. Rozhodnutí SDEU ze dne 25. října 2011 ve věci C-509/09 eDate Advertising a další.

71. Rozhodnutí SDEU ze dne 24. listopadu 2011 ve věci C-70/10 Scarlet Extended.

72. Rozhodnutí SDEU ze dne 30. května 2013 ve věci C-342/12 Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT).

73. Rozhodnutí SDEU ze dne 13. května 2014 ve věci C-131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

74. Rozhodnutí SDEU ze dne 8. dubna 2014 ve spojených věcech věcech C-293/12 a C-549/12 Digital Rights Ireland Ltd.

75. Rozhodnutí SDEU ze dne 17. července 2014 ve spojených věcech C-141/12 and C-372/12, YS (C-141/12) proti Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel (C-372/12) proti M, S.

76. Rozhodnutí SDEU ze dne 1. října 2015 ve věci C-230/14 Weltimmo.

77. Rozhodnutí SDEU ze dne 6. října 2015 ve věci C-362/14 Maximillian Schrems v Data Protection Commissioner.

78. Rozhodnutí SDEU ze dne 19. října 2016 ve věci C-582/14 Patrick Breyer v. Bundesrepublik Deutschland.

79. Rozhodnutí SDEU ze dne 21. prosince 2016, ve spojených věccech C-203/15 a C-698/15 Tele2 Sverige AB a Watson, kde SDEU odpovídal na předběžné otázky Spojeného království a Švédska.

