

Vysoká škola ekonomická v Praze

Národohospodářská fakulta

Hlavní specializace: Veřejná správa



PRÁVO BÝT ZAPOMENUT V KONTEXTU
ELEKTRONIZACE VEŘEJNÉ SPRÁVY V ČR
diplomová práce

Autor: Bc. Barbora Vycpálková

Vedoucí práce: Mgr. Tomáš Lechner, Ph.D.

Rok: 2017

Prohlašuji na svou čest, že jsem diplomovou práci vypracovala samostatně a s použitím uvedené literatury.

Bc. Barbora Vycpálková

V Praze, dne 30. 8. 2017

Poděkování

Úvodem bych chtěla poděkovat vedoucímu diplomové práce, Mgr. Tomáši Lechnerovi, Ph.D., za cenné rady, ochotu, vstřícnost a trpělivost během zpracovávání této práce. Velký dík patří také celé mé rodině a přátelům, kteří mě podporovali během celého studia.



ZADÁNÍ DIPLOMOVÉ PRÁCE

Zpracovatelka: **Bc. Barbora Vycpálková**
Studijní program: **Ekonomie a hospodářská správa**
Obor: **Veřejná správa**
Název tématu: **Právo být zapomenut v kontextu elektronizace veřejné správy v ČR**

Zásady pro vypracování:

1. Oblast ochrany osobních údajů je s ohledem na rostoucí stupeň elektronizace společnosti a s tím také veřejné správy velice důležitá. Od května 2018 ji bude regulovat nové Nařízení Evropského parlamentu a Rady EU 2016/679, které nahradí dosavadní národní právní úpravy. Nové nařízení se již přímo vyjadřuje také k právu být zapomenut.
2. Cílem práce je postihnout právo být zapomenut v kontextu rozvoje elektronizace veřejné správy v ČR a v návaznosti na novou evropskou právní úpravu. V práci bude provedena základní analýza dopadů nového nařízení na české předpisy s ohledem na aplikaci práva být zapomenut. Dále bude provedena analýza registrů veřejné správy ve vztahu k aplikaci tohoto práva.
3. Práce bude rozdělena do tří částí. V první části budou popsány aspekty práva být zapomenut a sumarizovány dosavadní výzkumy v této oblasti. Následně bude představena postupující elektronizace veřejné správy v ČR a vztah ke zmíněnému právu. V druhé části bude představeno Nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a jeho dopady na aktuálně platné české předpisy regulující tuto oblast (zejména zákon o ochraně osobních údajů). V třetí části bude provedena analýza vybraných registrů veřejné správy ve vztahu k aplikaci práva být zapomenut. Následně budou získané výsledky syntetizovány do doporučení aplikování práva být zapomenut v kontextu elektronizace veřejné správy v ČR.

Rozsah práce: 70

Seznam odborné literatury:

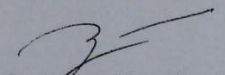
1. MATES, P. – SMEJKAL, V. *E-government v České republice : právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6.
2. VLÁČIL, J. *Veřejná správa: sociálně-psychologické problémy v historii a současnosti*. Praha: Linde, 2002. 322 s. ISBN 80-7201-379-3.
3. Jef Ausloos, The 'Right to be Forgotten' – Worth remembering?, *Computer Law & Security Review*, Volume 28, Issue 2, April 2012, Pages 143–152
4. Lee, Edward, Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten (July 28, 2015). *UC Davis Law Review*, Forthcoming; Chicago-Kent College of Law Research Paper No. 2015-13. Available at SSRN: <http://ssrn.com/abstract=2636856>
5. Mates, P, Janečková, E., Bartík, V. *Ochrana osobních údajů*. Praha: Leges, 2012. ISBN 978-80-87576-12-0.

Datum zadání diplomové práce:

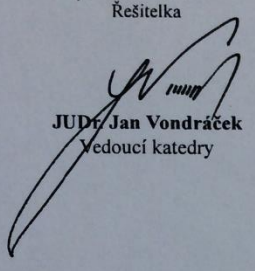
říjen 2016

Termín odevzdání diplomové práce:

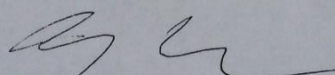
květen 2017



Bc. Barbora Vycpálková
Řešitelka



JUDr. Jan Vondráček
Vedoucí katedry



Mgr. Tomáš Lechner, Ph.D.
Vedoucí práce

doc. Ing. Miroslav Ševčík, CSc.
Děkan NF VŠE

Abstrakt

Tématem práce je institut práva být zapomenut, a to zejména v kontextu shromažďování dat veřejnou správou v České republice. Základem je analýza vybraných registrů veřejné správy, jimiž jsou insolvenční rejstřík, rejstřík trestů a evidence přestupků ve vztahu k tomuto právu. První část práce se věnuje sociologickým a historickým souvislostem, národnímu i komunitárnímu právnímu rámci a rozboru dosavadních výzkumů ve zkoumané oblasti. Ve druhé části jsou analyzovány vybrané databáze a na základě souvisejících právních předpisů jsou diskutovány možnosti a úskalí aplikace práva být zapomenut.

Klíčová slova

e-government, veřejná správa, právo být zapomenut, registry veřejné správy

Summary

This thesis deals with the institute of the right to be forgotten, especially in the context of collecting data by the public administration in the Czech Republic. There are analysed selected public registers, such as insolvency register, criminal record and offenses record, in relation to this right. The first part of the thesis deals with sociological and historical aspects, state and community legal framework and the analysis of the existing research in the considered area. In the second part, selected registers are analyzed. On the basis of related law regulations, possibilities and pitfalls of application of the right to be forgotten are discussed.

Key Words

e-government, public administration, right to be forgotten, public registers

JEL klasifikace

H83, L86, K24, O38

Obsah

Úvod	9
1 Ochrana osobních údajů všeobecně	11
1.1 Právo na soukromí v současném právním prostředí	11
1.2 Právo na soukromí vs. právo na informace.....	12
2 Právní zakotvení ochrany osobních údajů.....	14
2.1 Historie ochrany osobních údajů	14
2.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů	15
2.2.1 Úřad pro ochranu osobních údajů.....	17
2.2.2 Působnost.....	17
2.2.3 Základní pojmy.....	18
2.2.4 Práva a povinnosti při zpracování osobních údajů	20
3 Nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR).....	21
3.1 Porovnání stávajících a nových definic	27
3.2 Fáze implementace	29
4 Právo být zapomenut v celkovém pojetí	31
4.1 Studie č. 1: Rozdílné vnímání evropských a amerických občanů	31
4.2 Studie č. 2: Regulační faktory ovlivňující právo být zapomenut	33
4.3 Studie č. 3: Možnosti nahlížení na institut soukromí.....	36
4.4 Sumarizace.....	38
5 „Nové“ definování práva být zapomenut	39
6 Úvod do e-Governmentu	42
6.1 Stručný vývoj e-governmentu v České republice	45
7 Registry státní správy jako nástroj e-governmentu v České republice	48
7.1 Základní registry	49
7.2 Další registry státní správy	50
7.2.1 Insolvenční rejstřík	51
7.2.2 Trestní rejstřík	52
7.2.3 Evidence přestupků.....	56
7.2.4 Směrnice Evropského parlamentu a Rady EU 2016/680	57
8 Diskuze a doporučení	58
8.1 Komparativní analýza	58
8.2 Diskuze	61
8.3 Doporučení.....	65
Závěr.....	67

Seznam tabulek.....	69
Bibliografie.....	70

Úvod

Tato diplomová práce se zabývá právem být zapomenut, právem, jehož nárokování je v dnešní informační společnosti velmi aktuální. Ochrana osobních údajů je s rozvojem elektronizace společnosti velmi důležitá a od května roku 2018 by měla být výrazně posílena díky nabytí účinnosti nového nařízení Evropského parlamentu a Rady EU 2016/679, jež nahradí stávající právní úpravu. Tento legislativní dokument právo být zapomenut přímo vymezuje. Cílem práce je formulovat doporučení a zachytit dopady na veřejnou správu České republiky a některé její informační systémy, konkrétně registry veřejné správy.

První kapitola práce slouží jako uvedení do problematiky ochrany osobních údajů ve vztahu k soukromí a k právu na informace. Druhá kapitola je již věnována právnímu rámci ochrany osobních údajů a stávajícímu zákonu č. 101/2000 Sb., o ochraně osobních údajů, jemuž předchází krátký historický exkurz. Tato kapitola rozebírá strukturu zákona a některé stěžejní termíny. V následující třetí kapitole je představeno nové nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (angl. General Data Protection Regulation, GDPR). Součástí kapitoly je porovnání a sumarizace některých nových pojmů, včetně práva být zapomenut, které zmíněné nařízení přináší. Dále je nastíněn proces implementace nové legislativy, který se týká jak soukromoprávní, tak veřejnoprávní sféry. Čtvrtá kapitola navazuje vývojem institutu práva být zapomenut, které je zde rozvedeno formou rešerše několika dosavadních výzkumů v dané oblasti. Kapitola pátá představuje případ Google vs. AEPD, jež je považován za zlomový z hlediska ochrany osobních údajů a práva být zapomenut, a který podnítl odborné diskuze. Případ je zasazen do kontextu dosavadního unijního práva. Šestá kapitola je zaměřena na oblast e-governmentu v České republice, na jeho vývoj a nástroje. Finální sedmá kapitola je věnována nástinu základních registrů a dále potom konkrétním vybraným registrům veřejné správy s důrazem na jejich stávající právní úpravu ve vztahu k nadcházející nové legislativě.

Řešenou otázkou práce je předpokládaný dopad nového komunitárního nařízení a související směrnice na stávající právní úpravy některých registrů veřejné správy, a to konkrétně na insolvenční rejstřík, rejstřík trestů a evidenci přestupků, jež svou podstatou významně zasahují do oblasti osobních údajů a soukromí. Je provedena analýza

souvisejících zákonných úprav ve vztahu s ustanoveními Nařízení 2016/679, 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) a Směrnice 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

1 Ochrana osobních údajů všeobecně

S rozvojem moderní doby, dnešní společnosti a s pokrokem v oblasti informačních systémů nabývá institut ochrany osobních údajů na důležitosti. V dnešním životě se člověk setkává s ochranou osobních údajů téměř každý den při výkonu běžných činností, a to zřejmě aniž by si to plně uvědomoval. Svolení se zpracováním osobních údajů poskytujeme již takřka rutinně, jak osobně anebo přes internet. Ať už je to zájem o jejich ochranu nebo naopak nezájem, jedná se o celospolečensky diskutované a aktuální téma.

S rozšířením popularity a využívání sociálních sítí se výrazně zjednodušilo vyhledávání konkrétních osob a informací o nich, a lze tak hovořit o v podstatě „dobrovolných“ zásazích do soukromí, které si člověk před několika desítkami let nedokázal představit. Ve většině případů také dochází k absenci jakési prevence, absenci „brzd“ ve sdělování personálních informací, a tyto fakta mohou v konečném důsledku vést ke vzniku nepříjemných situací.

M. Matoušková a L. Hejlík nahlíží na ochranu osobních údajů ve třech rovinách. První reprezentují **základní lidská práva**. Druhou rovinou je **rovina právní**; jedná se o vzájemnou provázanost legislativních předpisů, proces jejich novelizací a v neposlední řadě také harmonii právního řádu České republiky s legislativou Evropské unie, která se také týká tématu předkládané práce. Třetí a poslední rovinou je **zabezpečení osobních údajů před únikem a zneužitím**; to je zajišťováno prostřednictvím odborných profesí a informačními technologiemi.¹

V následujících částech práce jsou tyto roviny rozvedeny podrobněji a zároveň je nastíněn historický vývoj ochrany osobních údajů.

1.1 Právo na soukromí v současném právním prostředí

Judikatura jak českých, tak zahraničních soudů zpravidla neobsahuje definici soukromí, a stejně tak ani jiné významné právní dokumenty a doktríny. Výjimečně lze reference nalézt v rozhodnutích Evropského soudu pro lidská práva, kde se tento široký pojem vztahuje zejména na fyzickou a psychickou integritu osoby (včetně sexuálního života).²

Před faktickou a legislativní stránkou je tedy vhodnější zařadit také filozofickou rovinu tématu. S nástupem internetu dochází ke snadnému, rychlému a efektivnějšímu šíření

¹ Kučerová, Alena, a další. 2003. Zákon o ochraně osobních údajů. Komentář. Praha : C. H. Beck, 2003. str. 406. ISBN 80-7179-762-6.

² Matejka, Ján. 2013. Internet jako objekt práva: hledání autonomie a soukromí. Praha : CZ.NIC, 2013. str. 262. ISBN 978-80-904248-7-6.

informací než kdy jindy. V 18. století se Rousseau zamýšlel nad neblahým morálním vlivem pokroku na lidskou civilizaci, dle jeho přesvědčení pokrok není zadarmo. Rozvoj technologií a internetu znamenal vznik mocných informačních nástrojů, ale ve vztahu například právě k soukromí, etice či autorským právům může znamenat hrozbu. Z důvodu jejich globální povahy zasáhly společenské a technologické změny do světových právních systémů natolik, že bylo nezbytné je přeformulovat.³

Právo na ochranu osobních údajů úzce souvisí se soukromím jednotlivců. Jak definovat pojem soukromí? Samuel Warren a Louis Brandeis ve svém článku *The Right to Privacy* zmiňují „*right to be let alone*“, volně přeloženo jako „právo být nechán“ nebo přesněji „právo být ponechán sám“⁴, a to v souvislosti s tehdy novými vynálezy, tiskem a obchodním rozvojem. V eseji je rovněž stanoveno, že „*běžné zákony zabezpečují každému jednotlivci právo si určit, v jakém rozsahu budou jeho myšlenky, postoje a emoce komunikovány (sdíleny) směrem k ostatním.*“⁵ Podle autorů je nezbytné činit kroky směrem k zajištění ochrany soukromí jednotlivců před zásahy ze strany novinářského průmyslu a v neposlední řadě také ze strany nových mechanických vynálezů.⁶ Velmi podobně definuje soukromí A. F. Westin ve své knize *Privacy and Freedom*: „*nárok jednotlivce, skupiny či instituce stanovit si kdy, jak a v jakém rozsahu budou informace o nich sdíleny s ostatními.*“⁷ Filozofický pohled Ch. Frieda v eseji *Privacy* uvádí soukromí do souvislosti s láskou, přátelstvím a důvěrou a zamýšlí se nad ním jako nad „*aspektem společenského řádu, pomocí kterého lidé kontrolují přístup (ostatních) k informacím o nich samých (...).* Je o pocitu záruky kontroly nad těmito informacemi.“⁸

Většina autorů tedy vymezila soukromí jako nárok každého na kontrolu, jaké informace (osobní údaje) a v jakém rozsahu jsou tyto informace zveřejňovány.

1.2 Právo na soukromí vs. právo na informace

Současná společnost je definována jako informační společnost, na jejíž platformě dochází ke střetům mezi právy a obecnými principy (např. morálka) stále častěji. J. Matejka tuto

³ Matejka, 2013

⁴ Matoušová, Miroslava a Hejlík, Ladislav. 2008. *Osobní údaje a jejich ochrana*. Praha : ASPI, Wolters Kluwer, 2008. str. 468. ISBN 978-80-7357-322-5.

⁵ Warren, Samuel a Brandeis, Louis. 1890. *The Right to Privacy*. [Online] 15. Prosinec 1890. [Citace: 13. 5. 2017]. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

⁶ Warren, a další, 1890

⁷ Westin, Alan F. 1968. *Privacy And Freedom*. Washington & Lee University School of Law. [Online] 1968. [Citace: 13. 5. 2017]. <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.

⁸ Fried, Charles. 1968. *Privacy*. [Online] 1968. [Citace: 8. 5. 2017]. <http://www.jstor.org/stable/794941>.

společnost popisuje jako společnost, která „*kteřá si postupně uvědomuje důležitost informací a která ke zvýšení své informovanosti využívá možností daných moderními informačními a komunikačními technologiemi.*“⁹

Dvě strany mince existujícího rozvoje informačních technologií: na jedné straně tento vývoj znamenal zvýšení tempa práce, rychlé obchodování nebo komunikaci na dálku s více než jedním subjektem. Na straně druhé se díky tomuto technickému prvku otevřely možnosti intenzivního monitoringu soukromí fyzických osob, vnikání do něj a v konečném důsledku jeho narušování.¹⁰ K těmto pokusům o monitorování vztahů a sběru informací může docházet ze strany státu, a tento fakt dává vzniku právním a etickým konfliktům a otázkám, jak k nim přistupovat.

Článek 17 Listiny základních práv a svobod zakotvuje právo na informace a svobodu projevu mezi politická práva:

„(1) Svoboda projevu a právo na informace jsou zaručeny.

(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.

(3) Cenzura je nepřipustná.

(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.

(5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.“¹¹

Právo na svobodu projevu a právo na informace jsou nepřímou součástí ochrany osobních údajů, protože součástí některých informací jsou často právě osobní údaje jednotlivců. Ve smyslu zákona o ochraně osobních údajů dochází jejich šířením (předáváním jiným subjektům) ke zpracování osobních údajů, na které se zmíněný zákon č. 101/2000 Sb.

⁹ Matejka, 2013, str. 38

¹⁰ Kučerová, a další, 2003

¹¹ Česká republika. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.

plně vztahuje.¹² Je nutné si uvědomit, že výše zmíněná práva nejsou právy absolutními, a mnohdy je třeba aplikovat je současně.

2 Právní zakotvení ochrany osobních údajů

2.1 Historie ochrany osobních údajů

Na úvod je proveden krátký historický exkurz k vývoji práva na ochranu osobních údajů. Za prvopočátek a pozdější vzor pro tvorbu právních předpisů týkajících se základních práv člověka lze považovat **Deklaraci práv člověka a občana**, která vznikla ve Francii roku 1789. Podle bodu IV. každý může činit vše, co neškodí druhému, a dále, že „výkon přirozených práv každého člověka nemá jiných mezí než ty, které zajišťují ostatním členům společnosti užívání týchž práv. Tyto meze mohou být ustanoveny pouze zákonem.“¹³ Je vhodné zmínit také bod XI., který zaručuje lidem svobodu projevu, avšak za každé zneužití této svobody se musí v případech stanovených zákonem zodpovídat.

Lidstvo po 2. světové válce, a zejména oblast střední Evropy, bylo poznamenáno praktikami, které byly spojeny s protiprávním zneužíváním dříve nashromážděných údajů ze strany nacistického režimu. Lidské myšlení se obrací k úvahám na ochranu soukromého života a postavení jedince ve společnosti.¹⁴ Právě tehdy přišel další milník: **Všeobecná deklarace lidských práv**. Ta byla schválena Valným shromážděním Organizace spojených národů roku 1948. Podle článku 12 této Deklarace nesmí být nikdo „vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“¹⁵ Z tohoto právně nezávazného dokumentu vychází o 18 let později **Mezinárodní pakt o občanských a politických právech**, který již právní závaznost má, a zcela přejímá výše citované stanovení do článku 17.¹⁶ Stanovená úroveň ochrany lidských práv je později rozvíjena i v mnoha dalších právních aktech.¹⁷

Roku 1981 vznikl v podstatě první komplexní dokument týkající se zpracování a ochrany osobních údajů – **Úmluva o ochraně osob se zřetelem na automatizované zpracování**

¹² Kučerová, a další, 2003, str. 32-33

¹³ Skoupý, Arnošt. 1989. *Texty k obecným dějinám kapitalismu I*. Katedra historie Filozofické fakulty Univerzity Palackého. [Online] 1989. [Citace: 8. 5. 2017]. <http://www.historie.upol.cz/19/prameny/prava.htm>. Bod IV.

¹⁴ Kučerová, a další, 2003

¹⁵ United Nations Information Centre. 1948. *Všeobecná deklarace lidských práv*. United Nations Human Rights. [Online] 1948. [Citace: 9. 5. 2017]. <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=czc.12>.

¹⁶ OSN. 1966. *Mezinárodní pakt o občanských a politických právech. Lidská práva*. [Online] 1966. [Citace: 9. 5. 2017]. http://www.lidskaprava.cz/uploads/03_dokumenty/04_uvod/01_ICCPR.pdf.

¹⁷ Kučerová, a další, 2003

osobních dat (č. 108) a její Dodatkový protokol. Mimo jiné obsahoval zpracované primární zásady ochrany osobních údajů a představoval určité záruky.