80. Rozhodnutí SDEU ze dne 9. března 2017 ve věci C-398/15 Manni.

81. Rozhodnutí SDEU ze dne 10. července 2018 ve věci C-25/17 Tietosuojavaltuutettu.

82. Rozhodnutí SDEU ze dne 24. září 2019 ve věci C-136/17 - GC a další.

83. Rozhodnutí SDEU ze dne 16. července 2020 ve věci C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems.

84. Rozhodnutí SDEU ze dne 5. dubna 2022 ve věci C-140/20 Commissioner of the Garda Síochána and Others.

85. Stanovisko generálního advokáta Niila Jääskinena přednesené dne 25. června 2013 ve věci C-131/12 Google Spain.

86. Stanovisko generálního advokáta Paola Mengozziho ze dne 1. února 2018 ve věci C-25/17, Tietosuojavaltuutettu.

87. Stanovisko generálního advokáta Macieje Szpunara ze dne 10. ledna 2019 ve věci C-136/17 - GC a další.

Judikatura českých soudů

88. Nález Ústavního soudu ze dne 19. ledna 1994, sp. zn. Pl. ÚS 15/93.

89. Nález Ústavního soudu ze dne 1. listopadu 1995, sp. zn. II. ÚS 192/95.

90. Nález Ústavního soudu ze dne 10. října 1996, sp. zn. I. ÚS 181/95.

91. Nález Ústavního soudu ze dne 6. ledna 1998, sp. zn. I. ÚS 282/97.

92. Nález Ústavního soudu ze dne 3. září 1998, sp. zn. IV. ÚS 13/98.

93. Nález Ústavního soudu ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02.

94. Nález Ústavní soud ze dne 28. září 2005, sp. zn. I. ÚS 394/04.

95. Nález Ústavního soudu ze dne 17. července 2007, sp. zn. IV. ÚS 23/05.

96. Nález Ústavního soudu ze dne 10. července 2008, sp. zn. III. ÚS 3118/07.

97. Nález Ústavního soudu ze dne 1. prosince 2008, sp. zn. I. ÚS 705/06.

98. Nález Ústavního soudu ze dne 8. června 2010, sp. zn. Pl. ÚS 3/09.

99. Nález Ústavního soudu ze dne 6. září 2010, sp. zn. I. ÚS 1744/10.

100. Nález Ústavního soudu ze dne 15. listopadu 2010, sp. zn. I. ÚS 517/10.

101. Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

102. Nález Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11.

103. Nález Ústavního soudu ze dne 6. března 2012, sp. zn. I. ÚS 1586/09.

104. Nález Ústavního soudu ze dne 11. září 2012, sp. zn. II. ÚS 1375/11.

105. Nález Ústavního soudu ze dne 20. února 2018, I. ÚS 3819/14.

106. Nález Ústavního soudu ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17.

107. Nález Ústavního soudu ze dne 27. února 2019, sp. zn. IV ÚS 774/18.

108. Nález Ústavního soudu ze dne 14. května 2019, sp. zn. Pl ÚS 45/17.

109. Nález Ústavního soudu ze dne 23. června 2020, sp. zn. IV. ÚS 2257/18.

110. Nález Ústavního soudu ze dne 3. listopadu 2020, sp. zn. Pl. ÚS 10/17.

111. Rozsudek Nejvyššího soudu ze dne 26. července 2000, sp. zn. 30 Cdo 2304/99.

112. Rozsudek Nejvyššího soudu ze dne 3. září 2002, sp. zn. 28 Cdo 1375/2002.

113. Rozsudek Nejvyšší soudu ze dne 18. března 2007, sp. zn. 30 Cdo 1385/2006.

114. Rozsudek Nejvyššího soudu ze dne 28. ledna 2010, sp. zn. 30 Cdo 2095/2008.

115. Rozsudek Nejvyššího soudu ze dne 30. října 2012, sp. zn. 22 Cdo 583/2011.

116. Rozsudek Nejvyššího správního soudu ze dne 27. února 2014, sp. zn. 7 As 20/2013 – 23.

117. Rozsudek Nejvyššího správního soudu ze dne 9. 8. 2018, sp. zn. 9 Azs 49/2018 – 50.

118. Rozsudek Nejvyššího soudu ze dne 15. prosince 2020, 25 Cdo 27/2020.

119. Rozsudek Nejvyššího soudu ze dne 17. ledna 2020, 30 Cdo 2003/2018.

120. Rozsudek Nejvyššího správního soudu ze dne 5. března 2021, sp. zn. 5 As 440/2019.

121. Usnesení Nejvyššího soudu ze dne 26. června 2014, sp. zn. 23 Cdo 1323/2012.

122. Usnesení Ústavního soudu ze dne 26. dubna 2016, sp. zn. I. ÚS 971/16.

123. Usnesení Krajského soudu v Brně ze dne 7. října 2015, sp. zn. 70 Co 228/2015 – 38.

124. Usnesení Nejvyššího soudu ze dne 1. září 2020, sp. zn. 7 Tdo 865/2020.

125. Usnesení Nejvyššího soudu ze dne 25. srpna 2020, sp. zn. 8 Tdo 647/2020.

Monografie a komentářová literatura

126. ANDRES, Bedřich, Antonín HARTMANN, František ROUČEK a Jaromír SEDLÁČEK. Komentář k československému obecnému zákoníku občanskému a občanské právo platné na Slovensku a v Podkarpatské Rusi. Díl 1, (§§ 1 až 284). Praha: Linhart, 1935, 1192 s.

127. AUSLOOS, Jef. The ‘Right to be Forgotten’ – Worth remembering? Computer Law & Security Review. 2012, 28(2), 143–152. ISSN 0267-3649.

128. BANNON, Liam J. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign. 2006,

2(1), 3–15. ISSN 1571-0882, 1745-3755. s. 5.; COYNE, Nora H. Exploring the Notion of Forgetting. The Gettysburg College Student Publications [online]. 2017, (509). Dostupné z: http://cupola.gettysburg.edu/student_scholarship/509/.

129. BANNON, Liam J. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign. 2006, 2(1), 3–15. ISSN 1571-0882.

130. BARTOŇ, Michal, Jan KRATOCHVÍL, Martin KOPA, Maxim TOMOSZEK, Jiří JIRÁSEK a Ondřej SVAČEK. Základní práva. Praha: Leges, 2016, 608 s. ISBN 978-80-7502-128-1.

131. BLANCHETTE, Jean-François a JOHNSON, Deborah G. Data retention and the panoptic society: The social benefits of forgetfulness. The Information Society. 2002, 18(1), 33–45.

132. BLUME Peter, The inherent contradictions in data protection law, International Data Privacy Law, Volume 2, Issue 1, February 2012, Pages 26–34. [online]. [cit. 2022-04-03]. Dostupné z https://doi.org/10.1093/idpl/ipr020.

133. BORGES, Jorge Luis. Funes, muž se zázračnou pamětí. In: Jorge Luis BORGES Spisy I. Praha: Argo, 2009. ISBN 978-80-257-0146-1.

134. BORKOWSKI, S.C. Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching business ethics (Dordrecht) [online]. Dordrecht: Kluwer Academic Publishers, 1999, 3(4), 402-406 [cit. 2022-03-14]. ISSN 1382-6891. Dostupné z: doi:10.1023/A:1009843728384.

135. BRÄUTIGAM, Peter a Torsten KRAUL. Internet of Things. München: Verlag C.H. Beck oHG, 2021. ISBN 978-3-406-74898-1.

136. BRÜGGEMEIER, Gert. Protection of personality rights in the law of delict/torts in Europe: mapping out paradigms. Personality Rights in European Tort Law [online]. Cambridge University Press, 2010, 5-37

[cit. 2022-03-20]. ISBN 0521194911. Dostupné z: doi:10.1017/CBO9780511676161.005.

137. CARBONE, Chelsea E. To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age. Virginia Journal of Social Policy & the Law. 2015, 22, 525–560.

138. CASTELLANO, Pere Simón. The Right to Be Forgotten under European Law: a Constitutional Debate. 2012, Lex Electronica, číslo 16.1 [online]. [cit. 2022-04-02] Dostupné z: www.lex-electronica.org/docs/articles_300.pdf.

139. CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

140. CRAIG, Paul P. a G. (Gráinne) DE BÚRCA. EU law: text, cases, and materials. 5th ed. Oxford: Oxford University Press, 2011, clvii, 1155 s. ; 25 cm. ISBN 978-0-19-957699-9.

141. DEYOUNG, Colin a Ian SPENCE. (2004). Profiling information technology users: En route to dynamic personalization. Computers in Human Behavior. 20. 55-65. 10.1016/S0747-5632(03)00045-1.

142. DIENST, S. in KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0.

143. DIZIKES, Peter. Study: On Twitter, false news travels faster than true stories. [online]. 8.3.2018. [cit. 2022-02-18]. Dostupné z https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

144. DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016, xi, 338. ISBN 978-80-7400-610-4.

145. DVOŘÁK, Jan, Jiří ŠVESTKA a Michaela ZUKLÍNOVÁ. Občanské právo hmotné. Díl první, Obecná část. Praha: Wolters Kluwer ČR, 2013, 429 s. ISBN 978-80-7478-326-5.

146. ELISCHER, David a kol. Náhrada majetkové a nemajetkové újmy podle občanského zákoníku, zákoníku práce, v oblasti průmyslového vlastnictví a podle autorského zákona. 1. vyd. Praha: Leges, 2020, 381 s. ISBN 978-80-7502-382-7.