Za konkrétním účelem ochrany osobních údajů je roku 1995 vydána **Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů**. Jejím cílem byla jednotná úprava ochrany dat a jejich pohybu na území Evropského společenství. Tato směrnice upravuje zásady zpracování osobních údajů, práva a povinnosti při jejich zpracování, jejich předávání do třetích zemí, soudní přezkum, odpovědnost a sankce, a i určité výjimky z ochrany osobních údajů. Dále zakládá povinnost dohledu nad dodržováním přijatých předpisů.¹⁸

O rok později, tedy v roce 1996, podala Vláda České republiky žádost o vstup do Evropské unie. V důsledku harmonizace právních norem České republiky s těmi unijními vešel roku 2000 v platnost (mimo jiné) zákon č. 101/2000 Sb., o ochraně osobních údajů. Roku 2016 bylo schváleno Nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které nabude účinnosti v květnu 2018 a které ruší Směrnici a bude mít nesporný vliv na českou legislativu.

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

Jak bylo řečeno již dříve, také v České republice se ochrana osobních údajů řadí mezi základní lidská práva a je chráněna Ústavou České republiky a Listinou základních práv a svobod:

„(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“¹⁹

Po ústavněprávní úpravě vznikl v roce 1992 zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech; poprvé se tak vlastně na území České republiky (tehdy

¹⁸ Evropská unie. 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.

¹⁹ Listina základních práv a svobod, čl. 10.

ještě Československa) objevuje institut ochrany osobních dat. Jeho prostřednictvím byly definovány základní pojmy a vymezeny hlavní zásady nakládání s osobními údaji. Později, kdy se již samostatná Česká republika ucházela o členství v Evropské unii, nastala potřeba zajistit kompatibilitu s jejími právními předpisy. Pro připomenutí: výchozím dokumentem pro nově vznikající zákon byla v případě práva na ochranu osobních údajů Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice“).

Aktuálně platným právním předpisem regulujícím analyzovanou oblast je zákon č. 101/2000 Sb., o ochraně osobních údajů (dále jen „zákon o ochraně osobních údajů“). Tato úprava se již řadila k právním normám, které směřovaly k harmonizaci práva České republiky a práva Evropské unie²⁰ a rušila předcházející zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

Legislativní rámec Evropské unie, ze kterého vycházela právní úprava ochrany osobních údajů, byl vymezen následujícími dokumenty²¹, z nichž některé byly již dříve v práci zmíněny:

- Úmluva o ochraně lidských práv a základních svobod,
- Úmluva o ochraně osob s ohledem na automatizované zpracování osobních dat (Úmluva č. 108),
- Směrnice Evropského parlamentu a Rady 95/46/ES (o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů) a 2002/58/ES (o ochraně soukromí a elektronických komunikací).

Cílem zákona o ochraně osobních údajů je chránit občana před neoprávněným zasahováním do jeho soukromého života a zabránit zneužívání osobních údajů.

Zákon o ochraně osobních údajů je strukturován do tří, resp. dvou částí (Část II byla zrušena) a obsahuje 51 paragrafů. Upravuje oblast ochrany osobních údajů fyzických osob (subjektů údajů), definuje práva a povinnosti správce a zpracovatele a je předmětem úpravy otázek spojených s předáváním osobních údajů do jiných států. V následujících

²⁰ Šmíd, Vladimír. *Srovnání právních úprav vztahujících se k ochraně osobních údajů v ČR a SR*. Fakulta informatiky Masarykovy univerzity. [Online] [Citace: 10. 5. 2017]. <https://www.fi.muni.cz/~smid/ochdcrsr1.html>.

²¹ Neuwirth, Karel. 2003. *Ochrana osobních údajů a vstup do EU*. Úřad pro ochranu osobních údajů. [Online] 2003. [Citace: 10. 5. 2017.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8087.

odstavcích je zmíněný zákon představen a jsou vymezeny a definovány klíčové pojmy spojené s problematikou tématu.

2.2.1 Úřad pro ochranu osobních údajů

Zákon o ochraně osobních údajů zakládá vznik Úřadu pro ochranu osobních údajů (dále jen „Úřad“), který působí jako dozorový orgán. Představuje ústřední správní úřad pro „*oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem, zvláštními právními předpisy, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie.*“²² Jedná se o nezávislý orgán, který:²³

- provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů,
- vede registr povolených zpracování osobních údajů,
- přijímá podněty a stížnosti občanů na porušení zákona,
- poskytuje konzultace v oblasti ochrany osobních údajů.

Při zřizování Úřadu a určování jeho postavení a kompetencí bylo využito zkušeností obdobných institucí, které fungují v jiných členských státech Evropské unie.²⁴

2.2.2 Působnost

Působnost zákona o ochraně osobních údajů upravuje § 3. Zákon o ochraně osobních údajů se vztahuje na takové osobní údaje, které jsou zpracovávány státními orgány, orgány územní samosprávy nebo jinými orgány veřejné moci, stejně jako fyzickými či právnickými osobami. Pokrývá veškeré způsoby jejich zpracování (automatizované, manuální anebo zpracování pomocí jiných prostředků). Dále zákon upravuje jeho použití ve výjimečných případech.

Je faktem, že fyzické osoby ve skutečnosti shromažďují osobní údaje na denní bázi; telefonní čísla, adresy nebo mailové adresy přátel... Na osobní údaje, které fyzická osoba shromažďuje výlučně pro svou potřebu (pozor, ne pro např. soukromé podnikání a jinou komerční potřebu), se zákon o ochraně osobních údajů nevztahuje. Stejně tak v případech nahodilého shromažďování, pokud takové údaje nejsou dále (systematicky) zpracovávány.

²² Česká republika. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. § 2.

²³ Úřad pro ochranu osobních údajů. 2013. *Úřad*. Úřad pro ochranu osobních údajů. [Online] 2013. [Citace: 12. 5 2017.] <https://www.uoou.cz/urad/ds-1059/p1=1059>.

²⁴ Kučerová, a další, 2003

2.2.3 Základní pojmy

Ustanovení § 4 jsou věnována základním termínům, a protože porozumění těmto pojmům je pro účely této práce nezbytné, věnuje se tato kapitola právě jim.

Osobní údaje. Podle zákona o ochraně osobních údajů se jimi rozumí „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů*“.²⁵ Směrnice definuje osobní údaje velmi podobně, a to jako „*veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity*“.²⁶ M. Matoušová a L. Hejlík upozorňují na jistá úskalí přesného definování a porozumění tomuto termínu z právního hlediska. Zákonná definice se omezuje na vymezení vztahu údajů k **subjektu údajů** (tedy k tomu, o kom dané údaje vypovídají).²⁷ Osobní údaj je každý údaj, který je uveden do vztahu k fyzické osobě, která se tak stává subjektem údajů; nelze vnímat pouze hodnoty vyjadřující charakteristiku subjektu údajů a opomíjet vazby na reálné fyzické osoby.²⁸

Určeností a určitelností se rozumí vztah mezi subjektem – fyzickou osobou a informací; subjekt lze přímo či nepřímo identifikovat na základě specifických údajů (kód, číslo, aj.). Zákon o ochraně osobních údajů mezi určeností a určitelností nerozlišuje – pro oboje stanoví podmínky zjištění totožnosti subjektu údajů na základě jednoho nebo několika osobních údajů.²⁹

Aby tedy bylo možné jednoznačně určit nějaký údaj jako osobní údaj, je třeba na jejich základě nejprve bez vynaložení nepřiměřeného úsilí identifikovat fyzickou osobu.³⁰ Je důležité si uvědomit, že například jméno a příjmení samotné ještě nemusí být nutně osobními údaji, avšak při vymezení určité skupiny se jimi mohou stát.

Zákon o ochraně osobních údajů dále rozlišuje osobní údaje **citlivé (senzitivní)** – ty je velmi jednoduché určit, neboť jsou taxativně vymezeny (národnostní, etnický či rasový původ, politický postoj, členství v odborových organizacích, náboženské či filozofické přesvědčení, trestná činnost, zdravotní stav, sexuální život subjektu údajů).

²⁵ Zákon č. 101/2000 Sb., § 4.

²⁶ Směrnice 95/46/ES, Kapitola I, čl. 2, odst. a).

²⁷ Matoušová, Miroslava a Hejlík, Ladislav. 2003. *Osobní údaje a jejich ochrana. Knižka pro praxi*. Praha : ASPI, 2003. str. 416. ISBN 80-86395-50-2.

²⁸ Matoušová, a další, 2003

²⁹ Matoušová, a další, 2003

³⁰ Kučerová, a další, 2003

Dalším typem údajů, které související zákon vymezuje, jsou **anonymní**, které v původním tvaru nebo po provedení jejich zpracování nelze vztáhnout k určenému nebo určitému subjektu údajů).³¹ Anonymizování údajů je proces, jímž je dosaženo přerušení vazby mezi hodnotou údaje a jeho subjektem, čímž se vytvoří výše zmíněný anonymní údaj.³² Tyto údaje je možné zpracovávat i bez souhlasu subjektu údajů, a to pro vědecké nebo statistické účely.³³

Co se týká výše zmíněného termínu, jde o významově široké spojení, jež lze vztáhnout prakticky s každou informací o fyzické osobě, která vypovídá něco o jejím soukromí. S každým údajem je možné nakládat a posuzovat jej jinak v závislosti na kontextu a situaci a na tom, kde a u koho se informace nacházejí.

Zpracování osobních údajů. Pod tímto termínem se dle zákona o ochraně osobních údajů rozumí „*jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky*“.³⁴ Definice, kterou uvádí Směrnice, je významově shodná, a sice: „*jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů*“.³⁵ Mezi takové úkony nebo operace se dle české zákonné úpravy řadí „*shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace*“³⁶, dle Směrnice pak „*shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace*“³⁷

Dle zákonné definice zpracováním osobních údajů nemusí rozumět celý soubor operací, mnohdy se může jednat jen o několik nebo i pouze jednu činnost. Pro téma práce je z výše zmíněných činností klíčová zejména **likvidace** osobních údajů, která představuje jejich nenávratné zničení. Protože se tato akce zpravidla nepojí se zlikvidováním samotného

³¹ Zákon č. 101/2000 Sb., § 4

³² Matoušová, a další, 2003

³³ Kučerová, a další, 2003

³⁴ Zákon č. 101/2000 Sb., § 4

³⁵ Směrnice 95/46/ES, Kapitola I, čl. 2, odst. b).

³⁶ Zákon č. 101/2000 Sb., § 4.

³⁷ Směrnice 95/46/ES, Kapitola I, čl. 2, odst. b).

nosiče dat, lze tento termín shledat poněkud zavádějícím. Je možné tedy spíše hovořit o **výmazu** osobních údajů způsobem neumožňujícím jejich obnovu.³⁸

Při nakládání s osobními údaji jsou rozlišeny role **správce** a **zpracovatele**. **Správce** může být „každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj“³⁹. Správce je oprávněn zmocnit nebo pověřit zpracováním osobních údajů **zpracovatele**, pokud není zvláštním zákonem stanoveno jinak. Dříve zmíněné určení účelu je hlavním rozlišujícím znakem mezi správcem a zpracovatelem.⁴⁰

Znalost a určení účelu zpracování osobních dat je v roli správce ve vztahu k zákonu o ochraně osobních údajů stěžejní. V případě státní správy, samosprávy nebo v případě pověřených subjektů s přenesenou státní pravomocí tento účel již vyplývá ze zvláštního zákona, na jehož základě bude ke zpracování docházet.⁴¹

2.2.4 Práva a povinnosti při zpracování osobních údajů

Oblast práv a povinností, které jsou spojeny se zpracováním osobních údajů, je ošetřena v Hlavě II zákona o ochraně osobních údajů o ochraně osobních údajů.

Správce je podle Zákona o ochraně osobních údajů povinen stanovit **účel** jejich zpracování, **prostředky** a **způsob** jejich zpracování a zpracovat pouze **přesné údaje** získané v souladu se zákonem. Informace je povinen shromažďovat pouze k účelu, jež byl stanoven, a v rozsahu nezbytně nutném k naplnění účelu. Totéž se týká doby uchovávání těchto informací. Údaje, které byly získány za jiným účelem, správce **nesmí sdružovat**.⁴²

Až na výjimky stanovené zákonem, ke zpracování osobních údajů dochází pouze na základě **souhlasu subjektu údajů**. Subjekt údajů musí být při udělení souhlasu informován o účelu zpracování, jakému správci je souhlas udělován, dále o tom, na jaké osobní údaje se souhlas vztahuje a na jaké období.⁴³

Dle § 12 má subjekt údajů právo požádat správce o informaci o zpracování jeho osobních údajů. Správce je povinen takovou informaci bez zbytečných odkladů sdělit.

³⁸ Kučerová, a další, 2003

³⁹ Zákon č. 101/2000 Sb., §4 písm. j).

⁴⁰ Kučerová, a další, 2003

⁴¹ Kučerová, a další, 2003

⁴² Zákon č. 101/2000 Sb.

⁴³ Zákon č. 101/2000 Sb.

Téma diplomové práce je úzce spjato se zabezpečením osobních údajů. Důležitou rolí správce a zpracovatele je, aby takové **zabezpečení** zajistili. Je jejich povinností přijmout taková opatření, aby bylo zabráněno neoprávněným přístupům zvenčí, úniku sebraných osobních údajů, jejich ztrátě nebo jinému zneužití. Ze strany správců a zpracovatelů musí být zaručena komplexní ochrana a zabezpečení a kontrola nad přístupy k datům ze stran oprávněných osob.⁴⁴

Zákon o ochraně osobních údajů zmiňuje oznamovací povinnost, kterou má správce vůči Úřadu. Učinit tak musí před započítím zpracování informací, pokud se na ně oznamovací povinnost vztahuje.⁴⁵

V §20 je zmíněna **likvidace** osobních údajů. K té dochází, pomine-li účel, za kterým byly údaje shromážděny. Likvidace dle zákona znamená fyzické zničení nosiče údajů, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování. Výjimky stanoví zvláštní zákon (může se jednat např. o zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, 40/2009, trestní zákoník aj.).

Hlava VII upravuje správní delikty, jichž se může dopustit fyzická osoba v postavení správce či zpracovatele anebo v poměru k nim. Přestupků se mohou dopustit i fyzické osoby podnikající nebo právnické osoby. Zákon stanovuje několikeré peněžité sankce v nezanedbatelné výši (v určitých případech až do 10 mil. Kč).

3 Nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)

V době, kdy začala platit současná směrnice o ochraně osobních údajů, neexistovaly cloudová úložiště nebo sociální sítě tak, jak je známe dnes. Stávající unijní legislativa se již dá díky rychlému rozvoji informační společnosti považovat za zastaralou, a proto bylo nutné podniknout kroky vpřed. Dalším důvodem byly i rozdíly mezi tím, jak je vnímána osobní svoboda v Evropské unii jak v jiných státech. Stanovení jasných pravidel ochrany tedy bylo nutné.

V květnu roku 2016 bylo v Úředním věstníku Evropské unie publikováno nové nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice

⁴⁴ Zákon č. 101/2000 Sb., § 13.

⁴⁵ Zákon č. 101/2000 Sb., § 16.

95/46/ES (angl. General Data Protection Regulation, GDPR). Toto nařízení vstoupilo v platnost 24. května 2016 a účinnosti nabude o dva roky později, konkrétně 25. května 2018. Návrh nařízení vycházel z platných unijních právních předpisů, a to z již zmíněné směrnice 95/46/EU a z Rámcového rozhodnutí rady EU 2008/977/SVV (o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech).

O důležitosti ochrany osobních údajů v souvislosti s jednotným digitálním trhem (a např. i o posílení důvěry v internet) hovoří také Digitální agenda pro Evropu (MEMO/10/200, klíčové opatření č. 4⁴⁶) a strategie Evropa 2020.⁴⁷

Předpokládá se, že změny, které vyplývají z této nové evropské normy, se dotknou řízení organizací na všech úrovních, a to v podobě nutných úprav některých jejich procesů nebo smluvních dokumentů (pracovněprávní nebo dodavatelské smlouvy aj.), aktualizací interních směrnic a veškeré dokumentace navázané na zpracování osobních údajů.⁴⁸ Nařízení se týká také online služeb; „zásadním způsobem se dotkne i informačních technologií, u kterých budou společnosti a státní instituce povinny projít revizí datové architektury, aktualizací a případným upgradem systémů a bezpečnostních opatření ve všech vrstvách ICT infrastruktury.“⁴⁹

Z právního pohledu je nařízení, které je přímo účinné ve všech členských státech, a národní legislativní předpisy bude potřeba s tímto novým komunitárním nařízením uvést do souladu. V případě České republiky bude mít toto nařízení dopad primárně na zákon č. 101/2000 Sb., o ochraně osobních údajů, buďto v podobě jeho novelizace anebo zrušení a schválení zákona nového. Stejně tak jako v případě zákona o ochraně osobních údajů, jedním z cílů nařízení je zajištění vysoké úrovně ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů.

Mimo soukromoprávní sféru se nové nařízení dotkne také veřejné správy, která zažívá proces elektronizace. Pro veřejný sektor znamená nástup nového nařízení nutnost revize klíčových právních předpisů a zároveň harmonizace stávajících dokumentů, procesů a informačních systémů s novou legislativou. Zásadní bude také zajištění bezpečnostních

⁴⁶ Evropská komise. 2010. *Digitální agenda pro Evropu: klíčové iniciativy*. European Commission. [Online] 19. květen 2010. [Citace: 13. 5. 2017]. http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm.

⁴⁷ Evropská komise. 2010. *Evropa 2020: Strategie pro inteligentní a udržitelný růst podporující začlenění*. EUR-Lex. [Online] 3. březen 2010. [Citace: 13. 5. 2017]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:CS:PDF>.

⁴⁸ Škorníčková, Eva. 2017. *GDPR cirkus přijíždí. Začínáme!* GDPR.cz. [Online] 27. duben 2017. [Citace: 15. 5. 2017]. <https://www.gdpr.cz/blog/gdpr-cirkus/>.

⁴⁹ Škorníčková, 2017

a organizačních opatření. Bude se tedy jednat o všechny její registry a informační systémy, které obsahují osobní údaje.

Je vhodné zmínit, že nařízení se netýká evidencí vedených fyzickými osobami pro jejich výlučné potřeby (podobně i stávající zákon o ochraně osobních údajů) a přímo se nevztahuje ani na zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.⁵⁰

Samotné nařízení lze shledat velmi rozsáhlým. Preambule čítá 173 bodů, dále je dokument rozdělen do 11 kapitol⁵¹:

- I. Obecná ustanovení (čl. 1-4)
- II. Zásady (čl. 5-11)
- III. Práva subjektu údajů (čl. 12-23)
- IV. Správce a zpracovatel (čl. 24-43)
- V. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (čl. 44-50)
- VI. Nezávislé dozorové úřady (čl. 51-59)
- VII. Spolupráce a jednotnost (čl. 60-76)
- VIII. Právní ochrana, odpovědnost a sankce (čl. 77-84)
- IX. Ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování (čl. 85-91)
- X. Akty v přenesené pravomoci a prováděcí akty (čl. 92, 93)
- XI. Závěrečná ustanovení (čl. 94-99)

V následujících odstavcích jsou tyto kapitoly podrobněji rozebrány a některým aspektům se práce ještě později blíže věnuje.

Kapitola I. Obsahem první kapitoly je **určení základního předmětu a cíle** nařízení, věcnou a místní působnost a definice základních termínů pro účely daného nařízení.

Kapitola II. Ve druhé kapitole jsou definovány **zásady** zpracování osobních údajů.⁵²

⁵⁰ Lechner, Tomáš. 2017. *Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)*. [Online] 2017. [Citace: 18. 5. 2017]. <https://www.iiss.cz/archiv/2017/download/iiss2017.pdf>.

⁵¹ Evropská unie. Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵² Nařízení Evropského parlamentu a Rady EU 2016/679, kapitola II, čl. 5.

- **Zákonnost, korektnost, transparentnost** – podmínky zákonnosti jsou stanoveny dále v čl. 6 nařízení, patří mezi ně zejména udělení souhlasu ze strany subjektu údajů, dále nezbytnosti zpracování pro splnění právních povinností, nezbytnost zpracování pro ochranu životně důležitých zájmů subjektů údajů či jiné fyzické osoby aj.
- **Účelové omezení** – osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem s těmito účely neslučitelným.
- **Minimalizace údajů** – jedná se o přiměřenost, relevantnost a omezení sběru osobních údajů na rozsah nezbytný ke stanovenému účelu zpracování.
- **Přesnost** – osobní údaje, které jsou zpracovávány, musí být přesné a případně také podléhají povinné aktualizaci. Tato zásada stanovuje povinnost přijetí opatření, aby nepřesné údaje byly vymazány nebo opraveny.
- **Omezení uložení** – uložení údajů ve formě umožňující identifikaci subjektu údajů nesmí být delší než doba nezbytná pro naplnění účelu jejich zpracování.
- **Integrita a důvěrnost** – osobní údaje musí být zpracovávány způsobem, který zajistí jejich zabezpečení na náležité úrovni, včetně ochrany s využitím vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.
- **Odpovědnost** – za dodržování zásad odpovídá správce. Správce musí být také schopen doložit dodržení souladu zpracování osobních údajů s výše uvedenými zásadami. Pokud se jedná o odpovědnost zpracovatele, ta je pak blíže upravena v článku 82 nařízení.