147. ELISCHER, David. Protiprávnost – co je jejím zdrojem v soukromém právu?. Časopis pro právní vědu a praxi [online]. Masaryk University Press, 2016, 24(4), 501-526 [cit. 2022-03-23]. ISSN 1210-9126. Dostupné z: doi:10.5817/CPVP2016-4-1.

148. ELVY, Stacy-Ann. "PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY." Columbia Law Review 117, no. 6 (2017): 1369–1459. http://www.jstor.org/stable/44392955.

149. ERDOS, David and GARSTKA, Krzysztof, The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frameworks (September 10, 2019). University of Cambridge Faculty of Law Research Paper No. 31/2019. [online]. 10.9.2019. [cit. 2022-02-20]. https://ssrn.com/abstract=3451269.

150. FILIP, Jan. Úvodní poznámky k problematice práva na soukromí. In: Vojtěch ŠIMÍČEK, ed. Právo na soukromí. Brno: Masarykova univerzita, 2011, s. 9–19. ISBN 978-80-210-6449-3.

151. FOSCH VILLARONGA, Eduard, KIESEBERG, Peter and LI, Tiffany, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten (August 13, 2017). Computer Security & Law Review (Forthcoming). Dostupné z: https://ssrn.com/abstract=3018186.

152. FREY, Carl Benedikt a Giorgio PRESIDENTE. The GDPR effect: How data privacy regulation shaped firm performance globally [online]. 10.3.2022 [cit. 2022-03-27]. Dostupné z: https://voxeu.org/article/how-data-privacy-regulation-shaped-firm-performance-globally.

153. FRIED, Charles. Privacy. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1968, 77(3), 475-493 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/794941.

154. FRONC, Jaromír. Google, právo být zapomenut a Listina základních práv EU. Revue pro právo a technologie [online]. 2020, 11(21) [cit. 2022-03-14]. ISSN 1805-2797. Dostupné z: doi:https://doi.org/10.5817/RPT2020-1-7.

155. G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. [online]. [cit. 2022-03-27]. Dostupný z https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

156. GAVISON, Ruth. Privacy and the Limits of Law. The Yale law journal [online]. New Haven, Conn: The Yale Law Journal Company, 1980, 89(3), 421-471 [cit. 2022-03-14]. ISSN 0044-0094. Dostupné z: doi:10.2307/795891.

157. GEALFOW, John Altair a Christian MAY. Anonymizace osobních údajů v soudních rozhodnutích. Revue pro právo a technologie [online]. 2019, 10(19), 3 [cit. 2022-03-16]. ISSN 1804-5383, s. 19. Dostupné z: https://www-ceeol-com.ezproxy.is.cuni.cz/search/viewpdf?id=797575.

158. GIERSCHMANN, Sibylle, Katharina SCHLENDER, Rainer STENTZEL a Winfried VEIL. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag, 2018. ISBN 978-3-8462-0639-3.

159. GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kol. Trestní zákoník. 2. vydání. Praha: C. H. Beck, 2012, s. 2303, marg. č. 1

160. H.R.4943 - CLOUD Act. Dostupné z https://www.congress.gov/bill/115th-congress/house-bill/4943.

161. HARAŠTA, Jakub, MYŠKA, Matěj. Budoucnost data retention. Trestněprávní revue, 2015, č. 10, s. 238-241.

162. HERBST. Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“). KÜHLING a BUCHNER. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. 2. vydání. 2018. ISBN 978-3-406-74994-0, s. 89-94.

163. HUSSEINI, Faisal, Michal BARTOŇ, Marian KOKEŠ a Martin KOPA. Listina základních práv a svobod: komentář. V Praze: C.H. Beck, 2021, xxxvii, 1413. ISBN 978-80-7400-812-2.

164. CHAN, Rosalie. The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

165. IT GOVERNANCE PRIVACY TEAM. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. Ely, Cambridgeshire, United Kingdom, IT Governance Publishing, 2016.

166. JONES, Meg Leta. You are what Google says you are: The right to be forgotten and information stewardship. International Review of Information Ethics. 2012, 17, 22–30.

167. KAMINSKA, Izabella. Cambridge Analytica probe finds no evidence it misused data to influence Brexit. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.ft.com/content/aa235c45-76fb-46fd-83da-0bdf0946de2d.

168. KMEC, Jiří. Evropská úmluva o lidských právech: komentář. Praha: C.H. Beck, 2012, xxvii, 1660 s. ISBN 978-80-7400-365-3.

169. KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4. podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6.

170. KNAP, Karel, Jiří ŠVESTKA, Oldřich JEHLIČKA, Pavel PAVLÍK a Vladimír PLECITÝ. Ochrana osobnosti podle občanského práva. 4.

podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, 435 s. ISBN 80-7201-484-6.

171. KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. Soudní rozhledy, 2019, č. 6.

172. KOOPS, Bert-Jaap Koops a Ronald LEENES (2014) Privacy regulation cannot be hardcoded. a critical comment on the 'privacy by design' provision in data-protection law, International Review of Law, Computers & Technology, 28:2, 159-17.

173. KORENHOF, Paulan, AUSLOOS, Jef, SZEKELY, Ivan, JONES, Meg Leta, SARTOR, Giovanni a LEENES, Ronald E. Timing the Right to Be Forgotten: a Study into „Time" as a Factor in Deciding About Retention or Erasure of Data [online]. SSRN Scholarly Paper. ID 2436436. Rochester, NY: Social Science Research Network. 2014 [cit. 21. 3. 2022]. Dostupné z: https://papers.ssrn.com/abstract=2436436.

174. KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. Praha: C.H. Beck, 2012, xvii, 516 s. ; 23 cm. ISBN 978-80-7179-226-0.

175. KUGLER, Tobias a Daniel RÜCKER. New European general data protection regulation: a practitioner's guide. München: C.H. Beck, 2018, 219 s. ISBN 978-3-406-69536-0.

176. KÜHN, Zdeněk. Ochrana soukromí v internetové době. In ŠIMÍČEK, Vojtěch. Právo na soukromí. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. 212 s. ISBN 8021054492110.

177. KÜHN, Zdeněk. Transformace pojmu soukromí na počátku třetího milénia. Jurisprudence. 2017, XXVI(2). ISSN 1802-3843. s. 7.

178. LAVICKÝ, Petr, Jakub HANDRLICA, Jiří SPÁČIL, et al. Občanský zákoník ..: komentář. 2. vydání. V Praze: C.H. Beck, 2020 - 2022, 4 svazky. ISBN 978-80-7400-852-8, s. 290.

179. LESS, Noel. SEO News – Why second page of Google might as well be the last [online]. [cit. 2022-03-16]. https://www.designforonline.com/seo-second-page-google-might-be-last/.

180. LEVERAGE MARKETING. How Far Down the Search Engine Results Page Will Most People Go? [online]. [cit. 2022-03-16]. Dostupné z https://www.theleverageway.com/blog/how-far-down-the-search-engine-results-page-will-most-people-go/, obdobně pak rovněž

181. LI, Wenlong. a tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation. International Data Privacy Law [online]. 2018, 2. července 2018, (Volume 8, 4,), 309-317 [cit. 2022-04-03]. ISSN 2044-4001. Dostupné z: https://academic.oup.com/idpl/article/8/4/309/5047861?login=true#no-access-message#no-access-message.

182. MALDOFF, G., CIPP/US, Top 10 operational impacts of the GDPR, part 6 – RTFB and data portability, iapp.org, 25. 1. 2016.

183. MATEJKA, Ján, Alžběta KRAUSOVÁ a Vojen GÜTTLER. Biometric data and its specific legal protection. Praha: Institute of State and Law of the Czech Academy of Sciences, [2020]. ISBN 978-80-87439-43-2.

184. MATEJKA, Ján. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. Praha: CZ.NIC, 2013, 256 s. ; 25 cm. ISBN 978-80-904248-7-6.

185. MATYSOVÁ, Monika, Robert NEŠPŮREK a Richard OTEVŘEL. Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj: 24.05.2017 [online]. [cit. 2022-03-16]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj.

186. MAYER-SCHÖNBERGER, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2011. ISBN 978-1-4008-3845-5.

187. MELZER, Filip a Petr TÉGL. Občanský zákoník: velký komentář. Svazek I, § 1-117 /Filip Melzer, Petr Tégl a kolektiv. 2013. ISBN 978-80-87576-73-1.

188. MEREDITS, Sam. Facebook-Cambridge Analytica: a timeline of the data hijacking scandal. [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

189. MITROU, Lilian a Maria KARYDA. EU's Data Protection Reform and the right to be forgotten—A legal response to a technological challenge?. 5th International Conference of Information Law and Ethics. 2012, str. 29 - 30 [online]. [cit. 2022-04-02] Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245.

190. MOORE, Adam. Defining Privacy. Journal of Social Philosophy. 2008, 39(3), 411–428. ISSN 00472786, 14679833. s. 413 ; DECEW, Judith. Privacy. In: Edward N. ZALTA, ed. The Stanford Encyclopedia of Philosophy [online]. Spring 2018. B.m.: Metaphysics Research Lab, Stanford University, 2018, dostupné z: https://plato.stanford.edu/archives/spr2018/entries/privacy/.

191. NONNEMANN, František. Osobní údaje jako platidlo?. Právní rozhledy, 2020, č. 5, s. 174-180.

192. NONNEMANN, František. Využití nahrávky fyzické osoby jako důkazního prostředku z pohledu ochrany osobních údajů. Právní rozhledy [online]. 2015 [cit. 2022-03-26].

193. NONNEMANN, František. Zpracování veřejně dostupných osobních údajů a GDPR. Právní rozhledy. 2018(5). ISSN 1210-6410.

194. NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014, xx, 484 s.; 24 cm. ISBN 978-80-7478-665-5, s XVII.

195. NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář. Praha: Wolters Kluwer, 2017, xvi, 525. ISBN 978-80-7552-765-3, s. 122.

196. PAGALLO, Ugo a DURANTE, Massimo. Legal memories and the right to be forgotten. In: Luciano FLORIDI, ed. Protection of Information and the Right to Privacy-A New Equilibrium? B.m.: Springer, 2014, s. 17–30. ISBN 978-3-319-05719-4.

197. PARKER, Elizabeth S., CAHILL, Larry a MCGAUGH, James L. a case of unusual autobiographical remembering. Neurocase. 2006, 12(1), 35–49.

198. PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ a Jiří ČERNÝ. Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě. Praha: Leges, 2018, 487 stran ; 21 cm. ISBN 978-80-7502-288-2.

199. PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. Obecné nařízení o ochraně osobních údajů (GDPR); Zákon o zpracování osobních údajů: komentář. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. ISBN 978-80-7502-396-4, s. 140

200. PATTYNOVÁ, Jana, Vladan RÁMIŠ, František NONNEMANN a Dominik VÍTEK. Zpracování údajů o politických názorech voličů na sociálních sítích pro volební kampaně [online]. 3.1.2019 [cit. 2022-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-udaju-o-politickych-nazorech-volicu-na-socialnich-sitich-pro-volebni-kampane-108618.html.

201. PAVLÍČEK, Václav, Ján GRONSKÝ, Jiří HŘEBEJK, et al. Ústavní právo a státověda. II. díl, Ústavní právo České republiky. 3. vydání. Praha: Leges, 2020, 1160 s. ISBN 978-80-7502-468-8, s. 524.

202. PEGUERA, Miquel. No More right-to-be-forgotten for Mr. Costeja, Says Spanish Data Protection Authority. The Center for Internet and Society, Stanford Law School, 2015 [online]. [cit. 2022-01-24]. Dostupné z: http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority.

203. PERRYER, Sophie. The internet never forgets, but people do. [online]. 13.11.2018. [cit. 2022-01-18].

https://www.theneweconomy.com/technology/the-internet-never-forgets-but-people-do

204. PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 125.

205. PINO, Giorgio. The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights [online]. SSRN Scholarly Paper. ID 1737392. Rochester, NY: Social Science Research Network. 2000 [vid. 2022-04-02]. Dostupné z: https://papers.ssrn.com/abstract=1737392.

206. POKORNÁ, Andrea. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek. Praha: Wolters Kluwer ČR, 2020, xviii, 331. ISBN 978-80-7598-309-1, s. 9.

207. POLČÁK, Radim. Getting European data protection off the Ground. International Data Privacy Law [online]. 2014, (Volume 4, 4,), 282–289 [cit. 2022-04-03]. ISSN 2044-4001. Dostupné z: https://academic.oup.com/idpl/article-abstract/4/4/282/2569059.

208. POLČÁK, Radim. Informace a data v právu. Revue pro právo a technologie [online]. 2016, 7(13/2016), 67-91 [cit. 2022-04-03]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4946/pdf.

209. REES Christopher, Tomorrow's privacy: personal information as property, International Data Privacy Law, Volume 3, Issue 4, November 2013, Pages 220–221. [online]. [cit. 2022-04-03]. Dostupné z https://doi.org/10.1093/idpl/ipt022.

210. ROSEN, Jeffrey. The Right to Be Forgotten. Stanford Law Review Online. 2011, 64, 88–92. s. 88.;

211. ROZEHNAL, Ales. Mediální právo, 2. vydání. ISBN 80-7380-549-9.

212. SALM, Lauren. 70% of employers are snooping candidates' social media profiles. Career Builder [online]. [cit. 1. 3. 2019]. Dostupné z: https://www.careerbuilder.com/advice/social-media-survey-2017.

213. SCHACTER, Daniel L., CHIAO, Joan Y. a MITCHELL, Jason P. The seven sins of memory: implications for self. Annals of the New York Academy of Sciences. 2003, 1001, 226–239. ISSN 0077-8923.

214. SCHRÖNDINGER, Erwin. What is life. Cambridge University Press, 1944. ISBN 0-521-42708-8.

215. SCHWARTZ, Paul M. and SOLOVE, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information (December 5, 2011). New York University Law Review, Vol. 86, p. 1814, 2011, UC Berkeley Public Law Research Paper No. 1909366, GWU Legal Studies Research Paper No. 584, GWU Law School Public Law Research Paper No. 584. [online]. [cit. 2022-04-03]. Dostupné z: https://ssrn.com/abstract=1909366.

216. SOLOVE, D. J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004.

217. SOLOVE, Daniel J. a Taxonomy of Privacy. University of Pennsylvania law review [online]. Philadelphia: University of Pennsylvania Law School, 2006, 154(3), 477-564 [cit. 2022-03-14]. ISSN 0041-9907. Dostupné z: doi:10.2307/40041279.

218. SOLOVE, Daniel J. Conceptualizing Privacy. California law review [online]. Berkeley: School of Law, University of California, Berkeley, 2002, 90(4), 1087-1155 [cit. 2022-03-14]. ISSN 0008-1221. Dostupné z: doi:10.2307/3481326.

219. SOLOVE, Daniel J. The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure. Duke law journal [online]. Duke University School of Law, 2003, 53(3), 967-1065 [cit. 2022-03-14]. ISSN 0012-7086.

220. SZEKELY, Ivan. The right to forget, the right to be forgotten. In: Serge GUTWIRTH, Ronald LEENES, Paul DE HERT a Yves POULLET, ed. European Data Protection: In Good Health? B.m.: Springer, 2012, s. 347–363. ISBN 978-94-007-2902-5.

221. ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012, 2 sv. (xvi, 1450, xiv s., s. 1451-3586). ISBN 978-80-7400-428-5.

222. ŠOŠOLÍKOVÁ, Hana. „The Right to Be Forgotten“ jako řešení problému permanence informací. Brno: Revue pro právo a technologie, 2013, 7. číslo, str. 3 – 12.

223. ŠVESTKA, Jiří, Jan DVOŘÁK, Irena PELIKÁNOVÁ, et al. ČESKO. Občanský zákoník: komentář. Svazek I. Praha: Wolters Kluwer ČR, 2013, s 1736. ISBN 978-80-7478-369-2.

224. TAMO, Aurelia a GEORGE, Damian. Oblivion, Erasure and Forgetting in the Digital Age. Journal of Intellectual Property, Information Technology and Electronic Commerce Law. 2014, 5, 71–87.