Lze tvrdit, že uvedené zásady poskytují velmi komplexní rámec, jak nakládat s osobními údaji. Správce, jako primární nositel zodpovědnosti, se musí pružně adaptovat na rychle se rozvíjející oblast informačních technologií a s tím i rostoucí rizika zneužití a neoprávněného zásahu do shromážděných osobních dat.

Kapitola III. Další kapitola je obecně věnována **právům subjektu údajů** a dělí se na pět oddílů. První oddíl upřesňuje právo subjektu údajů na stručné, transparentní, srozumitelné a snadno přístupné informace (ze strany správce), které se týkají postupů pro výkon práv subjektu údajů. Druhý oddíl specifikuje právo subjektu údajů na přístup k informacím o zpracovávaných osobních údajích. Rozlišuje dvě situace jejichž základě jsou informace poskytovány rozdílně: případy, kdy jsou osobní data získána od subjektu údajů a případy,

kdy tato data nejsou získána od subjektu údajů. Ve třetím oddíle lze nalézt právo na opravu, kdy správce bez zbytečného odkladu opraví nepřesné osobní údaje dotčeného subjektu údajů. Následující článek zmiňuje důležité právo na výmaz, současně uvedené v nové formě jako „**právo být zapomenut**“; subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, pokud je taková žádost v souladu alespoň s jedním z důvodů, které uvádí nařízení.⁵³ Blíže se tomuto institutu věnuje další podkapitola. Dalšími právy jsou právo na omezení zpracování a právo na přenositelnost údajů. Ve čtvrté oddíle kapitoly lze nalézt právo na vznesení námítky a právo subjektu údajů nebýt předmětem žádného rozhodnutí, jež bylo založeno výhradně na automatizovaném zpracování, včetně profilování. Posledním oddílem je stanoveno právo na legislativní omezení rozsahu povinností a práv uvedených ve třetí kapitole a v článku 5 a 34, jestliže omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření s cílem zajistit národní bezpečnost, obranu, veřejnou bezpečnost, ochranu nezávislosti soudnictví a soudního řízení aj.⁵⁴

Kapitola IV. Kapitola čtvrtá je také rozdělena do pěti oddílů a obsahuje ustanovení o **povinnostech správců a zpracovatelů**. První oddíl je věnován obecným povinnostem. Zabezpečení osobních dat při zpracovávání, ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a subjektu údajů je věnován oddíl druhý. Třetí oddíl se týká posouzení vlivu na ochranu osobních údajů a předchozích konzultací. Pokud existuje pravděpodobnost, že určitý druh zpracování osobních dat za pomoci využití nových technologií bude mít za následek vysoké riziko pro práva a svobody fyzických osob, správce provede před zpracováním posouzení vlivů zamýšlených operací zpracování. Obsah článku 35 daného oddílu stanoví případy, kdy je posouzení vlivu zejména nutné. Čtvrtý oddíl přináší do českého právního prostředí novinku – je v něm specifikována role **pověřence pro ochranu osobních údajů**, jeho jmenování, postavení a úkoly. Poslední pátý oddíl se věnuje kodexům chování a vydávání osvědčení. Vydávané kodexy mají přispívat k řádnému uplatňování nařízení s ohledem na povahu různých odvětví, které provádějí zpracování osobních údajů. Kodexy by dále měly sloužit pro určité potřeby mikropodniků a malých a středních podniků. Dále jsou oddíl popisuje zavedení mechanismů pro vydávání osvědčení o ochraně dat a zavedení pečeti a známek

⁵³ Specifikace důvodů je vymezena v článku 17 Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵⁴ Lechner, 2017, Nařízení Evropského parlamentu a Rady EU 2016/679.

prokazujících soulad s nařízením v případě operací zpracování, které jsou prováděny správci a zpracovateli. Osvědčení vydávají pouze akreditované subjekty.⁵⁵

Kapitola V. Další kapitola nařízení se týká **předávání osobních údajů do třetích zemí** nebo mezinárodním organizacím. Stanovuje obecné zásady a postupy a cílem jejich použití je zajistit, aby úroveň ochrany fyzických osob, která se tímto nařízením zaručuje, nebyla znehodnocena.⁵⁶

Kapitola VI. Obsahem šesté kapitoly je institut nezávislých dozorových úřadů, jež jsou pověřeny monitoringem uplatňování nařízení, a to s již několikrát zmiňovaným cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováváním jejich osobních dat a s cílem usnadnit volný pohyb těchto dat v rámci Evropské unie. První oddíl specifikuje nezávislost postavení dozorových úřadů, pravidla pro jejich zřízení, obecné podmínky pro členy dozorových úřadů. Druhý oddíl je věnován příslušnosti těchto úřadů, jejich úkolům a pravomocem.⁵⁷

Kapitola VII. Sedmá kapitola na předchozí navazuje a popisuje oblast **vzájemné spolupráce a pomoci mezi dozorovými úřady**. Druhý oddíl definuje mechanismus jednotnosti, jehož cílem je přispět k jednotnému uplatňování tohoto nařízení v celé Evropské unii, a to právě pomocí spolupráce mezi všemi stranami. Oddíl třetí se týká Evropského sboru pro ochranu osobních údajů. Jedná se o nezávislý orgán, který je tvořen vedoucími jednoho dozorového úřadu každé členské země a evropským inspektorem ochrany osobních údajů a jehož cílem je zajišťování jednotného uplatňování nařízení.⁵⁸

Kapitola VIII. **Právní ochrana, odpovědnost a sankce** jsou specifikovány v osmé kapitole nařízení. Je zde stanoveno právo podat stížnost u dozorového úřadu, právo na účinnou soudní ochranu vůči dozorovému úřadu, právo na účinnou soudní ochranu vůči správci nebo zpracovateli, právo na náhradu újmy a odpovědnost, Článek 83 dále stanovuje obecné podmínky pro ukládání správních pokut. Dle toho, která ustanovení jsou porušena, může výše takových pokut dosáhnout až 10 mil. EUR resp. 20 mil. EUR, a v případě, že se jedná o podnik, se jedná až o 2 %, resp. 4 % celkového ročního obrátu. Každý členský stát může stanovit pravidla po ukládání pokut veřejné moci a veřejným subjektům.⁵⁹ „Protože konkrétní výše pokuty vždy závisí na posouzení příslušným

⁵⁵ Lechner, 2017, Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵⁶ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵⁷ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵⁸ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁵⁹ Nařízení Evropského parlamentu a Rady EU 2016/679.

dozorovým úřadem, je zřejmé, že jejich rozhodovací pravomoc je tímto, zejména pro případ České republiky a dalších méně ekonomicky silných států EU, značně posílena.“⁶⁰

Kapitola IX. Devátá kapitola obsahuje **ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování.** V článku 85 je zde zmíněn střet se svobodou projevu a informací – členské státy prostřednictvím legislativních předpisů uvedou právo na ochranu osobních údajů dle nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a účely akademického, uměleckého nebo literárního projevu. Dále kapitola rozeznává další určité případy související s úředními dokumenty, národními identifikačními čísly, zpracování v souvislosti se zaměstnáním, zpracování pro účely archivace, vědecké historické výzkumy nebo statistické účely, dále i pravidla pro ochranu údajů uplatňovaná církvemi a náboženskými sdruženími. Jedním z prvků této kapitoly je i definice povinnosti mlčenlivosti.⁶¹

Předposlední **kapitola X** shrnuje **akty v přenesené pravomoci a prováděcí předpisy** a poslední **kapitola XI** obsahuje **závěrečná ustanovení** nařízení včetně určení jeho použitelnosti od 25. května 2018, jak bylo již zmíněno několikrát.⁶²

3.1 Porovnání stávajících a nových definic

Tato podkapitola je věnována novým termínům a také některým obecným pojmům, s nimiž se lze v nařízení setkat, a které jsou porovnány se stávající právní úpravou v České republice. Definice základních pojmů lze nalézt v již zmíněném článku 4 nařízení.

Osobní údaje. Nařízení jimi rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (kterou dále nazývá subjektem údajů). Takovou fyzickou osobou se rozumí fyzická osoba, kterou lze přímo nebo nepřímo identifikovat, zejména odkazem na určitý identifikátor – tím může být např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků její identity (fyzické, fyziologické, genetické, psychické, ekonomické, kulturní, společenské aj.).⁶³ Definici nařízení lze považovat za shodnou s definicí v zákoně o ochraně osobních údajů; jedná se o informace, za pomoci kterých lze přímo či nepřímo určit (identifikovat) fyzickou osobu.⁶⁴ Definice **zpracování osobních údajů, subjektu údajů, správce a zpracovatele**

⁶⁰ Lechner, 2017, str. 3.

⁶¹ Lechner, 2017, Nařízení Evropského parlamentu a Rady EU 2016/679.

⁶² Lechner, 2017, Nařízení Evropského parlamentu a Rady EU 2016/679.

⁶³ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁶⁴ Nařízení Evropského parlamentu a Rady EU 2016/679.

jsou rovněž významově i obsahově totožná v porovnání se současnou českou právní úpravou.⁶⁵

Zvláštní kategorie osobních údajů jsou uvedeny v devátém článku nařízení, a jedná se o takové údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, dále pak do zmíněné kategorie spadají genetické a biometrické údaje, údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci fyzické osoby. Až na výjimečné případy, které jsou následně uvedeny v tom samém článku, je zpracování těchto zvláštních kategorií osobních údajů zakázáno.⁶⁶ Zákon o ochraně osobních údajů hovoří o těchto datech jako o citlivých, rovněž uvádí podmínky, za kterých je možné takové údaje zpracovávat.⁶⁷

Profilování je jeden z nových pojmů, které nařízení přináší. Jde o jakoukoliv formu automatizovaného zpracování osobních údajů, které dále slouží k hodnocení některých osobních aspektů vztahujících se k fyzické osobě. Jedná se zejména o rozbor či odhad aspektů týkající se pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se fyzická osoba nachází anebo pohybuje.⁶⁸ Ačkoliv se z hlediska nařízení jedná o nově definovaný termín, o žádnou novinku se nejedná a běžně k němu v současné době dochází např. v oblasti marketingu a finančních služeb.

Pseudonymizace je také novinka. Pseudonymizace se mimo jiné řadí pod opatření podporující zabezpečení zpracování osobních dat.⁶⁹ Jedná se o způsob zpracování osobních údajů tak, aby nebylo možné jejich přiřazení konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně bezpečnostní opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované nebo identifikovatelné osobě.⁷⁰

Správce a zpracovatel. **Správce** je fyzická či právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. **Zpracovatelem** se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který provádí zpracování údajů pro

⁶⁵ Paták, Tomáš. 2017. *Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích*. Úřad pro ochranu osobních údajů. [Online] 2017. [Citace: 27. 5. 2017]. https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23790&n=obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-odpovedich.

⁶⁶ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁶⁷ Lechner, 2017

⁶⁸ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁶⁹ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁷⁰ Nařízení Evropského parlamentu a Rady EU 2016/679.

správce.⁷¹ Nařízení se v definicích vyjadřuje trochu určitěji, nicméně ve srovnání s těmi v zákoně o ochraně osobních údajů se jedná o významově stejné termíny.

Pověřenec pro ochranu osobních údajů. Zcela nový institut v českém právním prostředí, který je nařízením zaveden. Pověřenec musí být jmenován na základě svých profesních kvalit a odborných znalostí v oblasti ochrany osobních údajů. Není pravda, že každý správce musí mít takového pověřence; povinnost jmenovat pověřence přísluší správci po splnění jedné ze tří podmínek⁷²:

- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

3.2 Fáze implementace

Fáze implementace popisuje E. Škorníčková, která se nástupu nového nařízení Evropské unie věnuje. Jedná se o čtyři etapy⁷³, které jsou společné jak pro veřejný sektor, tak pro soukromé instituce.

1. Zmapování stávajícího stavu. Každá instituce, která sbírá, zpracovává a uchovává osobní údaje, by měla zmapovat, jaké údaje zpracovává, odkud jsou shromažďovány a zda jsou po pominutí účelu jejich použití smazány. Jedná se o údaje externí i interní – zákazníci, odběratelé, dodavatelé, zaměstnanci. Je důležité zajistit řádné zabezpečení především citlivých osobních údajů (o finanční situaci, zdravotním stavu apod.). Se změnami a dopady, které nové nařízení přináší, bude nezbytné seznámit vedoucí pracovníky dotčených institucí a firem. Nebude se jednat o změnu jednoho systému, ale o komplexní změnu téměř veškerých procesů.
2. Detailní analýza zpracování osobních údajů. Cílem této fáze jsou analýzy, revize a stanovení případných náprav pro dosažení kompatibility s nařízením, a to před

⁷¹ Nařízení Evropského parlamentu a Rady EU 2016/679.

⁷² Nařízení Evropského parlamentu a Rady EU 2016/679.

⁷³ Škorníčková, 2017

začátkem jeho účinnosti, tedy od 25.5.2018. Jde o shromáždění veškerých podkladů, na jejichž základě dochází k zákonnému zpracování osobních údajů. Následně je vhodné provést jejich důkladný rozbor, revidovat právní důvody zpracování a posoudit, zda stávající žádosti o souhlas disponují všemi náležitostmi v souladu s novým nařízením – tedy jsou-li souhlasy srozumitelné a jednoznačné. Nevyhnutelná bude také revize informačních systémů včetně jejich zabezpečení a zmapování veškerých zdrojů a úložišť, kde se data nacházejí. Výsledná zpráva pak bude obsahovat celkové vyhodnocení potenciálních rizik, která jsou se zpracováním osobních údajů spojena, na základě kterých budou případně zjednány nápravy (např. úprava firemní dokumentace, směrnic, změna informačních systémů a technologií).

3. Příprava projektových záměrů a jejich časového harmonogramu. Plynule navazující na fázi předchozí, za pomoci odborníků (v oblasti ochrany osobních dat, bezpečnosti informací, práv, projektového managementu atp.) je vhodné stanovit jasný harmonogram, dle kterého budou provedeny změny nutné k dosažení souladu s pravidly nařízení. Pokud nařízení instituci tuto povinnost ukládá, a v případě veřejné správy tomu tak je, součástí této fáze by měl být také výběr pověřence pro ochranu osobních údajů.
4. Spuštění jednotlivých projektových záměrů. Realizace změn by měla probíhat ideálně dále ve spolupráci s odborníky z předchozích fází. Výsledkem bude lepší zabezpečení dat, implicitní ochrana proti možným útokům zevnitř i zvenku a celkové očištění od nadbytečně uchovávaných dat.

Nástupu nového nařízení se věnuje také časopis eGovernment (na příkladů postupů společnosti ICZ, a.s.), a to z hlediska kybernetické bezpečnosti. Je potřeba vyhnout se několika izolovaným řešením, která nejsou v kontextu s firemním IT a s bezpečností celé infrastruktury. Prvním krokem je analýza aktuálního stavu bezpečnosti, jejímž výsledkem je srozumitelný podrobný výstup pro vrcholový management instituce. Zároveň je sledována aktivita uživatelů s rizikovými aplikacemi, hodnotí se stav a způsob zabezpečení mobilních zařízení a koncových stanic. V závěru by měla být s pomocí odborníků provedena hlubší analýza u vybraných rizikových událostí. Na základě

kompletních výsledků je pak možné definovat konkrétní problémy a soustředit se tak na jejich řešení i v souvislosti s nastupujícím nařízením o ochraně osobních údajů.⁷⁴

Základem je bezpečná síť jako funkční celek a následné přidávání dalších prvků, které přispějí k ochraně osobních údajů. Síť je potřeba zabezpečit proti vnějším hrozbám a následně je vhodné se zaměřit na interní služby. V současné době může ale vstup do firemní sítě představovat každé mobilní zařízení – nejedná se tak již o jasně definovanou část sítě, perimetr se tak velmi rozšíří a s ním i riziko.⁷⁵

4 Právo být zapomenut v celkovém pojetí

Další podkapitoly jsou věnovány vybraným odborným článkům, které se problematikou práva být zapomenut zabývají. Úkolem je toto téma a některé jeho aspekty přiblížit.

4.1 Studie č. 1: Rozdílné vnímání evropských a amerických občanů

Následující podkapitola je věnována představení studie *The Right to Inform vs. The right to be Forgotten: A Transatlantic Clash*, která byla publikována roku 2009. Jejím autorem je Franz Werro, jenž působí na významné americké univerzitě a který se specializuje na oblast srovnávacího a mezinárodního práva a soukromí.⁷⁶

V evropském právním prostředí převažují názory odborníků, které ideu práva být zapomenut podporují. Uživatelé internetu by měli mít právo na kontrolu a výmaz informací, které za nimi zanechává jejich aktivita na síti. V roce 2009 ještě existovala domněnka, že se soudy s podobnými problémy nebudou v nejbližších letech setkávat, F. Werro však na příkladu švýcarského právního systému upozorňuje, že již tehdy bylo být zapomenut uplatňováno v případech týkajících se osob odsouzených za trestné činy. Švýcarské právo rozeznává osobnostní práva („*rights of the personality*“, „*die Persönlichkeitsrechte*“), na základě kterých mají tyto osoby nárok na zamezení jejich přímé identifikace s kriminální minulostí po uplynutí určité doby. F. Werro se domnívá, že tato práva mohou být rozšířena i na oblast internetu a uživatelské aktivity. Jak bylo již dříve uvedeno, práva na důstojnost, čest a ochranu soukromého a rodinného života jsou zakotvena v Evropské úmluvě o lidských právech (Článek 8). Stejně tak je tomu i ve švýcarské ústavě a švýcarském občanském zákoníku, kde obecná klauzule říká, že tato

⁷⁴ Magazín Egovernment. 2017. *Kyberbezpečnost, eIDAS a GDPR - nejen osobní ochranný faktor*. Magazín Egovernment. [Online] únor 2017. [Citace: 17. 5. 2017]. <https://www.egovernment.cz/soubor/magazin-egovernment-2-2017/>.

⁷⁵ Magazín Egovernment, 2017

⁷⁶ Georgetown Law. 2017. *Franz Werro*. Georgetown Law. [Online] 2017. [Citace: 20. 7. 2017]. <http://www.law.georgetown.edu/faculty/werro-franz.cfm>.

práva jsou chráněna proti porušení. Je potom úkolem soudů nacházet rovnováhu při vykládání obsahu těchto práv, která mohou být v rozporu s jinými. V důsledku narůstajícího přesahování soukromého a veřejného práva začala být ochrana osobnostních práv zaručena nejen proti státu, ale i proti soukromým osobám a institucím (pozitivní povinnost, „*positive obligation*“). Osobnostní práva tak již nebudou řešena pouze v rovině soukromého, ale také ústavního a evropského práva.

Jako příklady evoluce překrývání soukromého a veřejného práva ilustruje rozebíraná studie F. Werra některé případy nárokování práva být zapomenut, které povětšinou souvisí s tiskovými médii, a tedy právem na svobodu projevu, tisku a práva na informace. Jedním z uváděných případů je *Caroline von Hannover versus Německo*⁷⁷. Von Hannover bojovala již od konce 90. let proti německým bulvárním magazínům, které zveřejnily její fotografie z osobního života⁷⁸, a podle von Hannover tak porušili její právo na soukromí.⁷⁹ V roce 1999 ale následoval neúspěch u německého ústavního soudu, kde převládla svoboda tisku a názor, že jako veřejně známá osobnost musí von Hannover do určité míry tolerovat legitimní zájem veřejnosti o její soukromí. Příklad byl roku 2000 postoupen k Evropskému soudu pro lidská práva. Štrasburský soud vzal tehdy v úvahu, že fotografie nebyly mediálně prospěšné – neměly žádnou informační hodnotu⁸⁰ a žalobkyně nepůsobila jako veřejný činitel ani v politice, a rozhodl ve prospěch Caroline von Hannover.

Případ ze zmiňovaného Švýcarska souvisí s vysíláním rozhlasového dokumentu o životě a popravě jistého zločince odsouzeného na smrt v roce 1939.⁸¹ Jeho syn se dožadoval zamezení vysílání dokumentu z důvodu narušení jeho soukromí a osobních pocitů jako potomka popraveného. Ačkoliv byla všechna fakta pro natáčení získána z veřejných zdrojů – veřejných záznamů, rozhodnutí soudu a rozhovorů s pozůstalými, federální soud rozhodl ve prospěch žalobce. Zdůraznil, že právo šíření jmen osob čelících trestnímu procesu je omezeno pouze po dobu, kdy takový proces probíhá, a po jeho uzavření by tisk ani veřejnost neměli mít k takovým informacím déle právo přístupu.

⁷⁷ Caroline von Hannover, monacká princezna, nejstarší dcera monackého prince Rainiera III.