225. TELEC, Ivo. Držba informací. Právní rozhledy. 2014, (4/2014), 115. ISSN 1210-6410.

226. TELEC, Ivo. Není informace jako informace. Právní rozhledy. 2014, (15-16/2014), 515. ISSN 1210-6410 nebo TELEC, Ivo. Držba informací. Právní rozhledy. 2014, (4/2014), 115. ISSN 1210-6410.

227. TENE, Omer. What Google Knows: Privacy and Internet Search Engines. Utah Law Review. 2008, 2008, 1433–1492;

228. THOMSON, Judith Jarvis. The Right to Privacy. Philosophy & Public Affairs. 1975, 4(4), 295–314. ISSN 0048-3915.

229. TICHÝ, Luboš, Rainer ARNOLD, Jiří ZEMÁNEK, Richard KRÁL a Tomáš DUMBROVSKÝ. Evropské právo. 5. přeprac. vyd. Praha: C.H. Beck, 2014, xlii, 756 s. ISBN 978-80-7400-546-6.

230. TOMAN, Petr a Stanislav DEVÁTÝ. Ochrana dobré pověsti a názvu právnických osob. 2. aktualiz. a dopl. vyd. Praha: Linde, 2001, 199 s. ISBN 80-7201-297-5.

231. UŘIČAŘ, Miroslav a Vladan RÁMIŠ. Obecné nařízení o ochraně osobních údajů: komentář. Praha: C. H. Beck, 2021, xxvii, 1386. ISBN 978-80-7400-815-3.

232. USTARAN, Eduardo. European Data Protection: Law and Practice (Electronic Copy). Portsmouth: IAPP Publications, 2018. ISBN 978-0-9983223-7-7.

233. VÁLOVÁ, Irena. Klíčový spor o „vlastnictví" dat v cloudu. USA vs. Microsoft a zbytek světa. [online]. 18.5.2016. [cit. 2022-04-03]. Dostupné z https://ekonomickydenik.cz/klicovy-spor-o-vlastnictvi-dat-v-cloudu-microsoft-vs-usa-a-zbytek-sveta/.

234. VÍTEK, Dominik a Jana PATTYNOVÁ. Využívání zveřejněných osobních údajů [online]. 14.6.2019 [cit. 2022-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/vyuzivani-zverejnenych-osobnich-udaju-109518.html.

235. VÍTEK, Dominik, SUCHÁNKOVÁ, Lenka. Advokátní tajemství v cloudu. Bulletin advokacie, 2020, č. 12, s. 19-22.

236. VLACHOVÁ, Barbora a Martin MAISNER. Zákon o zpracování osobních údajů: komentář. V Praze: C.H. Beck, 2019, xviii, 145. ISBN 978-80-7400-760-6, s. 54 – 58.

237. VOIGT, Paul a Axel VON DEM BUSSCHE. The EU General Data Protection Regulation (GDPR): a Practical Guide [online]. Springer International Publishing AG 2017. [cit. 2022-03-16]. ISBN 978-3-319-57959-7.

238. WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK a Ivo POSPÍŠIL. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer ČR, 2012, xxv, 906 s. ; 24 cm. ISBN 978-80-7357-750-6, s. 186.

239. WARREN, Samuel D. a BRANDEIS, Louis D. Right to privacy. Harv. L. Rev. 1890, 4, s. 193, dostupné online z https://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

240. WARMAN, M. (2012) Vint Cerf attacks European internet policy. Telegraph. [online]. 29.3.2012.[cit. 2022-02-18]. Dostupné z www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html.

241. WESTIN, Alan. Privacy and Freedom. New York: Ig Publishing, 2015. ISBN 978-1-935439-97-4. s. 35.

242. WHELANOVÁ, M. Účinky unijního práva ve světle judikatury Soudního dvora. 2011. Dostupné z https://www.mvcr.cz/clanek/ucinky-unijniho-prava-ve-svetle-judikaturysoudniho-dvora.aspx.

243. WHITMAN, J. Q. Human dignity in Europe and United States: the social foundations, in NOLTE, G. European.

244. XANTHOULIS, Napoleon. Conceptualising a Right to Oblivion in the Digital World: a Human Rights-Based Approach [online]. SSRN Scholarly Paper. ID 2064503. Rochester, NY: Social Science Research Network. 2012 [vid. 2022-04-01]. Dostupné z: https://papers.ssrn.com/abstract=2064503.

245. ZALNIERIUTE, Monika, Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security (April 14, 2021). Vanderbilt Journal of Transnational Law, (2022) 55(1), pp. 1- 48 , UNSW Law Research, Available at SSRN: https://ssrn.com/abstract=3826878.

Další citované zdroje

246. Bürgerliches Gesetzbuch (BGB). Dostupné z https://www.gesetze-im-internet.de/bgb/__90.html.

247. California Consumer Privacy Act. Assembly Bill No. 375. [online]. [cit. 2022-03-14]. Dostupný z

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

248. CAMBRIDGE DICTIONARY. Data. [online]. [cit. 2022-04-03]. Dostupné z https://dictionary.cambridge.org/dictionary/english/data.

249. CAMBRIDGE DICTIONARY. Information. [online]. [cit. 2022-04-03]. Dostupné z https://dictionary.cambridge.org/dictionary/english/information

250. Council of Europe, European Union Agency for Fundamental Rights: "Handbook on European data protection law" Luxembourg, 2018, ISBN 978-92-871-9849-5, s. 93.

251. Data Act: Commission proposes measures for a fair and innovative data economy. [online]. 23.2.2022. [cit. 2022-04-05]. Dostupné z https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

252. Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU ze dne 10. listopadu 2020, dostupné z https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_cs.pdf.

253. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework ze dne 25. 3. 2020 [online]. Dostupné z https://ec.europa.eu/commission/presscorner/detail/cs/ip_22_2087.

254. EUROPEAN COURT OF HUMAN RIGHTS. Guide to the Case-Law of the of the European Court of Human Rights. Data Protecion. [online]. 31.12.2021. [cit- 2022-04-03]. Dostupné z https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

255. Guidelines 05/2020 on consent under Regulation 2016/679. [online]. [cit. 2022-03-14]. Dostupné z https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

256. H.R.4943 - CLOUD Act. Dostupné z https://www.congress.gov/bill/115th-congress/house-bill/4943.

257. INFORMATION COMMISSIONER'S OFFICE. Investigation into the use of data analytics in political campaigns [online]. 10.4.2018. [cit. 2022-04-01]. Dostupné z https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

258. Instrukce Ministerstva spravedlnosti ze dne 24. července 2009, č.j. 13/2008-SOSV-SP,kterou se provádějí některá ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

259. Ke zpracování osobních údajů bývalých zaměstnanců, ÚOOÚ dne 21. března 2013, https:// www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=1585&n=ke-zpracovani-osobnich-udaju-byvalych-zamestnancu.

260. Kontrola zpracování veřejně přístupných údajů (společnost Úspěch Online s.r.o.). [online]. [cit 2019-06-01]. Dostupné z https://www.uoou.cz/kontrola-zpracovani-verejne-pristupnych-udaju-spolecnost-uspech-online-s-r-o/ds-5420/archiv=0&p1=5452.

261. Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452.

262. Licenci lze udělit k know-how (nebo obchodnímu tajemství. VÝTISK in PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. V Praze: C.H. Beck, 2017, lxii, 3081. ISBN 978-80-7400-653-1, s 2373.

263. Návrh nařízení Evropského parlamentu a Rady o evropské správě dat. [online]. 25.11.2020. [cit. 2022-04-05]. Dostupné z https://eur-

lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.

264. Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU a RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), dostupný z https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017PC0010&from=EN.

265. Pokyny č. 5/2019 ke kritériím práva být zapomenut v případech vyhledávačů podle nařízení GDPR (část 1), verze 2.0, přijato dne 7. července 2020, v českém znění dostupné z https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_cs.pdf.

266. Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 0829/14/CS, WP216, Stanovisko č. 5/2014 k technická anonymizace [online]. 10. dubna 2014 [cit. 2022-03-16]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

267. Pracovní skupina pro ochranu osobních údajů zřízené podle čl. 29, čj. 00720/12/EN, WP 193, Stanovisko č. 3/2012 k vývoji biometrických technologií, ze dne 27. dubna 2012, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_cs.pdf.

268. Pracovní skupina pro ochranu osobních údajů zřízené podle čl. 29, čj. 844/14/CS, WP 217, Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES, ze dne 9. dubna 2014, dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf.

269. Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. [online].

21.4.2021. [cit. 2022-03-18]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN#:~:text=It%20proposes%20a%20single%20future,the%20purpose%20of%20law%20enforcement.

270. Příručka evropského práva v oblasti ochrany osobních údajů. [online]. [cit. 2022-02-12]. Dostupná z https://www.echr.coe.int/Documents/Handbook_data_protection_CES.PDF.

271. Rozhodnutí Nejvyššího soudu USA ze dne 4. července 2018, ve věci United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018). Dostupné z https://casetext.com/case/united-states-v-microsoft-corp-9.

272. Rozhodnutí Úřadu pro ochranu osobních údajů, ve věci Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452. Úřad pro ochranu osobních údajů v této věci dospěl k závěru, že informační povinnost (bez uvedení dalších detailů) byla splněna dostatečně.

273. Rozsudek High Court, Queen's Bench Division ze dne 16. 1. 2014, [2014] EWHC 13 (QB), Vidal-Hall v Google Inc.

274. Rozsudek Nejvyššího soudu USA United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

275. Singapore - Data Protection Overview. [online]. [cit. 2022-03-14]. Dostupné z https://www.dataguidance.com/notes/singapore-data-protection-overview.

276. South Africa - Data Protection Overview. [online]. [cit. 2022-03-14]. https://www.dataguidance.com/notes/south-africa-data-protection-overview.

277. Stanovisko Úřadu pro ochranu osobních údajů K využívání rodných čísel [online]. 21.3.2013. Dostupné z https://www.uoou.cz/k-vyuzivani-

rodnych-cisel/d-1600#:~:text=Vzhledem%20k%20tomu%2C%20%C5%BEe%20rodn%C3%A9,lex%20specialis%20k%20tomuto%20z%C3%A1konu.

278. Stanovisko Úřadu pro ochranu osobních údajů ve věci „Zpracování politických názorů voličů pro kampaň je možné jen s jejich souhlasem“. [online]. 2.10.2018. [cit 2019-06-01]. Dostupné z https://www.uoou.cz/zpracovani-politickych-nazoru-volicu-pro-nbsp-kampan-je-mozne-jen-s-nbsp-jejich-souhlasem/d-31947.

279. Stanovisko WP29 „Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain“ ze dne 16. prosince 2015, 176/16/EN. [online]. [cit. 2022-03-14]. Dostupné z https://ec.europa.eu/newsroom/article29/redirection/document/56127.