⁷⁸ Jednalo se o fotografie zachycující aktivity Caroline von Hannover s rodinou a dětmi, v plavkách apod.

⁷⁹ European Court of Human Rights. 2005. *European Court of Human Rights - Chamber judgment (just satisfaction) - von Hannover v. Germany*. Council of Europe. [Online] 2005. [Citace: 3. 6. 2017]. <https://wcd.coe.int/ViewDoc.jsp?p=&id=890483&Site=COE&direct=true>.

⁸⁰ European Court of Human Rights. 2004. *CASE OF VON HANNOVER v. GERMANY*. European Court of Human Rights. [Online] 24. červen 2004. [Citace: 3. 6. 2017]. <http://www.bailii.org/eu/cases/ECHR/2004/294.html>.

⁸¹ Jednalo se o případ X v. Société Suisse et de Télévision, 1983.

Ačkoliv je povinností i právem tisku informovat veřejnost a veřejnost má právo na to být informována, tato práva jsou na druhé straně limitována právem jednotlivců na ochranu jejich soukromí. Uvedené příklady naznačují, že úlohou soudů je najít rovnováhu především mezi svobodou tisku a projevů na jedné straně a respektem k soukromí a důstojnosti jednotlivců na straně druhé.

Ve druhé části své studie F. Werro představuje institut práva být zapomenut v americkém prostředí, kde se vnímání soukromí ve vztahu k ostatním fundamentálním právům značně odlišuje od evropského. Největší důraz je kladen na první dodatek⁸² americké ústavy z roku 1791, který zaručuje mimo jiné svobodu projevu a svobodu tisku. Roku 1890 vzniká již dříve zmíněné dílo L. Brandeise a S. Warrena, *The Right to Privacy*, které lze považovat za první krok k uznání práva na soukromí právě ve vztahu k tisku a novinářskému průmyslu. Většina případů z oblasti spojených států, které jsou ve studii uvedeny, se vyznačuje preferencí prvního dodatku, tedy svobody tisku, před zájmem o soukromí jednotlivce. Rozdíly ve vnímání mezi Amerikou a Evropou plynou z odlišného socio-politického vývoje; evropské právní prostředí je mimo jiné silně ovlivněno francouzskými a germánskými idejemi spojené s reputací, autonomií a sebeurčením a zároveň má vyšší důvěru ve vládní aparát.

4.2 Studie č. 2: Regulační faktory ovlivňující právo být zapomenut

Možnost „hodit minulost za hlavu“ je postupně víc a víc narušována rozvojem moderních technologií. Informace jsou uchovávány ve světě mailových schránek, sociálních sítí a jiných virtuálních úložišť a lze říci, že žádná informace není navždy ztracena. Druhá rozebíraná studie od autorů H. Graux, J. Ausloos a P. Walcke *The Right to be Forgotten in the Internet Era* (r. 2012) polemizuje o tom, jak dalece je schopna legislativa do této oblasti zasahovat.

Počátky fenoménu práva být zapomenut jsou ilustrovány na již zmíněném případě ze Švýcarska, který se týkal vysílání dokumentu o již zesnulém odsouzeném vrahovi, jehož syn se domníval, že zveřejnění dokumentu bude znamenat narušení jeho soukromí. Na právo být zapomenut se primárně odvolává v případech, kdy by mohlo dojít právě k takovému veřejnému odkrytí minulosti jednotlivce, které by poškodilo jeho fundamentální práva.

⁸² Anglicky „The First Amendment“.

Právo být zapomenut je v kontextu poslední doby vnímáno jako aspekt ochrany osobních údajů. Jedná se o koncept vytvoření a udržení přiměřené úrovně ochrany soukromí prostřednictvím vhodně zvolených mechanismů kontroly osobních dat. Autoři studie využili pohledu skrze čtyři regulační faktory Lawrence Lessiga: pravidla (*Norms*), trh (*Market*), technologie (*Code*) a právo (*Law*).

Pravidla. V dnešní informační společnosti dochází k masivnímu sběru a zpracování osobních dat mnoha různými aktéry. Lidé si začínají pomalu uvědomovat, že mají stále menší přehled o tom, kdo údaje zpracovává a do jaké míry k tomu dochází. Ačkoliv je soukromí široký pojem, nepochybně to souvisí se schopností mít kontrolu nad tím, co se s našimi osobními daty děje – právě to se zdá být velmi ceněnou normou. Idea práva být zapomenut je tak projevem hlubšího přání kontroly nad osobními údaji.

Trh. Je možné říci, že internet se v průběhu doby přeměnil na prostředí vhodné především k obchodu, kde jsou osobní data hlavním oběživem. Technologie, která umožňuje téměř neomezené hromadění a ukládání informací, způsobuje zásadní rozdíly mezi jejich uživateli a jejich původci – subjekty údajů; v rámci internetového prostředí jsou subjekty oproti uživatelům prakticky bezmocní. Studie zdůrazňuje, že lze sledovat dvě protichůdné tendence: poptávka po službách, jejichž funkce je založena právě na zpracování osobních dat (fitness aplikace, sledování stravy, online bankovníctví aj.) je stále vyšší, a zároveň dochází k intenzivnějšímu dožadování se vyšší ochrany osobních údajů⁸³.

Technologie. Osobní údaje musí být uchovány pouze po dobu ne delší než je nezbytně nutné k naplnění účelu, za jakým byly shromážděny. V této souvislosti bylo diskutovaným nápadem označení shromažďovaných údajů datem ukončení platnosti jako součástí jejich metadat. Výhodou tohoto konceptu je sejmutí aktivní role jednotlivce, co se týká jeho zodpovědnosti po sdílení svých osobních údajů. Washingtonská univerzita také pracovala na technologii „*Vanish*“⁸⁴, jejíž podstatou byla schopnost autodestrukce dat po uplynutí určité doby. Různé způsoby technologického řešení ochrany osobních dat se zdají být užitečné ve vztahu k praktické aplikaci práva být zapomenut, autoři studie však upozorňují na fakt, že je stále přítomné riziko zneužití a zkopírování takových dat třetí stranou. Subjekt údajů osobní informace poskytuje v dobré víře a pouze se spoléhá

⁸³ Tomuto jevu se také přezdívá paradox soukromí („the privacy paradox“).

⁸⁴ V překladu „zmizet“.

na zpracovatele dat, že budou použita přesně za účelem, který byl stanoven. Pro zaručení ochrany subjektům údajů je v tomto případě zákonná intervence nezbytná.

Právo. Plní důležitou roli v ujišťování občanů, že jejich soukromí je dostatečně chráněno. I tato studie zde podotýká, že ačkoliv právo být zapomenut sice není ve stávající směrnici explicitně zmíněno, je svým způsobem zajištěno v Článku 6, který říká, že osobní údaje „*uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány*“.⁸⁵ a dále, že „*aby nepřesné nebo neúplné údaje s ohledem na účely, pro které byly shromažďovány nebo dále zpracovávány, byly vymazány nebo opraveny*“.⁸⁶ Na základě těchto ustanovení se od správců žádá, aby byly osobní údaje, u nichž účel zpracování pominul, vymazány. Studie dále ale předkládá jisté slabé stránky, které současný evropský legislativní rámec týkající se ochrany osobních údajů má a které mají vliv na jeho efektivitu v aplikaci. Dříve zmíněné právo na výmaz či opravu je právem pasivním, a v praxi jen málokdy dochází k jeho prosazování. Navíc mají správci dat značnou volnost, co se týká určování toho, jak dlouho uchovávání osobních údajů stále slouží jejich legitimní účelu (např. sociální sítě – uchovávání poskytnutých údajů uživateli po dobu neurčitou je legitimní, protože spadá mezi legitimní účely činnosti sítě). Co se týká aktivních práv subjektu údajů, stávající směrnice mu dle Článku 12 zaručuje získat od správce „*sdělení srozumitelnou formou o údajích, které jsou předmětem zpracování, a veškeré dostupné informace o původu údajů*“⁸⁷ a „*opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů*“⁸⁸. Jak už bylo řečeno dříve, subjekt údajů má právo požádat o vymazání personálních dat, a to například v případech, že tato data již nejsou přesná či nejsou relevantní pro účel, za jakým byla původně shromážděna, nebo uplynula doba nezbytně nutná pro naplnění účelu; situace v praxi se ale může lišit. V situacích, že subjekt údajů udělil souhlas se zpracováním dat k určitému účelu, správce dat může později tvrdit, kdy tato data jsou ve vztahu k danému účelu stále relevantní. V těchto případech se subjekt údajů výmazu bohužel pravděpodobně nedočká.

Výše zmíněné slabé stránky použití některých práv v praxi se dle studie týkají právě souhlasu se zpracováním. Řešení situace není tak snadné, jakmile je souhlas udělen;

⁸⁵ Směrnice Evropského parlamentu a Rady 95/46/ES, Článek 6 odst. 1 písm. e.

⁸⁶ Směrnice Evropského parlamentu a Rady 95/46/ES, Článek 6 odst. 1 písm. d.

⁸⁷ Směrnice Evropského parlamentu a Rady 95/46/ES, Článek 12, písm. a.

⁸⁸ Směrnice Evropského parlamentu a Rady 95/46/ES, Článek 12, písm. b.

současný legislativní rámec totiž v praxi není schopen zajistit subjektům údajů dostatečnou kontrolu nad jejich personálními daty. Podle vyjádření WP29 by měli mít jednotlivci vždy právo udělený souhlas odvolat. Taková akce ale není retroaktivní a zamezí pouze budoucímu zpracování údajů.⁸⁹

Studie dále předkládá důvody, jaké stojí za navrhovaným „novým“ právem být zapomenut. Z hlediska dnešní informační společnosti je téměř nemožné předvídat všechny následky, často negativní, které jsou spojeny s využíváním osobních údajů. Právo být zapomenut by mělo sloužit jako bezpečnostní pojistka proti nepředvídatelným situacím souvisejícím s ochranou personálních dat. Osobní údaje jsou velmi širokým pojmem, kde při použití velmi záleží na kontextu a sekundárních informacích, které se s nimi pojí. Nové právo být zapomenut by mělo být schopno se na tuto dynamiku adaptovat a dát tak lidem možnost hodnotit a přehodnocovat používání jejich údajů. V neposlední řadě by tato skutečnost měla znamenat i zvýšení kontroly jednotlivců nad jejich identitou. Návrh nového opatření ubíral na důležitosti výše zmíněného souhlasu se zpracováním, a to například právě díky skutečnosti, že by subjekt údajů měl mít právo na jeho okamžité odvolání.

4.3 Studie č. 3: Možnosti nahlížení na institut soukromí

Další studie, která se věnuje fenoménu práva být zapomenut, je studie R. K. Walkera *Right to be Forgotten* (r. 2012). Věnuje se mu především z hlediska možnosti aplikace tohoto práva ve Spojených státech ve vztahu ke svobodě projevu, která byla již zmíněna v rozboru jednoho z předchozích článků; nicméně pro komparaci je zde využít také pohled na právní a kulturní prostředí Evropské unie a návrh nového opatření.

Studie č. 3 se vrací k otázce, jak definovat soukromí. Existuje řada vědeckých názorů, které se dohadují, že soukromí by mělo být považováno za formu duševního či kvazi-duševního vlastnictví. Zastánci této teorie se domnívají, že jednotlivci by měli mít na svá data vlastnické právo, což by jim jakožto uživatelům umožnilo i vyšší kontrolu. Duševní vlastnictví by mohlo být vhodným základem pro právo být zapomenut, jehož pozitivem by byl i fakt, že tento přístup by byl závazný pro všechny, a nikoliv jen pro strany vázané smluvními vztahy. Tento koncept, kde by se personální informace staly zcizitelnými, by pravděpodobně vyústil ve vznik trhu, kde by jednotlivci mohli své informace prodávat či jinak směřovat. Z ústavního hlediska je ale tento model problematický – jedním z aspektů

⁸⁹ Article 29 Data Protection Working Party. 2011. *Opinion 15/2011 on the definition of consent*. European Commission. [Online] 13. červen 2011. [Citace: 13. 7. 2017]. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

vlastnického práva je vylučitelnost ostatních. Ve vztahu k duševnímu vlastnictví je to pak vylučitelnost týkající se komunikování informací – v podstatě právo zabránit ostatním *mluvit*. Tato skutečnost by se pravděpodobně dostávala do konfliktu především v americkém prostředí (ve vztahu k prvnímu dodatku ústavy, který hovoří právě o nedotknutelnosti svobody projevu a tisku).

R. K. Walker také zdůrazňuje existenci odlišného vnímání soukromí Američany a Evropany. Na obecné úrovni se jedná o soukromí spíše jako aspekt osobní svobody na jedné straně (Spojené státy Americké) a součást osobní důstojnosti na straně druhé (Evropa). Američané jsou charakterističtí svou nedůvěrou v centralizovanou moc a ve vládě spatřují základního nepřítele svého soukromí. V evropském prostředí jsou zákony související s ochranou soukromí primárně určeny na ochranu důstojnosti, reputace a toho, jak je jednotlivec vnímán veřejností nežli na ochranu před zásahy ze strany vládního aparátu. Tento postoj je reflektován v již několikrát citovaném Článku 8 Úmluvy o ochraně lidských práv a základních svobod. Evropské soudy mají tendenci se méně znepokojovat ochranou svobodného projevu a jsou ochotny projev omezit, pokud je to nutné právě k ochraně důstojnosti občanů.

Dle studie č. 3 tyto rozdíly dávají v konečném důsledku vzniknout otázce *kdo* by měl být ochráncem personálních informací, nežli *jaké* informace by měly být chráněny. V evropském prostředí má hlavní slovo stát, zatímco ve Spojených státech se klade důraz především na svobodu projevu a je tak na každém jednotlivci chránit si své soukromí.

Původ práva být zapomenut lze nalézt ve francouzské legislativě, která zaručuje tzv. *le droit à l'oubli*, anglicky *right to oblivion*, v překladu jako právo zapomenout⁹⁰, které se vztahovalo na nárok zamezení publikace informací o odsouzených, kteří si trest již odpykali. Má se za to, že kriminální minulost by neměla ovlivňovat současnou reputaci osoby, jejímž cílem je úspěšné znovuzapojení do běžného života.

Na základě těchto odůvodnění vydala Evropská komise roku 2010 sdělení věnované komplexnímu přístupu k ochraně osobních dat. Takový přístup by měl zahrnovat rozšířené právo být zapomenut, které se vztahuje nejen na osobní údaje rehabilitovaných odsouzených, ale i na osobní údaje všech osob. Toto právo bylo v návrhu definováno jako právo jednotlivců na výmaz sdělených dat, pokud již déle neslouží k legitimním účelům.

⁹⁰ Překlady se jen málo liší od zkoumaného termínu „právo být zapomenut“, množství odborných studií ale upozorňuje, že tato práva nemají být zaměňována.

Tato definice však navazuje na Článek 6 stávající evropské Směrnice o ochraně osobních údajů. V roce 2012 Viviane Reding⁹¹ navrhla, že by právo být zapomenut mělo být převzato napříč všemi členskými státy Evropské unie. Prohlásila tehdy, že jestliže si jednotlivec nepřeje, aby jeho data byla dále zpracovávána a uložena (správcem dat), pak by taková data měla být odstraněna ze systému, pokud neexistují legitimní důvody k jejich uchování. Následovaly debaty, jaké dopady bude mít návrh na svobodu projevu a na hospodářství.

4.4 Sumarizace

Výše zmíněné články ilustrovaly jistý přirozený vývoj práva být zapomenut, kde případy souvisely ve velké míře s narušením soukromí fyzické osoby ze strany médií. S rozvojem informačních technologií a informační společnosti je rok od roku snazší dostávat se k různým informacím a datům a je rovněž snazší je uchovávat a nebo dále šířit. Obrovský boom internetu znamenal také nutnou změnu některých stávajících dogmat a v neposlední řadě si žádá i změnu legislativy.

Je vhodné připomenout zajímavý „paradox soukromí“, kdy dochází k růstu poptávky po službách (aplikacích), které vyžadují zadání personálních údajů, a zároveň k dožadování se vyššího stupně jejich ochrany. Studie často hovoří o právu být zapomenut ve vztahu ke stopě, kterou zanechává aktivita uživatele na internetové síti; lidé se často dovolávají tohoto práva ve chvílích, kdy zveřejněnými informacemi utrpí jejich důstojnost či mají pocit nepřiměřeného zásahu do soukromí. Lze tvrdit, že evropské prostředí se vyznačuje vyšší důvěrou ve vládní aparát, a také věří v zajištění ochranných prostředků z jeho strany; je tedy možné se domnívat, že při sdělování personálních dat a vyjadřování souhlasu s jejich zpracováním směrem k veřejné správě nebude docházet k větším konfliktům. Ze strany státu je ovšem nutné zabezpečit data proti vnějším i vnitřním útokům a zařadit kyberbezpečnost do dlouhodobé strategie.

Studie mimo jiné osvětlily oblasti, které lze považovat za základní pilíře ochrany osobních údajů. Co se týká společnosti, bude nezbytné zdůrazňovat informační etiku, tj. oblast morálky, která je uplatňována při vzniku, šíření, transformaci, ukládání, vyhledávání, využívání a organizaci informací. Souvisí zejména se žurnalistikou, kde se soukromí často střetává se svobodou projevu a tisku. Informace byly ve studiích pokládány za oběživo na internetovém trhu, zmíněna byla idea nakládání s nimi jako

⁹¹ Evropská komisařka pro spravedlnost.

s majetkem – s duševním vlastnictvím. Tato teorie ale jistě bude dále nestabilní vzhledem k bariéře vylučitelnosti ze spotřeby ve vzniknuvším tržním prostředí – *zakázat* někomu o informacích *mluvit*.

Zajištění ochrany ve smyslu úniku, zneužití, napadení či jiné manipulace se shromažďovanými daty bude velkou výzvou pro technologii, stejně jako jejich diskutované smazání a odstranění.

5 „Nové“ definování práva být zapomenut

Následující podkapitola je věnována soudnímu případu španělského občana Maria Costeji Gonzáleze, jehož následkem bylo mimo jiné rozšíření povědomí občanů o právu na likvidaci osobních údajů v prostředí internetové sítě. Současně odstartoval diskuze o bezpečnosti osobních údajů v době nebývalého rozvoje internetu (a především internetových vyhledávačů), kdy je ale stále platná direktiva z roku 1995 z doby internetových počátků.

Roku 2010 podal španělský občan Mario Costeja González stížnost k Agencia Española de Protección de Datos (Státní úřad pro ochranu údajů, dále jen „AEPD“) proti velké vydavatelské společnosti La Vanguardia Ediciones SL (dále jen „La Vanguardia“) a současně také proti společnostem Google Spain a Google Inc. Důvodem stížnosti a předmětem sporu byla skutečnost, že se po vyhledání Costejova jména pomocí internetového vyhledávače Google zobrazuje odkaz na článek deníku La Vanguardia z roku 1998. V tomto článku bylo tehdy uvedeno Costejovo jméno ve spojitosti s dražbou nemovitostí v důsledku dluhů na sociálním zabezpečení. Protože zmíněné pohledávky byly již několik let vyrovnány, a tudíž zmínky o nich irelevantní, Mario Costeja González se domáhal dvou věcí; tou první bylo odstranění či změna stránek ze strany La Vanguardia, a to tak, aby se na nich déle neobjevovaly jeho osobní údaje, anebo aby se využilo nástrojů, které k ochraně osobních údajů poskytují internetové vyhledávače. Dále se dožadoval, aby společnosti Google Spain či Google Inc. odstranily nebo skryly tyto osobní údaje takovým způsobem, aby se dále nezobrazovaly ve výsledcích vyhledávání a nebyly propojeny s odkazem na deník La Vanguardia.⁹²

⁹² Soudní dvůr Evropské unie. 2014. *Rozsudek Soudního dvora*. CURIA. [Online] 13. květen 2014. [Citace: 17. 6. 2017]. <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=cs>.

Mario Costeja González se ve své věci odkazoval na Článek 8 Listiny základních práv Evropské unie:

„1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.“

V souvislosti se zpracováním a ochranou osobních údajů se žádost dále vztahovala k výkladu Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.⁹³ Na tomto místě je vhodné citovat Článek 12, písm. b), kde je uvedeno, že členské státy zaručí každému subjektu údajů právo získat od správce „*podle daného případu opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů*“, a Článek 14, písm. a), kdy členské státy přiznávají subjektu údajů právo „*alespoň v případech uvedených v čl. 7 písm. e) a f) vznést kdykoli z vážných a legitimních důvodů souvisejících s jeho osobní situací námitku proti zpracování osobních údajů, které se ho týkají, ledaže vnitrostátní právo stanoví jinak. Je-li námitka oprávněná, nesmí se zpracování zahájené správcem těchto údajů nadále týkat*“.

V tom samém roce podání žádosti, tedy v roce 2010, došlo ze strany AEPD k zamítnutí Costejovy žádosti v rozsahu, v jakém se týkala deníku La Vanguardia. V rámci zkoumání došel AEPD k závěru, že dotčené informace uvedené v deníku byly v té době právně odůvodněné – k jejich zveřejnění došlo tehdy na základě nařízení místního ministerstva práce a sociálních věcí, s účelem informovat a zajistit co nejvyšší účast při dražbě nemovitostí.⁹⁴

Na druhé straně ale bylo vyhověno žádosti v rozsahu týkající se společností Google Spain a Google Inc. Dle AEPD „*provozovatelé vyhledávačů podléhají právní úpravě v oblasti ochrany údajů, neboť provádějí zpracování údajů, za které odpovídají, a jednají jako zprostředkovatelé informační společnosti*“.⁹⁵ V případě, že by umístění a šíření

⁹³ Na konkrétní články odkazuje rozsudek.

⁹⁴ Soudní dvůr Evropské unie, 2014.

⁹⁵ Soudní dvůr Evropské unie, 2014.

některých údajů mohlo vést k porušení základního práva na ochranu údajů a lidské důstojnosti, AEPD může být oprávněn uložit výmaz nebo zákaz přístupu k těmto údajům ze strany provozovatelů vyhledávačů (v tomto případě obě společnosti Google). Podle AEPD není nezbytné, aby došlo k výmazu na webových stránkách, kde se informace původně nacházejí, a tím spíš, pokud jsou kryty právním předpisem.⁹⁶ Rozsudek byl vynesena Evropským soudním dvorem v květnu roku 2014.

Evropskému soudnímu dvoru byla tehdy kauza postoupena s následujícími otázkami:⁹⁷

1. Územní působnost: vztahují se právní předpisy EU na společnost Google Spain v tomto případě, kdy se server zpracovávající data nachází v USA?
2. Věcná působnost: vztahuje se směrnice EU 45/96/ES na vyhledávače typu Google?
3. Právo být zapomenut: má jedinec právo na to, aby jeho osobní údaje nebyly ostatním uživatelům internetu známy a byly odstraněny z dosahu vyhledávačů (čili být zapomenut)?

Soudní dvůr Evropské unie uvedl ve svém rozsudku:⁹⁸

1. Pokud provozovatel internetových vyhledávačů vlastní pobočku nebo dceřinou společnost, která se zabývá podporou prodeje a prodejem reklamního prostoru (pozn. jedná se o zásadní část obchodní činnosti společnosti Google, která by mohla být úzce spojena s Google Search), pravidla Evropské unie se na něj vztahují i tehdy, pokud se server pro zpracování dat nachází mimo Evropu.
2. Vyhledávače na osobní údaje dohlíží, jsou tedy správci, a Google se tak nemůže vyhnout povinnosti vyplývající z evropského práva při nakládání s nimi.
3. Fyzické osoby mají právo za určitých podmínek požadovat po vyhledávačích odstranění výsledků, které jsou spojeny s jejich osobními údaji. Je tomu tak v případě, že zveřejněné informace jsou nepřiměřené, nepodstatné a přesahují míru s ohledem na účely zpracování, nejsou aktualizované nebo jsou uchovávané po dobu delší než nezbytně nutnou. Právo být zapomenut však není absolutním

⁹⁶ Soudní dvůr Evropské unie, 2014.

⁹⁷ Jääskinen, Niil. 2014. *Stanovisko generálního advokáta N. Jääskinena přednesené dne 25. června 2013*. CURIA. [Online] 25. červen 2014. [Citace: 17. 6. 2017]. curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=433733.

⁹⁸ Soudní dvůr Evropské unie, 2014.

právem, vždy je potřeba přihlížet k individuálním skutečnostem a k dalším základním právům, jako např. svoboda projevu.

Rozsudek Evropského soudního dvora zavdal vzniku diskuzím, jaké povinnosti přísluší provozovatelům vyhledávačů (které se náhle dostaly do role správců) a jak aktuální Směrnici vykládat v kontextu neustále se rozvíjejících technologiích. Důležitá je ale skutečnost, že tento rozsudek v podstatě představil nový koncept práva být zapomenut v internetovém prostředí.

6 Úvod do e-Governmentu

Především kapitoly poskytly náhled na pojetí soukromí, ochranu osobních údajů a jejich legislativní úpravu a nastínily problematiku práva být zapomenut. Využívání internetu je již globální záležitostí a „potřeba“ být zapomenut a znovu nabýt kontrolu nad osobními daty není řešena pouze na soukromé rovině; k některým střetům může docházet také ve veřejné správě, kdy ke shromažďování osobních údajů dochází ze strany států či jiných orgánů veřejné moci. Následující kapitoly jsou věnovány právě veřejné správě, která také prochází modernizací a elektronizací s dopady na sběr, publikaci a uchovávání některých personálních dat. Tato kapitola poslouží jako vhodné přemostění k závěrečné kapitole.

Lze se domnívat, že e-government – elektronická veřejná správa⁹⁹ fakticky vznikla se zavedením prvního počítače, samotný pojem však v té době neexistoval. Obecně je tedy e-government vnímán jako rozsáhlý transformační proces týkající se širokého spektra oblastí napříč vládnutím a správou, ke kterému dochází s rozvojem internetu (především v druhé polovině 90. let 20. století).¹⁰⁰

Dle definice OECD¹⁰¹ se e-government zaměřuje na využívání nových informačních a komunikačních technologií (ICTs¹⁰²) v celé řadě vládních funkcí, tedy i činnostech veřejné správy.¹⁰³ Zapojení těchto technologií by mělo vést k efektivnějšímu a transparentnějšímu fungování správy, poskytování většího množství a kvalitnějších informací a služeb pro veřejnost a usnadnit občanskou participaci v samotném procesu vládnutí. V neposlední řadě tak dochází k výraznému usnadnění komunikace.¹⁰⁴ Podobně

⁹⁹ Pojem e-government je v českém prostředí běžně užíván bez konkrétního překladu. Obecně se jím rozumí elektronická veřejná správa.

¹⁰⁰ Curtin, Gregory G. 2007. *E-Government*. Bedrosian Center. [Online] 2007. [Citace: 3. 8. 2017]. https://bedrosian.usc.edu/files/2012/07/encyclopedia_of_political_communications.pdf.

¹⁰¹ Organisation for Economic Co-operation and Development. Organizace pro hospodářskou spolupráci a rozvoj.

¹⁰² Z anglického Information and Communication Technologies.

¹⁰³ OECD. 2002. *Glossary of Statistical Terms*. OECD Statistics. [Online] 2002. [Citace: 18. 6. 2017]. <https://stats.oecd.org/glossary/detail.asp?ID=4752>.

¹⁰⁴ Curtin, 2007

chápe e-government také Evropská komise, která tento pojem vymezila ve svém Akčním plánu. Rovněž se tímto pojmem rozumí administrativní komunikace a procedury, které jsou realizované elektronicky.¹⁰⁵ Ze strany OECD také dochází k pravidelnému monitoringu uplatňování e-governmentu ve vybraných zemích.¹⁰⁶

V domácí literatuře je e-government vymezen jako využívání informačních technologií veřejnými institucemi pro zajištění interakce a výměny informací s občany, soukromými podniky a nebo jinými orgány veřejné správy. Hlavní účel spočívá ve zvýšení efektivity fungování a poskytování rychlých, dostupných a kvalitních služeb a informací. Bývalé Ministerstvo informatiky definovalo daný pojem pouze úžeji pouze ve vztahu k veřejné správě jako „*proces transformace vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím posláním je rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu k jejím uživatelům.*“¹⁰⁷

Přestože neexistuje jednotná definice e-governmentu, lze říci, že obecným hlavním smyslem elektronizace veřejné správy je větší transparentnost a zvýšení komfortu komunikace soukromých subjektů s orgány veřejné moci, a to za pomoci zefektivnění interních procesů tohoto veřejného sektoru. Tento koncept by měl také přispívat k vytváření tzv. dobré správy (Good Governance).¹⁰⁸ Problematika Good Governance se zabývá hledáním optimálního a efektivního stavu vládnutí, který v dlouhém období vede k ekonomické prosperitě a sociální vyváženosti, jež mají za cíl posílit důvěru ve vládu a její legitimitu v demokratickém prostředí. Idea dobré správy vznikla jako reakce na předchozí formy tzv. špatného vládnutí, kdy převažovala vysoká míra korupce a malý respekt k lidským právům. Mezi základní znaky konceptu Good Governance patří¹⁰⁹:

- efektivní, nestranný a rychlý soudní proces,
- transparentní veřejné instituce,
- odpovědnost za rozhodování veřejných činitelů,
- převod zdrojů a rozhodování z centra na místní úroveň,

¹⁰⁵ Mates, Pavel a Smejkal, Vladimír. 2012. *E-government v České republice: Právní a technologické aspekty*. Praha : Leges, 2012. ISBN 978-80-87576-36-6.

¹⁰⁶ Mates, a další, 2012)

¹⁰⁷ Mates, a další, 2012), str. 39.

¹⁰⁸ Mates, a další, 2012

¹⁰⁹ Good Governance. *O Good Governance*. Good Governance. [Online] [Citace: 16. 7. 2017]. <http://goodgovernance.cz/o-good-governance/>.

- smysluplná účast občanů při projednávání veřejných politik,
- univerzální ochrana lidských práv,
- nediskriminační zákony.

Za zmínění stojí také definice Světové banky, která ve své podstatě shrnuje skutečnosti uvedené v předchozích odstavcích. Vládní aparát využívá informační technologie (širokopásmové sítě, internet, mobilní zařízení aj.), které mají schopnost transformovat vztahy s občany, soukromými institucemi a jinými veřejnými orgány. Tyto technologie mohou být prostředkem k naplnění mnoha různých cílů – lepší poskytování vládních služeb občanům, lepší spolupráce s jinými podniky a v oblasti průmyslu, posílení postavení občana za pomoci přístupu k informacím nebo efektivnější vládní řízení. Výsledné přínosy mohou být snížení korupce, zvýšená transparentnost, růst výnosů a/nebo snížení nákladů.¹¹⁰

Vedle monitoringu OECD existuje také E-government Survey, průzkum, který je prováděn OSN¹¹¹. Od roku 2003 jsou zveřejňovány výsledky průzkumů a umístění zemí v žebříčku e-governmentu dle indexu EGDI¹¹². V mezinárodním srovnání se aktuální pozice České republiky nachází až na 50. místě¹¹³ a v rozvoji e-governmentu tak zaostává.¹¹⁴ Jedním z cílů iniciativy 202020.cz je posunout se v tomto hodnocení do první dvacítky států, mezi kterými se nachází Spojené království, Jižní Korea, Dánsko, Švédsko nebo Francie.¹¹⁵

Strategický rámec rozvoje veřejné správy pro období 2014-2020 stanovil následující cíle¹¹⁶:

1. Modernizace veřejné správy.
2. Revize a optimalizace výkonu veřejné správy v území.
3. Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu.

¹¹⁰ Curtin, 2007

¹¹¹ Organizace spojených národů.

¹¹² E-government Development Index.

¹¹³ Index je dále rozdělen na kategorie velmi vysoký – vysoký – střední – nízký. Česká republika se i přes své umístění nachází ve skupině zemí s vysokým indexem. Department of Economic and Social Affairs. 2016. *United Nations E-Government Survey 2016*. [Online] 2016. [Citace: 20. 7. 2017]. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf>.

¹¹⁴ Iniciativa 202020. 2016. *Náše vize. 202020*. [Online] 2016. [Citace: 22. 7. 2017]. <http://202020.cz/nase-vize/>.

¹¹⁵ United Nations. 2016. *UN E-Government Survey 2016*. Public Administration and Development Management. [Online] 2016. [Citace: 22. 7. 2017]. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.

¹¹⁶ MVČR. 2017. *Implementační plány*. Ministerstvo vnitra České republiky. [Online] 2017. [Citace: 29. 7. 2017]. <http://www.mvcr.cz/clanek/implementacni-plany.aspx>.

4. Profesionalizace a rozvoj lidských zdrojů ve veřejné správě.

Implementační plán pro strategický cíl č. 3 zmiňuje především dobudování e-governmentu, rozšíření, propojení a konsolidaci datového fondu veřejné správy, úplné elektronické podání nebo kybernetickou bezpečnost.

6.1 Stručný vývoj e-governmentu v České republice

Již po vzniku samostatné České republiky se v rámci transformace státu do moderní ústavní demokracie objevovala snaha o elektronizaci veřejné správy. Roku 1991 vzniká Komise vlády České republiky pro Státní informační systém, jejímž primárním úkolem bylo sjednocení tehdy velmi roztržštěných informačních systémů a zaměřit se na rozvoj jednotného státního informačního systému. V témže roce je také přijato ustanovení o řešení státního informačního systému, založené na územně identifikačním registru, dále na registrech občanů, nemovitostí a hospodářských subjektů. Výstavba státního informačního systému započala až o několik let později v roce 1995, kdy došlo k jejímu odsouhlasení. Roku 1996 vzniká Úřad pro státní informační systém, který nahradil jako koordinátor tehdejší Ministerstvo hospodářství.¹¹⁷

Roku 1999 je přijata Státní informační politika¹¹⁸, kterou lze považovat za první ucelenou koncepci. Hlavní ideou bylo zefektivnit a usnadnit občanům agendu s veřejnou správou a za tímto účelem vytvoření vhodných informačních systémů. Pokrývala tři základní oblasti: informatizace veřejné správy, informační gramotnost (vzdělávání) a elektronický obchod.¹¹⁹ Dále měla být vytvořena síť kontaktních míst veřejné správy, kde data, sdělená jednomu subjektu veřejné správy, budou dostupná také pro její ostatní subjekty. Pro realizaci budování zmíněného informačního systému veřejné správy bylo potřeba zaměřit se také na související komunikační infrastrukturu.¹²⁰ Na dříve zmíněnou Státní informační politiku navázal dokument „Akční plán realizace státní informační politiky do roku 2003“, který obsahoval konkrétnější rozpracování jednotlivých cílů. Původní představa jednotného státního informačního systému byla nahrazena ideou individuálních informačních systémů veřejné správy, které by byly vzájemně propojeny a poskytovaly tak širokou škálu služeb veřejné správě i občanům.¹²¹

¹¹⁷ Špaček, David. 2012. *eGovernment - cíle, trendy a přístupy k jeho hodnocení*. Praha : C.H. Beck, 2012. 978-80-7400-261-8.

¹¹⁸ „Státní informační politika – cesta k informační společnosti.“

¹¹⁹ Česká republika. 1999. *Státní informační a komunikační politika - e-Česko 2006*. Culturenet. [Online] 1999. [Citace: 30. 7. 2017]. <http://www.culturenet.cz/res/data/002/000269.pdf>.

¹²⁰ Špaček, 2012

¹²¹ Česká republika., 1999

Z pohledu související legislativy je zlomový rok 2000. Dochází k přijetí dvou zákonů, a to zákona č. 227/2000 Sb., o elektronickém podpisu a zákona č. 365/2000 Sb., o informačních systémech veřejné správy¹²². Zákon o elektronickém podpisu byl vytvořen na základě směrnice Evropské unie 1999/93/EC, o zásadách Společenství pro elektronické podpisy a jeho smyslem bylo umožnění použití digitálního podpisu v rámci elektronické komunikace. Digitální podpis představoval ekvivalent k vlastnoručnímu podpisu využívaného v běžné listinné komunikaci.¹²³ Zákon o informačních systémech veřejné správy stanovil práva a povinnosti správců těchto systémů a dalších souvisejících subjektů. Tento zákon by měl přispívat ke zkvalitnění systémů veřejné správy a představovat tak dobrý nástroj pro její výkon.¹²⁴ Na základě zákona o informačních systémech veřejné správy mělo být také vytvořeno jednotné přístupové místo k zaručeným informacím a elektronickým službám veřejné správy pro občany, podnikatelské subjekty i orgány a organizace veřejné správy – a v roce 2004 byl spuštěn portál veřejné správy portal.gov.cz.¹²⁵

Ke konci roku 2002 byl schválen vznik Ministerstva informatiky¹²⁶, které bylo zřízeno od počátku roku 2003. Pod nově vzniknuvší ministerstvo spadaly mimo jiné i kompetence Úřadu pro ochranu osobních údajů v oblasti elektronických podpisů. Ke zrušení Ministerstva informatiky však došlo již v roce 2007.¹²⁷

Další zákony, které souvisejí s vývojem e-governmentu v České republice, patří dále:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- zákon č. 480/2004 Sb., o některých službách informační společnosti,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- zákon č. 500/2004 Sb., správní řád,
- zákon č. 127/2005 Sb., o elektronických komunikacích,

¹²² Zákon 365/2000 Sb. vychází z dříve zmíněného „Akčního plánu realizace státní informační politiky do roku 2003“ a idey propojených informačních systémů veřejné správy.

¹²³ MVČR. 2012. *Zákon č. 227/2000 Sb., o elektronickém podpisu*. Ministerstvo vnitra České republiky. [Online] 1. říjen 2012. [Citace: 30. 7. 2017]. <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

¹²⁴ MVČR. *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy*. Ministerstvo vnitra České republiky. [Online] 24. říjen 2016. [Citace: 30. 7. 2017]. <http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx>.

¹²⁵ Peterka, Jiří. 2003. *Portál veřejné správy odstartuje za měsíc*. Archiv článků a přednášek Jiřího Peterky. [Online] 2003. [Citace: 30. 7. 2017]. <http://www.earchiv.cz/b03/b0915001.php3>.

¹²⁶ iDNES.cz. 2002. *Senát schválil vznik ministerstva informatiky*. iDNES.cz. [Online] 15. listopad 2002. [Citace: 30. 7. 2017]. http://mobil.idnes.cz/senat-schvalil-vznik-ministerstva-informatiky-f54-/mob_tech.aspx?c=A021114_5182628_mob_aktuality.

¹²⁷ eGov.cz. 2014. *Ministerstvo informatiky*. eGov.cz. [Online] 2014. [Citace: 30. 7. 2017]. <http://www.egov.cz/kdo-je-kdo/institute/ministerstvo-informatiky>.

- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů („Zákon o e-Governmentu”) – zákon upravuje oblast elektronických úkonů orgánů veřejné moci vůči fyzickým a právnickým osobám, elektronických úkonů fyzických a právnických osob vůči orgánům veřejné moci a elektronických úkonů mezi orgány veřejné moci navzájem prostřednictvím datových schránek, dále datové schránky, informační systémy datových schránek a autorizovanou konverzi dokumentů,
- zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů,
- zákon č. 111/2009 Sb., o základních registrech,
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce – vychází z 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 (zkráceně eIDAS) a zrušuje zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.

E-government je obsažen v mnoha právních předpisech, a dle některých odborníků se jedná spíše o nahodilou činnost nežli vědomý a kontinuální proces. Část předpisů vznikala pod vlivem legislativy Evropské unie, část v rámci cesty za modernizací a zvýšením efektivity veřejné správy. Roli hrála také aktuální politická situace. Jako další problém se objevuje z legislativně-technické stránky věci, kdy je nutné do právních úprav zakotvit vysoce odborné termíny (mnohdy definované odlišně pro účely toho kterého zákona), které jsou pro běžné uživatele těžko srozumitelné. Právo také nemá schopnost předcházet regulaci, zejména v oblasti tak dynamické jako je e-government, a to ze zřejmých důvodů – lze očekávat, že se v průběhu let budou objevovat nové prostředky jeho realizace a nové funkce, kde může být e-government uplatňován.¹²⁸ Mezi základní nástroje e-governmentu lze zahrnout:

- informační portál veřejné správy,
- kontaktní místa veřejné správy,
- datové schránky,

¹²⁸ Mates, a další, 2012

- elektronický podpis,
- základní registry.