280. Thailand - Data Protection Overview. [online]. [cit. 2022-03-14]. Dostupné z https://www.dataguidance.com/notes/thailand-data-protection-overview.

281. The world’s most valuable resource is no longer oil, but data. [online]. 6.5.2017 [cit. 2022-03-16]. Dostupné z https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

282. The world’s most valuable resource is no longer oil, but data. [online]. 6.5.2017 [cit. 2022-03-16]. Dostupné z https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

283. Úřad pro ochranu osobních údajů ve věci „Předávání osobních údajů do jiných zemí“. [online]. [cit. 2022-03-14]. dostupné z https://www.uoou.cz/10-predavani-osobnich-udaju-do-jinych-zemi/d-27284.

284. Vodítka WP29 č. 225 ze dne 16. listopadu 2016 k implementaci rozsudku Soudního dvora Evropské unie ve věci Google Spain a Inc v.

Agencia Española de Protección de Datos (AEPD) a Mario Costeja Gonzáles

285. Závěry Úřadu pro ochranu osobních údajů ve věci Kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků (Mladá fronta a.s.), dostupné z https://www.uoou.cz/kontrola-zverejnovani-osobnich-udaju-na-internetu-v-tzv-klonech-verejnych-rejstriku-mlada-fronta-a-s/ds-5402/archiv=0&p1=5452.

Abstrakt – Právo být zapomenut jako součást ochrany osobnosti

Právo být zapomenut je nový fenomén formulovaný poprvé Soudním dvorem Evropské unie v případu Google Spain z roku 2014. Toto právo bylo následně zakotveno v obecném nařízení o ochraně osobních údajů, díky čemuž se stalo jako zákonný institut univerzálně aplikovatelné na území EU i EHP od 25. května 2018. Tato práce se však nezaměřuje jen na otázku ochrany osobních údajů (dle GDPR), ale zvažuje rovněž otázky, zda právo být zapomenut tvoří součást ochrany osobnosti a práva na ochranu soukromí jako takové, tedy chráněného na lidskoprávní úrovni. Z tohoto hlediska práce dále zvažuje, zda toto právo náleží rovněž právnickým osobám. Tyto otázky jsou poměřovány na základě testu proporcionality základních lidských práv – tedy práva na soukromí (vycházejícího zároveň z obecných principů nedotknutelnosti člověka a jeho důstojnosti) v porovnání s dalšími lidskými právy, jako jsou zejména právo na svobodu projevu a právo na informace, které je nezbytné přu uplatňování práva být zapomenut zvažovat. Při aplikace práva být zapomenut je přitom nezbytné vycházet z jeho účelu a ze základních principů soukromí a jeho ochrany, stejně jako z funkce zapomínání, které je významné nejen pro konkrétní jednotlivce, ale pro fungování společnosti jako celku.

Tyto otázky jsou přitom kladeny v kontextu právní povahy dat (a osobních údajů) a nových technologií zpracovávajícími taková data na každodenní bázi. Moderní technologie tak mohou narážet na zásadní limity vyplývající z podstaty nemožnosti zapomínat (jelikož stroje, na rozdíl od lidí, nezapomínají). Hodnota dat navíc, která jsou považovaná za „novou ropu“ navíc začíná být nedocenitelná a pro další vývoj technologií přitom stěžejní. Např. tedy rozvoj umělé inteligence může přinést zásadní výzvy pro další existenci soukromí a zapomínání (v pojetí práva být zapomenut), jak jej vnímáme dnes.

Tato práce se rovněž zabývá důsledky porušení práva být zapomenut se zaměřením zejména na náhradu újmy, pro níž GDPR rovněž poskytuje specifickou úpravu v oblasti ochrany osobních údajů.

Klíčová slova: právo být zapomenut, výmaz, data, GDPR, osobní údaje, soukromí, osobnost, technologie

Abstract – Right to be forgotten as part of personality rights

Right to be forgotten (or also right to oblivion) is a new phenomenon formed by the Court of Justice of the European Union in 2014 in the case of Google Spain. The right was then enacted as part of the General Data Protection Regulation and consequently became applicable throughout the EU and EEA since 25 May 2018. This thesis goes beyond the scope of personal data protection (under the GDPR) and considers whether the right to be forgotten forms a part of the personality and the right to privacy as such, thus being protected as a fundamental human right. On this basis, it also considers whether not only individuals but also legal entities could benefit from the right to be forgotten. These questions are assessed in view of the conflict of fundamental human rights and their proportionality test – right to privacy (also relying on and stemming from human inviolability and dignity) as balanced against other human rights, in particular, freedom to speech and freedom of information that need to be evaluated when performing the right be forgotten. It is also necessary to consider the purpose and fundamental principles of privacy and its protection and the purpose of forgetting and its meaning for individuals and society as a whole.

All these questions are dealt with in view of the legal nature of (personal) data and new technologies processing such data on a daily basis. Modern technologies may reach the limits stemming from their incapability to forget (as the machines, unlike humans, never forget). Moreover, data is a "new oil" and its value is priceless while being crucial for further technology development. By way of example, any further development of artificial intelligence may be especially challenging for future shapes of privacy and forgetting (as applicable under the right to be forgotten).

The thesis also deals with the consequences of infringement of this right, mainly focusing on damages that are also specifically governed under the GDPR for the area of personal data protection.

Key words: right to be forgotten, right to oblivion, erasure, data, gdpr, personal data, privacy, personality, technology