7 Registry státní správy jako nástroj e-governmentu v České republice

Registry státní správy jsou jedním z nástrojů českého e-governmentu. Již v 90. letech minulého století byla diskutováno zřízení registrů pro potřeby užívání veřejných orgánů, které by obsahovaly systematicky uspořádané a bezchybné údaje. Stávající evidence byly roztržité a tehdejší nekomplexní právní úprava vedla k neefektivitě užívání shromážděných dat. Právní úprava, která by umožnila sdílení a lepší využívání těchto dat, neexistovala. „*Cílem právní úpravy je přeměna současného systému sběru a uchovávání údajů roztržitých v různých rejstřících, registrech a evidencích v systém nový, který umožní díky jasně definovaným pravidlům stanovené informace sbírat a se zárukou spolehlivosti využívat v celé veřejné správě.*“¹²⁹ K realizaci tohoto záměru došlo v roce 2009, kdy byla Poslaneckou sněmovnou přijata komplexní úprava v podobě jednoho zákona.¹³⁰ Jedním z hlavních principů navrhované úpravy bylo sdílení referenčních údajů orgány veřejné moci, které by již nezískávaly údaje z různých zdrojů, ale pouze ze základních registrů, odkud budou přebírány do dalších informačních systémů veřejné správy. Tento přístup zároveň zajistí zkvalitnění údajů a zároveň umožní klientům veřejné správy hlásit údaje pouze jednou. Veřejná správa by tak měla dosáhnout slibované výkonnosti a efektivity za pomoci snížení počtu administrativních úkonů.¹³¹

Mezi hlavní výhody zavedení je tedy možné zmínit následující:¹³²

- v důsledku omezení byrokracie dojde ke zvýšení komfortu fyzických i právnických osob při jednání s úřady – nebude již nutné předávat stejné údaje různým úřadům; úřady si budou moci samy obstarat některé doklady, které by jinak fyzické nebo právnické osoby musely předkládat,
- snížení administrativní náročnosti a rychlejší vyřizování žádostí bude mít pozitivní vliv na podnikatelské prostředí,

¹²⁹ Mates, a další, 2012, str. 90

¹³⁰ Mates, a další, 2012, str. 90

¹³¹ Česká republika. Důvodová zpráva k zákonu č. 111/2009 Sb., o základních registrech

¹³² Důvodová zpráva k zákonu č. 111/2009 Sb., o základních registrech.

- celkové zvýšení výkonnosti státní správy díky lepší výměně informací a výše zmíněného snížení počtu administrativních úkonů.

Další podkapitoly jsou věnovány nastínění funkce základních registrů a některých základních pojmů ze související zákonné úpravy a blíže pak rozlišení registrového systému se zaměřením na vybrané konkrétní databáze.

7.1 Základní registry

Zákon o základních registrech vznikl v roce 2009 a jedná se o veskrze českou právní úpravu, která se, až na některá obecná pravidla, unijního práva nedotýká.¹³³ O několik let později došlo v roce 2016 k jeho novelizaci, která nabyla účinnosti od počátku roku 2017. V následujících odstavcích budou některé změny porovnány s původním zněním před novelizací.

Předmětem úpravy řečeného zákona je vymezení obsahu základních registrů, jejich informačních systémů a informačních systémů územní identifikace. Stanovuje práva a povinnosti, které se týkají jejich vytváření, užívání a provozu. Zákon o základních registrech také zřizuje Správu základních registrů.

Základní registr. Základním registrem se rozumí informační systém veřejné správy, které se dále vymezují do čtyř oblastí dle § 3 zákona o základních registrech:

- základní registr obyvatel (registr obyvatel, ROB),
- základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob, ROS),
- základní registr územní identifikace, adres a nemovitostí (registr územní identifikace, RUIAN),
- základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností (registr práv a povinností, RPP).

Po poslední novelizaci byl zmiňovaný zákon doplněn o termín **soukromoprávní uživatel**. Dle definice je to podnikající fyzická nebo právnická osoba, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základního registru nebo z agendového informačního systému. Zatímco původní znění zákona

¹³³ Mates, a další, 2012

o základních registrech omezovalo práci s registry pro orgány veřejné správy, tato úprava rozšiřuje okruh subjektů, které mají k informacím z registrů přístup.

Agenda. Jedná se o ucelenou oblast činností, ve které působí orgány veřejné moci nebo soukromoprávní uživatelé údajů. Původní definici, kde agenda představovala „*souhrn činností spočívajících ve výkonu vymezeného okruhu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci*“, ¹³⁴ shledávali někteří odborníci poněkud problematickou např. v souvislosti s ochranou soukromí – přístup k určitým údajům měla ta která úřední osoba pouze v rámci výkonu příslušné agendy a jejího vymezeného informačního systému. ¹³⁵ Úřední osoby byly ve starém znění určené úřední osoby, které působí v jednotlivých rolích. ¹³⁶

Informační systém základních registrů. Prostřednictvím tohoto systému je zajišťováno sdílení dat navzájem mezi jednotlivými základními registry, základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem. V rámci tohoto informačního systému veřejné správy jsou také spravována oprávnění přístupu k datům a další činnosti dle zmíněného zákona. Je součástí referenčního, sdíleného a bezpečného rozhraní informačních systémů veřejné správy.

Soustava základních registrů spadá dle souvisejícího zákona pod Správu základních registrů, která je podřízena Ministerstvu vnitra. Zákon také stanovuje její práva a povinnosti.

7.2 Další registry státní správy

Předchozí kapitoly práce jsou věnovány nastínění ochrany osobních údajů a vnímání soukromí jako takového. Ze výše rozebraných odborných studií a esejí vyplývá, že u jednotlivců existuje tendence zabývat se zejména informacemi, které z dlouhodobého hlediska škodí jejich reputaci. Proto je vhodné zaměřit se na další registry veřejné správy, které jsou z tohoto pohledu zajímavé – insolvenční rejstřík, rejstřík trestů a evidence přestupků. Tyto registry (rejstříky, databáze) nejsou v gesci Správy základních registrů, ale jiných ústředních správních orgánů.

¹³⁴ Česká republika. 2017. *Porovnání dvou znění dokumentu č. 111/2009 Sb., znění platná od 1.7.2012 a od 1.6.2017. Změny zákonů*. [Online] 2017. [Citace: 30. 7. 2017].

<http://www.zmenyzakonu.cz/zakon.aspx?k=111/2009%20Sb.&d1=01072012&d2=01062017&cmd=compareshort>.

¹³⁵ Mates, a další, 2012

¹³⁶ Znění zákona o základních registrech, platnost od 1.7.2012, § 56, odst. 3.

7.2.1 Insolvenční rejstřík

Existenci insolvenčního rejstříku zakládá zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (dále jen „insolvenční zákon“). Předmětem úpravy zákona je řešení úpadku a hrozícího úpadku dlužníka některým ze zákonně stanovených způsobů za pomoci soudního řízení, a to tak, aby došlo k uspořádání majetkových vztahů a k co nejvyššímu uspokojení věřitelů. Insolvenční rejstřík je zde vymezen jako informační systém obsahující údaje dle insolvenčního zákona.

Samotnému rejstříku se věnuje Část čtvrtá zmíněného zákona, § 419–425. Jak bylo již řečeno, jedná se o jeden z informačních systémů veřejné správy, kde správcem je Ministerstvo spravedlnosti. Obsah insolvenčního rejstříku tvoří seznam insolvenčních správců, seznam dlužníků a insolvenční spisy, přičemž pro každého dlužníka je veden právě jeden spis. Je důležité zmínit, že tato databáze je veřejně přístupná¹³⁷; jednotlivé záznamy obsahují osobní data týkající se dlužníka (jméno, bydliště, rodné číslo, stav majetku), údaje o případném právním zástupci a v neposlední řadě výši dluhů a dotčené věřitele. Dle zveřejňovaných dokumentů tak lze také sledovat stav jednotlivých případů. Každý má právo do rejstříku nahlížet, pořizovat si kopie a výpisy.

Do insolvenčního rejstříku se zapisují fyzické osoby, fyzické osoby podnikající i právnické osoby. Pokud je dlužníkem fyzická osoba, záznam obsahuje následující údaje:¹³⁸

- jméno a příjmení,
- bydliště,
- rodné číslo, datum narození v případě, že fyzická osoba nemá rodné číslo.

U fyzické osoby, která je podnikatelem, jde o následující údaje:

- jméno a příjmení,
- bydliště,
- rodné číslo, datum narození v případě, že fyzická osoba nemá rodné číslo,
- dodatek odlišující firmu (používá-li jej),
- sídlo (pokud je odlišné od bydliště),

¹³⁷ S výjimkou údajů, o kterých tak insolvenční zákon stanoví. Insolvenční rejstřík lze navštívit např. na <https://isir.justice.cz/>, kde je možné dohledat dlužníky, proti kterým bylo zahájeno insolvenční řízení po 1. lednu 2008 a nebyli vyškrtnuti. K vyhledávání záznamů před tímto datem slouží předcházející Evidence úpadců (dostupná z http://upadci.justice.cz/cgi-bin/sqw1250.cgi/upkuk/s_i8.sqw).

¹³⁸ V případě, že má fyzická osoba podle zvláštního právního předpisu sídlo, запиše se do seznamu dlužníků i toto.

- identifikační číslo (IČO).

V případě, že je dlužníkem právnická osoba, do seznamu dlužníků je zapsáno:

- obchodní firma nebo název,
- sídlo,
- identifikační číslo (IČO).

Insolvenční soud do rejstříku chronologicky zveřejňuje¹³⁹

- rozhodnutí insolvenčního soudu,
- veškerá podání ohledně dlužníka, která se vkládají do soudního spisu vedeného insolvenčním soudem,
- další informace, o kterých tak stanoví insolvenční zákon nebo insolvenční soud.

Při vkládání výše zmíněných informací či písemností je vždy uveden okamžik vložení.

Insolvenční zákon dále v § 425 upravuje **vyškrtnutí** dlužníka ze seznamu dlužníků. Insolvenční soud vyškrtně dlužníka ze seznamu po uplynutí 5 let od okamžiku, kdy nabylo moci právní rozhodnutí (jedná se o situaci, kdy je úpadek vyřešen jedním ze zákonem stanovených způsobů – konkurs, oddlužení, reorganizace).¹⁴⁰ Údaje a další dokumenty v insolvenčním rejstříku jsou následně **znepřístupněny**. Insolvenční řízení může skončit na základě jiných rozhodnutí o insolvenčním návrhu dle § 142 – jeho odmítnutí pro vady či zjevnou bezdůvodnost, zastavení řízení pro nedostatky nebo zpětvzetí návrhu, zamítnutí insolvenčního návrhu. V takových případech má dlužník nárok požádat o vyškrtnutí po uplynutí 3 měsíců od právní moci rozhodnutí; soud provede vyškrtnutí dlužníka ze seznamu a znepřístupnění údajů v insolvenčním rejstříku do 15 dnů od doručení dlužníkovy žádosti.

Úlohou insolvenčního rejstříku je zajistit maximální míru publicity o insolvenčních řízeních a jejich průběhu. Kromě této informační funkce slouží rovněž k doručování¹⁴¹ soudních rozhodnutí a jiných písemností.

7.2.2 Trestní rejstřík

Na rozdíl od insolvenčního rejstříku, rejstřík trestů je upraven ve zvláštním zákoně č. 269/1994, Zákon o Rejstříku trestů (dále jen „zákon o Rejstříku trestů“). Další odlišností

¹³⁹ Insolvenční zákon, Část čtvrtá, Hlava I, § 421.

¹⁴⁰ Tyto způsoby jsou blíže vymezeny zákonem v Části druhé, Hlava I, II, V.

¹⁴¹ Doručování se děje prostřednictvím zveřejňování v insolvenčním rejstříku na základě § 71 insolvenčního zákona.

od předchozího rejstříku je jeho zákonné vymezení – dle souvisejícího zákona se Rejstříkem trestů rozumí organizační složka státu, která spadá pod Ministerstvo spravedlnosti a v jejímž čele stojí ředitel. Jedná se tedy o úřad, obecně se jím ale rozumí evidence. Zákon o rejstříku trestů také upravuje případy, kdy se věc týká cizinců a vztahy s legislativou Evropské unie. Cílem následujících odstavců je tento kratší (zákon má rozsah 18 paragrafů), nicméně obsahově bohatý zákon, náležitě nastínit.

Hlavním úkolem Rejstříku trestů je vedení evidence fyzických a právnických osob, jež byly pravomocně odsouzeny v trestních řízeních a dále evidenci jiných významných skutečností pro trestní řízení, stanoví-li tak zmíněný či jiný zákon. Údaje z evidence slouží pro potřebu trestního, občanskoprávního nebo správního řízení a také k prokazování bezúhonnosti. Rejstřík trestů je pro účely přístupu do informačních systémů veřejné správy považován za orgán, který se spolupodílí na vyšetřování, odhalování a stíhání trestných činů.¹⁴²

Pro výkon své působnosti využívá Rejstřík trestů údaje ze základního registru obyvatel a z dalších informačních systémů veřejné správy (registr rodných čísel, informační systém evidence obyvatel, informační systém evidence občanských průkazů, informační systém evidence cestovních dokladů, informační systém cizinců).

Základní registr obyvatel poskytne Rejstříku trestů následující údaje:¹⁴³

- jméno (popř. jména) a příjmení,
- adresa místa pobytu,
- datum, místo a okres narození (u fyzické osoby, která se narodila v cizině, datum, místo a stát narození),
- datum, místo a okres úmrtí (pokud jde o úmrtí mimo území České republiky, poskytuje se datum úmrtí, místo a stát, na jehož území k úmrtí došlo),
- státní občanství (popř. více státních občanství).

Trestní rejstřík využívá také informační systém evidence obyvatel, jenž poskytuje ještě podrobnější informace o státních občanech České republiky a bývalých státních občanech, kteří občanství pozbyli. Výčet těchto údajů stanovuje § 2a zákona o Trestním rejstříku a jedná se například o údaje o svéprávnosti, rodinném stavu, registrovaném

¹⁴² Insolvenční zákon, § 2.

¹⁴³ Insolvenční zákon, § 2a.

partnerství aj. Tento informační systém je upraven zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel).

Z registru rodných čísel se pro výkon působnosti získává:¹⁴⁴

- jméno (popř. jména), příjmení, rodné příjmení,
- rodné číslo (v případě změny rodného čísla původní rodné číslo),
- den, měsíc a rok narození,
- místo a okres narození (u fyzické osoby, která se narodila v cizině, stát narození).

Další údaje získává, jak bylo již dříve zmíněné, z evidence občanských průkazů a cestovních dokladů – jedná se např. o čísla dokladů, jejich data vydání a doba platnosti nebo označení úřadu, kde byl konkrétní doklad vydán. Co se týká cizinců, jsou požadované informace ještě podrobnější.

Údaje o osobách, které byly pravomocně odsouzeny, se **uchovávají** 100 let od

- narození fyzické osoby, které se týkají,
- pravomocného odsouzení právnické osoby, které se týkají,
- právní moci jiné skutečnosti významné pro trestní řízení evidované podle § 2 odst. 1, která se týká právnické osoby.

Evidence Rejstříku trestů čítá 5 evidencí stanovených v § 2b:

- odsouzení – zde je vhodné zmínit obsah této evidence; obsahuje údaje z trestních listů, kde trestní list je oznámení soudu, který obsahuje zevrubné údaje o pravomocně odsouzeném subjektu (např. vyloučení zaměnitelnosti osob, spisové značky, rozhodnutí o vině, trestu, ochranném opatření a jejich výkonu, udělení milosti, **zahlázení** odsouzení aj.)
- podmíněného zastavení trestního stíhání,
- podmíněného odložení návrhu na potrestání,
- narovnání,
- odstoupení od trestního stíhání.

Rejstřík trestů ze své evidence vydává opisy a výpisy.¹⁴⁵ V **opisu** jsou uváděny veškeré údaje týkající se odsouzení, výkonu trestů a opatření atd. Opis taktéž obsahuje údaje

¹⁴⁴ Insolvenční zákon, § 2a.

¹⁴⁵ trestni-rizeni.com. 2006-2017. *Rejstřík trestů*. trestni-rizeni.com. [Online] 2006-2017. [Citace: 10. 8. 2017]. <http://www.trestni-rizeni.com/vyklad-pojmu/rejstrik-trestu>.

o zhlazení odsouzení fyzické osoby či o zániku účinků odsouzení osoby právnické. Dokument se vydává pro potřeby trestního řízení pouze orgánům v něm činným a Ministerstvu spravedlnosti na jejich žádost. Jiné orgány a osoby mají nárok na vydání opisu pouze v případě, že tak stanoví zvláštní právní předpis.¹⁴⁶ Osoba, které se vydávaný opis týká, má po ověření totožnosti právo do něj nahlédnout.¹⁴⁷

Výpis je možné vydat na písemnou žádost fyzické osoby, jejíž totožnost byla ověřena. Dokument je však možné dostat na počkání – žádost lze provést na kontaktních místech veřejné správy. Dalším způsobem, jak o výpis zažádat, je prostřednictvím portálu veřejné správy za pomoci datové zprávy.¹⁴⁸ Lze jej vydat také na základě úředně ověřené plné moci i zmocnění dané osoby. Výpis, který se týká právnické osoby, je vydán na písemnou žádost kterékoliv osoby. Žádosti o výpis jsou uchovávány¹⁴⁹ po dobu 2 let od jejich podání. Ve výpisu jsou uváděny údaje o pravomocných odsouzeních, která nebyla zhlazena.¹⁵⁰

Dříve zmiňované **zhlazení** je definováno v zákoně č. 40/2009 Sb., trestním zákoníku, v § 105. Jde o právo odsouzených, kteří vedou spořádaný život po výkonu nebo prominutí trestu anebo po promlčení jeho výkonu. V praxi zhlazení znamená, že se na dotyčného nebude hledět jako na odsouzeného – zhlazené odsouzení se, jak bylo psáno výše, neuvádí do výpisu z trestního rejstříku. K zhlazení dochází na žádost odsouzeného, a po uplynutí určité doby dle typu trestu, ke kterému byla osoba odsouzena:¹⁵¹

- odsouzení k výjimečnému trestu – zhlazení po 15 letech,
- odsouzení k trestu odnětí svobody převyšujícímu pět let – zhlazení po 10 letech,
- odsouzení k trestu odnětí svobody převyšujícímu jeden rok – zhlazení po 5 letech,
- odsouzení k trestu odnětí svobody nepřevyšujícímu jeden rok nebo k trestu vyhoštění – zhlazení po 3 letech,
- odsouzení k trestu domácího vězení, k trestu propadnutí majetku, k trestu propadnutí věci, k trestu zákazu pobytu, k trestu zákazu vstupu na sportovní,

¹⁴⁶ Česká republika. Zákon č. 269/1994 Sb., o Rejstříku trestů.

¹⁴⁷ Redakce ePravo.cz. 2001. *Opis a výpis z Rejstříku trestů*. EPRAVO.CZ. [Online] 23. říjen 2001. [Citace: 10. 8. 2017]. <https://www.epravo.cz/top/clanky/opis-a-vypis-z-rejstriku-trestu-15264.html>.

¹⁴⁸ Czech POINT.

¹⁴⁹ V listinné nebo elektronické podobě anebo po provedení autorizované konverze.

¹⁵⁰ trestni-rizeni.com, 2006-2017

¹⁵¹ Zákon o trestním rejstříku.

kulturní a jiné společenské akce nebo k peněžitému trestu za úmyslný trestný čin – zahlazení po 1 roce.

Trestní rejstřík fyzických osob není veřejně přístupný.¹⁵²

7.2.3 Evidence přestupků

Rejstřík trestů vede také celostátní centrální evidenci přestupků¹⁵³, která byla zřízena od 1. října 2016 a je samostatná.¹⁵⁴ Tato evidence má pomoci oprávněným institucím a správním orgánům lépe sdílet informace o pachatelích závažnějších přestupků a také díky tomu efektivněji postihovat recidivu.¹⁵⁵

Mimo zevrubnou identifikaci přestupku a jeho náležitostí obsahuje zmíněná evidence následující údaje:¹⁵⁶

- jméno (popř. jména), příjmení, rodné příjmení, nebo název pachatele,
- místo a okres narození, nebo jeho sídlo; u pachatele přestupku, který se narodil v cizině, místo a stát, kde se narodil,
- rodné číslo nebo datum narození pachatele přestupku, anebo identifikační číslo osoby, bylo-li jí přiděleno,
- státní občanství.

Oproti rejstříku trestů evidence přestupků nenabízí možnost získat výpis.¹⁵⁷ Je možné získat **opis**, který se na žádost vydává následujícím entitám:

- oprávněnému správnímu orgánu,
- orgánu činnému v trestním řízení,
- národnímu členovi Eurojustu pro účely plnění úkolů v Eurojustu,
- soudu pro účely soudního řízení,
- státnímu zastupitelství pro účely jiného než trestního řízení,
- Ministerstvu spravedlnosti,
- Kanceláři prezidenta republiky.

¹⁵² Je ale přístupná evidence odsouzených právnických osob (dle zákona o rejstříku trestů, § 13, odst. 4), kde lze nalézt podrobnosti o firmě, rozsudku, vlastnosti trestného činu a délky trestu.

¹⁵³ Předmětem evidence budou dle zákona o přestupcích pravomocná rozhodnutí o těchto přestupcích: ochrany před alkoholismem a jinými toxikomaniemi; úsek zemědělství a myslivosti; úsek obrany České republiky; proti veřejnému pořádku; proti občanskému soužití; proti majetku.

¹⁵⁴ Nevrkla, Luboš. 2015. *Centrální evidence přestupků*. EPRAVO.CZ. [Online] 10. listopad 2015. [Citace: 10. 8. 2017]. <https://www.epravo.cz/top/clanky/centralni-evidence-prestupku-99548.html>.

¹⁵⁵ justice.cz. 2016. *Nově spuštěná centrální evidence přestupků je plně funkční*. Bulletin advokacie. [Online] 5. říjen 2016. [Citace: 20. 8. 2017]. <http://www.bulletin-advokacie.cz/nove-spustena-centralni-evidence-prestupku-je-plne-funkcni>.

¹⁵⁶ Zákon o Rejstříku trestů, Část třetí, § 16i

¹⁵⁷ Tato skutečnost však koliduje s právem na podání stížnosti na nesprávnost údajů.

Data, která evidence přestupků obsahuje, se dle zákona o Rejstříku trestů **vyřazují** po 5 letech od vydání pravomocného rozhodnutí. Ustanovení § 16k zakládá, že tyto vyřazené údaje se dále **uchovávají** v úschovně dokumentace po dobu 10 let od okamžiku uložení. Nárok na přístup k takto uchovávaným dokumentům má osoba, již se týkají, soud a Ministerstvo spravedlnosti za zákonem určených podmínek.

7.2.4 Směrnice Evropského parlamentu a Rady EU 2016/680

Ve vztahu k výše zmíněným rejstříkům je vhodné také zmínit další evropskou směrnici, a to o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.¹⁵⁸ Jak již název napovídá, jedná se o trestněprávní směrnici, která se týká ochrany osobních údajů v oblasti justiční a policejní spolupráce. V platnost vstoupil dokument koncem dubna roku 2016. Dokument vznikl proto, že se stávající Směrnice 95/46/EU nevztahovala na zpracování osobních dat prováděné pro výkon činností, které právě s takovou spoluprací souvisí.¹⁵⁹ Nařízení 2016/679 se použije v případě, že orgány veřejné moci zpracovávají osobní údaje pro jiné účely než pro účely této směrnice.¹⁶⁰ Strukturou a částečně i obsahem je směrnice velmi podobná novému nařízení, které bylo rozebráno v přechodných částech práce; následující odstavce představí pouze některé její stěžejní části. Členské státy Evropské unie přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí do 6. května 2018.

Preambule směrnice obsahuje 107 bodů a další struktura kapitol je následující:¹⁶¹

- I. Obecná ustanovení (čl. 1-3)
- II. Zásady (čl. 4-11)
- III. Práva subjektu údajů (čl. 12-18)
- IV. Správce a zpracovatel (čl. 19-34)
- V. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (čl. 35-40)
- VI. Nezávislé dozorové úřady (čl. 41-49)
- VII. Spolupráce (čl. 50, 51)

¹⁵⁸ Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech.

¹⁵⁹ Evropská unie. Směrnice Evropského parlamentu a Rady EU 2016/680, článek 5.

¹⁶⁰ Směrnice Evropského parlamentu a Rady EU 2016/680, článek 11.

¹⁶¹ Lze porovnat se strukturou nařízení v kapitole 3.

- VIII. Právní ochrana, odpovědnost a sankce (čl. 52-57)
- IX. Prováděcí akty (čl. 58)
- X. Závěrečná ustanovení (čl. 59-65)

Dle prvního článku směrnice stanoví pravidla, která se týkají ochrany fyzických osob v souvislosti se zpracováním 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.

Ve směrnici 2016/680 dochází k definování základních pojmů, totožnému s těmi, se kterými pracuje nařízení 2016/679 – jde o například definice osobních údajů, zpracování, správce, zpracovatele, profilování a pseudonymizace. Zásady zpracování se rovněž shodují.

V pátém článku směrnice je stanoveno, že členské státy určí přiměřené lhůty pro **výmaz** osobních údajů nebo pro pravidelný přezkum potřeby uložení osobních údajů.

Jedním z práv subjektů osobních údajů je právo přístupu k nim a také právo na informaci o **předpokládané době**, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby. Subjekt údajů také může správce požádat o opravu nebo **výmaz** dat. V případě výmazu dat je po správci požadováno, aby tak učinil bez zbytečného odkladu¹⁶² – děje se tak v situaci, kdy jsou porušeny zásady zpracování, zákonnost zpracování, při porušení podmínek při zpracování zvláštních kategorií osobních údajů nebo pokud údaje musí být vymazány ke splnění právní povinnosti správce.¹⁶³ Pokud existuje potřeba uchování údajů pro účely dokazování, jejich zpracování je ze strany správce omezeno a k výmazu nedochází.

8 Diskuze a doporučení

8.1 Komparativní analýza

Následující tabulka obsahuje přehled zkoumaných institutů, konkrétně tedy insolvenční rejstřík, trestní rejstřík a evidenci přestupků. Z hlediska ochrany osobních údajů a tématu práce je vhodné se zaměřit na reálně shromažďované údaje, jejich uchovávání a jejich likvidaci. Druhá tabulka potom zobrazuje související aspekty nových komunitárních předpisů.

¹⁶² Směrnice Evropského parlamentu a Rady EU 2016/680, článek 14.

¹⁶³ Směrnice Evropského parlamentu a Rady EU 2016/680, články 4, 8, 10, 16.

Tabulka 1 - Srovnání některých aspektů vybraných rejstříků

	Insolvenční rejstřík	Trestní rejstřík	Centrální evropské přeshraniční
Právní úprava	upraven v zákoně č. 182/2006 Sb., insolvenční zákon	zákon č. 269/1994 Sb., Trestní rejstřík	upravena v zákoně č. 269/1994 Sb., Trestní rejstřík (některé podmínosti v § 106 a 107 zákona č. 250/2016 Sb., o odpovědnosti za přešlupky a řízení o nich)
Zapisované údaje FO	jméno a příjmení; bydliště; rodné číslo / datum narození	ROB: jméno (popř. jména) a příjmení; adresa místa pobytu; datum, místo a okres narození (u fyzické osoby, která se narodila v cizině, datum, místo a stát narození); datum, místo a okres úmrtí; státní občanství; RRC: jméno (popř. jména), příjmení, rodné příjmení; rodné číslo (v případě zněny rodného čísla původní rodné číslo); den, měsíc a rok narození; místo a okres narození (u fyzické osoby, která se narodila v cizině, stát narození); dále evidence občanských průkazů a cestovních dokladů	jméno (popř. jména), příjmení, rodné příjmení, nebo název pachatele; místo a okres narození, nebo jeho sídlo; rodné číslo nebo datum narození (identifikační číslo osoby; bylo-li jí přiděleno); státní občanství
Zapisované údaje podnikatel FO	jméno a příjmení; bydliště; rodné číslo / datum narození; dodatek odlišující firmu; sídlo; identifikační číslo (IČO)	-	-
Zapisované údaje PO	obchodní firma nebo název; sídlo; identifikační číslo (IČO)	-	-
Likvidace	vyškrtnutí ze seznamu dlužníků a zneprůstřednění údajů v rejstříku po 5 letech od nabýání právní moci rozhodnutí	možnost zaházení odsouzení (de případů od 1 roku do 15 let po pravomocném odsouzení) - trestný čin se neuvádí ve výpisu, ale zůstává v opisu	vyřazení z evidence po 5 letech od pravomocného rozhodnutí
	v případě rozhodnutí de § 142 InsZ - dlužník má nárok požádat o vyškrtnutí po 3 měsících od právní moci rozhodnutí; soud vyškrtnutí ze seznamu a zneprůstřednění údaje v rejstříku do 15 dní od doručení žádosti		
Uchovávaní	-	v úřední dokumentace u pravomocně odsouzených - 100 let (od narození PO, pravomocného odsouzení PO)	v úřední dokumentace: 10 let (od úmrtí)
Další	veřejně přístupný (online); přílohy spisů dlužníků obsahují dále informace o stavu majetku, pracovní smlouvy, výkonné pásky, různá vyřazení právního zápisu aj.	využívá základní a další registry a informační systémy VS	-

Zdroj: Insolvenční zákon, Zákon o trestním rejstříku, Nařízení EU 2016/679, Směrnice EU 2016/680, vlastní zpracování

Tabulka 2 - Vybrané aspekty unijních právních úprav

	Nařízení EU 2016/679 (GDPR)	Směrnice EU 2016/680
Právní úprava	nařízení; přímá účinnost od 25.5.2018	směrnice; soulad předpisů do 6.5.2018
Zapísované údaje FO	definice osobních údajů: veškeré informace o identifikované nebo identifikovatelné fyzické osobě	definice osobních údajů: veškeré informace o identifikované nebo identifikovatelné fyzické osobě
Zapísované údaje podnikající FO	-	-
Zapísované údaje PO	<i>nevztahuje se</i>	<i>nevztahuje se</i>
Likvidace	možnost odvolání souhlasu se zpracováním; "právo na zapomnění" - úplný výmaz, podmínky stanoví článek 17	neodkladný výmaz při porušení směrnici uvedených podmínek
Uchovávání	uložení údajů ve formě umožňující identifikaci subjektu údajů pouze po dobu nezbytně nutnou pro naplnění účelu jejich zpracování	členské státy určí přiměřené lhůty pro výmaz osobních údajů nebo pro pravidelný přezkum potřeby jejich uložení

Zdroj: Nařízení 2016/679, Směrnice 2016/680, vlastní zpracování

Tabulka 1 ilustruje, které údaje fyzických osob jsou shromažďovány pro účely záznamů do obou rejstříků a evidence. Trestní rejstřík pracuje s větším objemem dat než zbylé dvě databáze, nicméně insolvenční rejstřík může ve výsledku obsahovat více údajů citlivějšího charakteru, a to vzhledem k publikované dokumentaci a faktu, že je veřejně přístupný. Pro všechny registry je společné, že obsahují také podrobný popis podstaty případu.

Tabulka 2 znázorňuje, jak se k vybraným oblastem vztahuje nové nařízení a nová směrnice. Údaje zapisované do databází lze dle definic kvalifikovat jako údaje osobní. Oba unijní předpisy zmiňují možnost a podmínky likvidace a výmazu, nařízení potom přímo rozeznává právo být zapomenut.

8.2 Diskuze

Insolvenční rejstřík je veřejně přístupný na internetu. V tomto rejstříku je možné vyhledávat dle zadaných kritérií, jimiž jsou standardní údaje jako jméno a příjmení, popř. název, IČO, rodné číslo, datum narození, možné je také vyhledávání pomocí spisové značky, dále pak lze filtrovat záznamy podle stavu řízení. Po vyhledání je možné zobrazit detail lustrovaného subjektu, který obsahuje související dokumenty řízení – lze se tak dostat k dokumentaci celého průběhu řízení, která zahrnuje insolvenční návrhy, seznam věřitelů a dlužných částek, soupisy majetkové podstaty dlužníka, pracovní smlouvy, výplatní pásky aj. Všechny tyto dokumenty jsou dostupné v elektronické podobě, je tedy možné je stahovat, ukládat a jinak využívat. Z těchto zveřejněných souborů je možné o fyzické osobě zjistit velké množství informací za zlomek času. Všechna uvedená data lze kvalifikovat jako data, která umožňují přímou či nepřímou identifikaci fyzické osoby. Jedním z úkolů insolvenčního rejstříku je již zmiňované zajištění vysoké míry publicity o probíhajících (ale také již pravomocně ukončených) řízeních, přesná identifikace dlužníků vychází již z podstaty tohoto institutu. Na jednu stranu se jedná o informace, které jsou veřejně prospěšné a mimo jiné mohou mít také preventivní účinky. Na straně druhé stojí skutečnost zvýšeného rizika zneužití daných informací a dokumentů, a to za pomoci dnes běžně dostupných technologií. Dále lze také hovořit o jistém společenském stigma, jímž mohou dlužníci následně trpět.

Z insolvenčního zákona, resp. z jeho části o insolvenčním rejstříku, vyplývá, že po uplynutí 5 let od pravomocného rozhodnutí může dojít k vyškrtnutí a znepřístupnění shromážděných údajů v rejstříku. Stát se tak ovšem musí na základě žádosti dlužníka, nikoliv automaticky. Ve vztahu k ochraně osobních údajů se mi zdá poněkud nevhodné, že jsou tyto údaje dostupné na internetu v poměrně velkém rozsahu po relativně dlouhou dobu; na internetu, který je dnes dostupný téměř kdykoliv a kdekoliv, a s existencí zařízení, která jsou schopna mnohé informace ihned ukládat nebo šířit (a ne vždy ve veřejném zájmu). V zákoně není explicitně zmíněno, zda se jedná o výmaz, a kde se dříve veřejně přístupná dokumentace dlužníků posléze uchovává. Jedna ze zásad, společná pro nové nařízení, novou směrnici i stávající zákon pro ochranu osobních údajů, je ta, že údaje nesmí být zachovány ve formě umožňující identifikaci po dobu delší, než je nezbytně nutné k naplnění původního účelu, za nímž byly shromážděny. Směrnice také říká, že členské státy určí přiměřené časové lhůty pro výmaz osobních údajů nebo pravidelný přezkum potřeby jejich uložení.

Výše zmíněná fakta dávají vzniknout několika otázkám:

- Co se s údaji reálně děje po vyškrtnutí?
- Je nutné, aby byla data v určitých případech odstraňována po uplynutí stanovené doby na žádost dotčené osoby nebo automaticky?
- Jaká je přiměřená časová lhůta než dojde k odstranění shromážděných osobních údajů?
- V jakém rozsahu by měly být zveřejněny údaje o dlužnících?

Platí, že neznalost zákona neomlouvá, takže nelze „vinit“ státní sektor, pokud dlužník zapomene o vyškrtnutí a znepřístupnění požádat, nicméně lze tvrdit, že po vyřešení případu a pravomocném rozhodnutí svým způsobem začíná pomíjet účel, za kterým byly informace o dlužníkovi shromážděny. I z tohoto důvodu by se hodilo uvažovat nad automatickým odstraněním předmětných insolvenčních spisů z veřejně přístupné databáze. S účelem souvisí také časová lhůta, která je aktuálně vymezená 5 lety. Časové náklady na získání informací se v posledních letech výrazně zredukovaly; pokud jde o publicitu insolvenčních řízení, která by měla působit jako prevence navazování některých (smluvních) vztahů se zadluženou osobou, vnímám 5 let jako dlouhou dobu. Tempo šíření informací je nyní mnohonásobně vyšší a možnosti přístupu k těmto informacím jsou téměř neomezené, proto se domnívám, že je možné diskutovat nad snížením této pětileté hranice. Také si myslím, že v podstatě pomíjí důvod udržovat některá data „při životě“ na veřejném portálu z hlediska veřejného zájmu v delším časovém horizontu. Snížení časové hranice by rovněž mohlo mít pozitivní vliv ze společenského hlediska a z hlediska rehabilitace, kdy je kladen velký důraz na reputaci a v neposlední řadě i soukromí. Je ale potřeba neopomínat, že v některých případech je důležité insolvenční minulost občana znát, a proto by informace o bývalých dlužnících měly být po určitý čas dostupné na opodstatněné vyžádání. Za jakých podmínek by ale taková žádost byla opodstatněná? Dle mého názoru dochází v současné době často například k uzavírání předmanželských smluv; ačkoliv se toto zdá jakkoliv neosobní a nevhodné, jistě se lze domnívat, že právě v podobných případech by jedna nebo obě strany mohly podobnou lustraci vyžadovat. Dále by se zřejmě mohlo jednat o případy, kdy se jednotlivec uchází o zaměstnání v některých odvětvích veřejného sektoru. Myslím si, že v odvětvích (ať už ve veřejném nebo soukromém sektoru), kde dochází k přímé manipulaci s finančními prostředky, se nejvíce jako vhodné prostředí pro „notorické“ dlužníky. Dále se může jednat o případy, kdy vstupujeme do nějakých obchodních

vztahů, např. žádosti o úvěr, výběr dodavatele, volba zaměstnavatele (který není všeobecně známý, jako např. zavedená banka). Ve všech případech ale považuji za nutné posuzovat dle kontextu a dalších faktorů; věřím, že u mnoha případů insolvence se mohlo jednat o „mladické“ nerozvážnosti či kombinaci jiných nešťastných životních situací.

Po uplynutí stanovené doby by pak mělo dojít k likvidaci insolvenčních spisů, s přihlédnutím k „dobrému chování“ nebo v opačném případě k obnovení spisu a prodloužení jeho uložení s přihlédnutím k recidivě (bývalého) dlužníka.

Na tuto oblast práva se tedy nové nařízení primárně nevztahuje, nicméně by jeho aplikace byla možná ve chvíli, kdy by například po provedeném vyškrtnutí a znepřístupnění došlo později k publikaci (např. v médiích) dat dříve stažených z insolvenčního rejstříku. Podobný případ byl nastíněn v kapitole 5 (Google vs. Mario Costeja González). I v těchto případech se lze domnívat, že by nedošlo k úplnému odstranění ze zdroje (kterým by byl státní sektor, jenž jednal ze zákonné povinnosti). Společnost počítá se zajištěním vysoké úrovně ochrany ze strany státního sektoru, kterou vyžaduje také unijní právní rámec. Nové nařízení zmiňuje pseudonymizace osobních údajů, která se jeví jako vhodným řešením, co se právě může týkat ukládání osobních dat, jež byly shromážděny veřejnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Zákonné úpravy podobných evidencí, zde konkrétně insolvenční rejstřík a související insolvenční zákon, by tedy měly projít revizí a být doplněny o specifikaci a podmínky *ex post* nakládání s těmito údaji.

Zákon o Trestním rejstříku definuje právo na **zahlázení** trestného činu, které se dá považovat za určitou formu práva být zapomenut – po uplynutí zákonně stanovené doby a v případě, že odsouzený vede spořádaný život, dochází k zahlázení, které v praxi znamená, že trestný čin, jehož se fyzická osoba dopustila, není uváděn ve výpisu z rejstříku trestů, který je běžně požadován při nástupu do zaměstnání. Trestný čin však nadále zůstává v opisu rejstříku trestů, ke kterému má přístup Ministerstvo spravedlnosti a orgány činné v tomto trestním řízení. Do rejstříku trestů není možné nahlížet způsobem, jako do insolvenčního rejstříku, nicméně „popularita“ trestných činů fyzických osob je mnohem vyšší a pozornost médií je v této oblasti koncentrovanější. Neznaменá to však, že by měla být insolvence přímo porovnávána s trestným činem. Myslím si, že některé trestné činy nejsou hodny zapomnění, zároveň je ale vždy potřeba vše zasadit do kontextu, uvažovat všechna fakta a posuzovat případy individuálně. Co se týká právní úpravy,

trestní rejstřík je zastřešen samostatným zákonem. Jak bylo uvedeno v předchozích kapitolách, jedná se vlastně o úřad, jenž vede evidenci trestných činů a jiné evidence. Dle mého názoru lze tuto právní úpravu lze považovat za dostačující; institut zahlazení vhodně zastupuje jistým dílem právo odsouzeného být zapomenut například ve vztahu k potenciálnímu zaměstnavateli, časové lhůty lze také posuzovat jako přiměřené. Co se veřejnosti týče, lze předpokládat, že do jejího povědomí vstoupí zejména trestné činy takového charakteru, za něž je udělován výjimečný trest nebo pokud si jiným způsobem vyslouží pozornost médií. V některých z těchto případů si viníci zřejmě ani nezaslouží něco jako právo být zapomenut, ale to je již spíše otázka morální.

Spisy odsouzených se uchovávají v úschovně po dobu 100 let od pravomocného rozhodnutí. Zákon explicitně nezmiňuje, podobně jako insolvenční zákon, co se se záznamy děje po uplynutí této doby. V případě fyzických dokumentů by skartace nebo spálení mohlo být dostatečně definitivním odstraněním, ale pouze za předpokladu, že by neexistovaly další fyzické nebo elektronické kopie. Zákonem stanovená doba se mi zdá relativně dlouhá. Jako moment, kdy pomine účel uchovávání předmětných záznamů, vnímám smrt odsouzeného, jehož se týkají. Další uchovávání by mohlo být v některých případech zajímavé z hlediska dějin, psychologie či jiných vědeckých disciplín.

Evidence přestupků je relativně mladou databází. Hlavním přínosem je možnost zjištění, zda se pachatel dopouští přestupků opakovaně a lépe tak postihovat recidivu.¹⁶⁴ Ačkoliv je od rejstříku trestů odlišná, považovala bych i v případě přestupkové evidence možnost pořízení výpisu. Výpis by se rovněž vydával řádně prokázaným osobám, jichž se dokumentace týká, a na jeho základě by mimo jiné docházelo právě ke kontrole správnosti uvedených údajů. Zákon o Trestním rejstříku dále hovoří o vyřazení z evidence po 5 letech od nabytí právní moci rozhodnutí a podobně jako u trestního rejstříku jsou záznamy dále uchovávány v úschovně dokumentace; odlišná je časová lhůta, která je stanovena na 10 let od chvíle, kdy k uložení dané dokumentace dojde. Evidence přestupků nedisponuje žádným právem, které by bylo podobné právu na zahlazení, jako tomu je u trestního rejstříku. Rovněž se související právní předpis nezmiňuje o výmazu jako takovém, který by mohl být po uplynutí doby úschovy očekáván. Společně s dalšími zmíněnými rejstříky tak tyto databáze představují jakýsi souhrnný a citlivý „balíček“ přečinů.

¹⁶⁴ Před zavedením evidence přestupků se na opakované případy přišlo pouze tehdy, pokud byly řešeny stejnou přestupkovou komisí. - Advokátní kancelář Paroulek & spol. 2006. *Vzniká nová centrální evidence přestupků*. Advokátní kancelář Paroulek & spol. [Online] 14. říjen 2006. [Citace: 24. 8. 2017.] <http://ak-pr.cz/cs/vznika-nova-centralni-evidence-prestupku/>.

Za jedno z velkých úskalí práva na výmaz, neboli práva být zapomenut, lze považovat právě nárok na jeho aplikaci – v dnešní době je prakticky nemožné něco trvale vymazat, odstranit, zvláště jedná-li se o data, která byla jednou, byť třeba jen na chvíli, zveřejněna v elektronické podobě na internetu. Téměř každý má možnosti přístupu k síti, ke mnoha typům úložišť a takřka neomezenému stahování a ukládání různých informací. To, že se informace odstraní z jedné webové stránky, byť i na základě pravomocného soudního rozhodnutí, neznamená, že u některých uživatelů neexistuje kopie inkriminovaného záznamu, print screen, fotografie, kterou již někdo stihnul zveřejnit na některé z mnoha sociálních sítí.

Lze se domnívat, že ochrana osobních údajů bude velmi často řešena jako občan vs. občan, občan vs. média (tisk, televize, internet aj.), právo na soukromí a ochranu osobních údajů vs. právo na svobodný přístup k informacím a právo na svobodu tisku. Studie, které byly zmíněny v kapitole 4, ilustrovaly právě takové případy – jedním z následků dožadování se práva na soukromí (resp. práva být zapomenut) byla paradoxně ještě větší publicita a vznik precedentů.

8.3 Doporučení

V současné době tedy lze sledovat existenci dvou legislativních dokumentů, které se dotknou českého právního prostoru – Nařízení Evropského parlamentu a Rady EU 2016/679 (přímo účinné) a Směrnice Evropského parlamentu a Rady EU 2016/680 (nutná transpozice). Ačkoliv byl mimo jiné jedním ze záměrů nového nařízení alespoň částečně snížit administrativní zátěž pro hospodářské subjekty, některé modifikace zjevně mohou znamenat opak. Jedná se zejména o nové povinnosti správců údajů: posuzování dopadu na ochranu osobních údajů, žádosti o konzultace s dozorovým orgánem, vedení dokumentace o zpracování, jmenování inspektora, oznamování v případě narušení bezpečnosti. Zmíněné novinky bude nutné zpracovat do obecné právní úpravy, kterou je zákon o ochraně osobních údajů. Domnívám se, že v tomto ohledu by byla dostačující novelizace zmíněného zákona; dosavadní podoba dle mého názoru splňuje přísné požadavky ochrany osobních údajů, které evropského nařízení klade, také se příliš neliší v základních definicích. Institut pověřence pro ochranu osobních údajů považuji za vhodně zvolený prostředek, jak dosahovat efektivní ochrany osobních dat, zvláště za předpokladu jmenování stávajícího zaměstnance společnosti, který je seznámen s jejími procesy a chodem. V tomto ohledu ovšem považuji za problematický požadavek na odbornost, již pověřenec musí disponovat. Další bod, který by měl být v zákonných

úpravách blíže specifikován, je likvidace údajů po uplynutí stanovené časové lhůty. S tím souvisí také to, v jaké podobě je dokumentace uchovávána (fyzicky, elektronicky) a za jakých bezpečnostních podmínek. Okolnosti likvidace a její vymezení považuji za zásadní, aby bylo možné řádně „uchopit“ právo být zapomenut.

S nástupem nové legislativy lze předpokládat významné rozšíření obsahu předpisů. Z legislativního hlediska tedy považuji za vhodné revidovat dosavadní právní předpisy (zde insolvenční zákon a zákon o rejstříku trestů, popř. i trestní řád) ve vztahu k nové komunitární směrnici 2016/680, což vyústí buďto v novelizace nebo vznik nových, zvláštních právních úprav. Protože se jedná o registry veřejné správy, domnívám se, že z důvodu přehlednosti a komplexnosti by bylo přínosné vyčlenit právě zvláštní zákony pro jednotlivé databáze, které by byly snadno dohledatelné; webové stránky správy registrů by na ně mohly rovněž snáze odkazovat.

Uchovávání informací a jiných dat není dle mého názoru prakticky možné absolutně sledovat; myslím si, že v nejbližší době nebude technologicky možné kontrolovat, kdo a jakým způsobem data reprodukuje do vlastního úložiště a jak dlouhou dobu je bude schraňovat. V tomto ohledu se jako jedno z přijatelných řešení jeví technologie zajišťující autodestrukci dat po uplynutí určité doby, jež zmiňovala studie *Right to Be Forgotten in the Internet Era* v kapitole 4.2. Nicméně stále zůstává problémem široká škála možností, jak data kopírovat, a tedy globální fungující použití této technologie.

V současné pokrokové době, a možná i v budoucnu, bude legislativa vždy zaostávat za technologickým rozvojem a novými možnostmi, který tento rozvoj nabízí. Aktuálně není možné, aby je právo předcházelo. Lze předpokládat, že z hlediska kybernetické bezpečnosti a zajištění správného fungování institutu práva být zapomenut (a práva na ochranu osobních údajů vůbec) bude nutné zaměřit se hlavně na takové technologie, které budou disponovat „schopnostmi“, aby bylo možné zmíněnému právu dostát. Právo být zapomenut se zatím spíše jeví jako ne příliš vhodně zvolený *terminus technicus*.

Závěr

S rostoucím tempem technologického pokroku dochází také k nevyhnutelné přeměně společnosti, na který se nutně musí adaptovat také systém právních regulací. Cena za zjednodušení některých procesů v běžném životě je mnohdy vyšší, než si uvědomujeme, a hlavním oběživem se stalo něco ne přímo hmatatelného – osobní údaje. Je možné zaznamenat jasný paradox soukromí, kdy mnohdy opakovaně umožňujeme druhým stranám zpracovávat stále větší množství osobních dat, jejichž vyšší ochrany se současně dožadujeme. Považuji za nezbytné tento proces řešit vzájemně na více rovinách – právní, technologické, strategické a dalších.

V práci jsem se soustředila na zlomový případ v souvislosti s právem být zapomenut, který podnítil úvahy o dostatečnosti stávající unijní legislativy. Rozsudek padnul roku 2014 a o dva roky později vešlo v platnost nové Nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a Směrnice Evropského parlamentu a Rady EU 2016/680, 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. Na implementaci nařízení, které se vztahuje na fyzické osoby a které je přímo účinné, byly ponechány dva roky do 25. května 2018. Vzhledem k tomu, že toto nařízení zavádí několik nových povinností správce a výrazně modifikuje některé oblasti, nelze pochybovat o nutnosti aktualizace stávajícího zákona č. 101/2000 Sb., o ochraně osobních údajů. Domnívám se, že nepůjde o razantní zpřísnění norem, protože současná podoba zmíněného zákona již poměrně přísná je, a postačila by vhodná novelizace. Myslím si, že nové nařízení, které posiluje pozici fyzické osoby při chránění jejích osobních údajů, bude mít zásadní dopad zejména na správce údajů ze soukromého sektoru. Protože nová legislativa stanovuje například nová a zásadní specifika souhlasu se zpracováním, nebude již možné vztáhnout jej jedním kliknutím nebo podpisem na často obšírné všeobecné obchodní podmínky (e-shopů či jiných zprostředkovatelů). Oproti původní situaci také vrostla výše peněžitých sankcí, i tento fakt pokládám za „motivaci“ řádné implementace do podnikových regulí. S novými povinnostmi, jež nařízení o ochraně osobních údajů přináší, lze předvídat počáteční nárůst nákladů dotčených institucí, a to jak finančních, tak administrativních. Nové nařízení ale přináší také pozitiva, a to především jasně definované právo na

přenositelnost údajů, výše zmíněná konkretizace souhlasu se zpracováním osobních údajů a možnost jeho odvolání.

Provedená analýza tří vybraných registrů a její následný rozbor ukázaly, že související právní úpravy daných databází jasně nevymezují provedení výmazu po uplynutí zákonně stanovené doby. Insolvenční zákon, jež upravuje insolvenční rejstřík, rozlišuje pouze termíny „vyškrtnutí“ a „zneprístupnění“. Zajímavou skutečností ve vztahu k právu být zapomenut je existence práva na zahrazení trestného činu, které zakládá trestní řád. Co se týká evidence přestupků, z hlediska sdílení některých údajů napříč veřejnou správou se jedná o relativně mladý institut. Spolupráce mezi základními a ostatními registry je zmíněna pouze v zákoně o Rejstříku trestů, kde dochází k získávání některých údajů, mj. skrze základní Registr obyvatel (ROB). Pokud jde o centrální evidenci přestupků, domnívám se, že představuje vhodný doplněk k rejstříku trestů.

Byly popsány některé aspekty práva být zapomenut a problematiky jeho praktické aplikace. V souvislosti s nadcházející čtvrtou průmyslovou revolucí je nutné zaměřit se nejen na technologickou, ale také na sociální a morální stránku věci. Jedná se o celkovou transformaci společnosti, jejího vnímání a jednání.

Téma diplomové práce nabízí další oblasti hodné zkoumání. Zajímavým tématem je dle mého názoru otázka hranic mezi právem na soukromí a právem na informace spojeným se svobodou tisku, nad čímž lze debatovat už dnes, a i za mnoho let. Práce také mimo jiné uvedla jednu z teorií, kdy je na osobní údaje nahlíženo jako na specifickou formu duševního vlastnictví. Rozvedení této koncepce by se mohl stát předmětem dalších odborných prací.

Seznam tabulek

Tabulka 1 - Srovnání některých aspektů vybraných rejstříků	59
Tabulka 2 - Vybrané aspekty unijních právních úprav	60

Bibliografie

Advokátní kancelář Paroulek & spol. 2006. Vzniká nová centrální evidence přestupků. *Advokátní kancelář Paroulek & spol.* [Online] 14. říjen 2006. [Citace: 24. 8. 2017]. <http://ak-pr.cz/cs/vznika-nova-centralni-evidence-prestupku/>.

Article 29 Data Protection Working Party. 2011. Opinion 15/2011 on the definition of consent. *European Commission.* [Online] 13. červen 2011. [Citace: 13. 7. 2017]. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

Curtin, Gregory G. 2007. E-Government. *Bedrosian Center.* [Online] 2007. [Citace: 3. 8. 2017]. https://bedrosian.usc.edu/files/2012/07/encyclopedia_of_political_communications.pdf.

Česká republika. Důvodová zpráva k zákonu č. 111/2009 Sb., o základních registrech.

Česká republika. 2017. Porovnání dvou znění dokumentu č. 111/2009 Sb., znění platná od 1.7.2012 a od 1.6.2017. *Změny zákonů.* [Online] 2017. [Citace: 30. 7. 2017]. <http://www.zmenyzakonu.cz/zakon.aspx?k=111/2009%20Sb.&d1=01072012&d2=01062017&cmd=compareshort>.

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

Česká republika. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Česká republika. Zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon).

Česká republika. Zákon č. 269/1994 Sb., o Rejstříku trestů.

Česká republika. 1999. Státní informační a komunikační politika - e-Česko 2006. *Culturenet.* [Online] 1999. [Citace: 30. 7. 2017]. <http://www.culturenet.cz/res/data/002/000269.pdf>.

Department of Economic and Social Affairs. 2016. United Nations E-Government Survey 2016. [Online] 2016. [Citace: 20. 7. 2017]. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf>.

Donát, Josef a Tomíšek, Jan. 2016. *Právo v síti. Průvodce právem na internetu.* Praha : C. H. Beck, 2016. str. 350. ISBN 978-80-7400-610-4.

eGov.cz. 2014. Ministerstvo informatiky. *eGov.cz.* [Online] 2014. [Citace: 30. 7. 2017]. <http://www.egov.cz/kdo-je-kdo/institute/ministerstvo-informatiky>.

European Court of Human Rights. 2004. CASE OF VON HANNOVER v. GERMANY. *European Court of Human Rights.* [Online] 24. červen 2004. [Citace: 3. 6. 2017]. <http://www.bailii.org/eu/cases/ECHR/2004/294.html>.

European Court of Human Rights. 2005. European Court of Human Rights - Chamber judgment (just satisfaction) - von Hannover v. Germany. *Council of Europe.* [Online] 2005. [Citace: 3. 6. 2017]. <https://wcd.coe.int/ViewDoc.jsp?p=&id=890483&Site=COE&direct=true>.

Evropská komise. 2010. Digitální agenda pro Evropu: klíčové iniciativy. *European Commission*. [Online] 19. květen 2010. [Citace: 13. 5. 2017]. http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm .

Evropská komise. 2010. Evropa 2020: Strategie pro inteligentní a udržitelný růst podporující začlenění. *EUR-Lex*. [Online] 3. březen 2010. [Citace: 13. 5. 2017]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:CS:PDF>.

Evropská unie. Nařízení Evropského parlamentu a Rady EU 2016/679.

Evropská unie. 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.

Evropská unie. Směrnice Evropského parlamentu a Rady EU 2016/680.

Fried, Charles. 1968. Privacy. [Online] 1968. [Citace: 8. 5. 2017]. <http://www.jstor.org/stable/794941>.

Georgetown Law. 2017. Franz Werro. *Georgetown Law*. [Online] 2017. [Citace: 20. 7. 2017]. <http://www.law.georgetown.edu/faculty/werro-franz.cfm>.

Good Governance. O Good Governance. *Good Governance*. [Online] [Citace: 16. 7. 2017.] <http://goodgovernance.cz/o-good-governance/>.

Graux, Hans, Ausloos, Jef a Valcke, Peggy. 2012. The Right to be Forgotten in the Internet Era. [Online] 2012. [Citace: 17. 7. 2017]. <http://ssrn.com/link/ICRI-RES.html>.

iDNES.cz. 2002. Senát schválil vznik ministerstva informatiky. *iDNES.cz*. [Online] 15. listopad 2002. [Citace: 30. 7. 2017]. http://mobil.idnes.cz/senat-schvalil-vznik-ministerstva-informatiky-f54-/mob_tech.aspx?c=A021114_5182628_mob_aktuality.

Iniciativa 202020. 2016. Naše vize. *202020*. [Online] 2016. [Citace: 22. 7. 2017]. <http://202020.cz/nase-vize/>.

Jääskinen, Niil. 2014. Stanovisko generálního advokáta N. Jääskinena přednesené dne 25. června 2013. *CURIA*. [Online] 25. červen 2014. [Citace: 17. 6. 2017]. curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=433733.

justice.cz. 2016. Nově spuštěná centrální evidence přestupků je plně funkční. *Bulletin advokacie*. [Online] 5. říjen 2016. [Citace: 20. 8. 2017]. <http://www.bulletin-advokacie.cz/nove-spustena-centralni-evidence-prestupku-je-plne-funkcni>.

Kučerová, Alena, a další. 2003. *Zákon o ochraně osobních údajů. Komentář*. Praha : C. H. Beck, 2003. str. 406. ISBN 80-7179-762-6.

Lechner, Tomáš. 2017. Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR). [Online] 2017. [Citace: 18. 5. 2017]. <https://www.isss.cz/archiv/2017/download/isss2017.pdf>.

Magazín Egovernment. 2017. Kyberbezpečnost, eIDAS a GDPR - nejen osobní ochranný faktor. *Magazín Egovernment*. [Online] únor 2017. [Citace: 17. 5. 2017]. <https://www.egovernment.cz/soubor/magazin-egovernment-2-2017/>.

Matejka, Ján. 2013. *Internet jako objekt práva: hledání autonomie a soukromí.* Praha : CZ.NIC, 2013. str. 262. ISBN 978-80-904248-7-6.

Mates, Pavel a Smejkal, Vladimír. 2012. *E-governmment v České republice: Právní a technologické aspekty.* Praha : Leges, 2012. ISBN 978-80-87576-36-6.

Matoušová, Miroslava a Hejlík, Ladislav. 2008. *Osobní údaje a jejich ochrana.* Praha : ASPI, Wolters Kluwer, 2008. str. 468. ISBN 978-80-7357-322-5.

Matoušová, Miroslava a Hejlík, Ladislav. 2003. *Osobní údaje a jejich ochrana. Knižka pro praxi.* Praha : ASPI, 2003. str. 416. ISBN 80-86395-50-2.

MVČR. 2017. Implementační plány. *Ministerstvo vnitra České republiky.* [Online] 2017. [Citace: 29. 7. 2017]. <http://www.mvcr.cz/clanek/implementacni-plany.aspx>.

MVČR. 2012. Zákon č. 227/2000 Sb., o elektronickém podpisu. *Ministerstvo vnitra České republiky.* [Online] 1. říjen 2012. [Citace: 30. 7. 2017]. <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

MVČR. 2016. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. *Ministerstvo vnitra České republiky.* [Online] 24. říjen 2016. [Citace: 30. 7. 2017]. <http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx>.

Neuwirth, Karel. 2003. Ochrana osobních údajů a vstup do EU. *Úřad pro ochranu osobních údajů.* [Online] 2003. [Citace: 10. 5. 2017]. https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8087.

Nevrkla, Luboš. 2015. Centrální evidence přestupků. *EPRAVO.CZ.* [Online] 10. listopad 2015. [Citace: 10. 8. 2017]. <https://www.epravo.cz/top/clanky/centralni-evidence-prestupku-99548.html>.

OECD. 2002. Glossary of Statistical Terms. *OECD Statistics.* [Online] 2002. [Citace: 18. 6. 2017]. <https://stats.oecd.org/glossary/detail.asp?ID=4752>.

OSN. 1966. Mezinárodní pakt o občanských a politických právech. *Lidská práva.* [Online] 1966. [Citace: 9. 5. 2017]. http://www.lidskaprava.cz/uploads/03_dokumenty/04_uvod/01_ICCPR.pdf.

Paták, Tomáš. 2017. Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích. *Úřad pro ochranu osobních údajů.* [Online] 2017. [Citace: 27. 5. 2017]. https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23790&n=obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-odpovedich.

Peterka, Jiří. 2003. Portál veřejné správy odstartuje za měsíc. *Archiv článků a přednášek Jiřího Peterky.* [Online] 2003. [Citace: 30. 7. 2017]. <http://www.earchiv.cz/b03/b0915001.php3>.

Redakce ePravo.cz. 2001. Opis a výpis z Rejstříku trestů. *EPRAVO.CZ.* [Online] 23. říjen 2001. [Citace: 10. 8. 2017]. <https://www.epravo.cz/top/clanky/opis-a-vypis-z-rejstriku-trestu-15264.html>.

- Skoupý, Arnošt. 1989.** Texty k obecným dějinám kapitalismu I. *Katedra historie Filozofické fakulty Univerzity Palackého*. [Online] 1989. [Citace: 8. 5. 2017]. <http://www.historie.upol.cz/19/prameny/prava.htm>.
- Soudní dvůr Evropské unie. 2014.** Rozsudek Soudního dvora. *CURIA*. [Online] 13. květen 2014. [Citace: 17. 6. 2017]. <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=cs>.
- Škorníčková, Eva. 2017.** GDPR cirkus přijíždí. Začínáme! *GDPR.cz*. [Online] 27. duben 2017. [Citace: 15. 5. 2017]. <https://www.gdpr.cz/blog/gdpr-cirkus/>.
- Šmíd, Vladimír.** Srovnání právních úprav vztahujících se k ochraně osobních údajů v ČR a SR. *Fakulta informatiky Masarykovy univerzity*. [Online] [Citace: 10. 5. 2017]. <https://www.fi.muni.cz/~smid/ochdcrsr1.html>.
- Špaček, David. 2012.** *eGovernment - cíle, trendy a přístupy k jeho hodnocení*. Praha : C.H. Beck, 2012. 978-80-7400-261-8.
- trestni-rizeni.com. 2006-2017.** Rejstřík trestů. *trestni-rizeni.com*. [Online] 2006-2017. [Citace: 10. 8. 2017]. <http://www.trestni-rizeni.com/vyklad-pojmu/rejstrik-trestu>.
- United Nations Information Centre. 1948.** Všeobecná deklarace lidských práv. *United Nations Human Rights*. [Online] 1948. [Citace: 9. 5. 2017]. <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=czc>.
- United Nations. 2016.** UN E-Government Survey 2016. *Public Administration and Development Management*. [Online] 2016. [Citace: 22. 7. 2017]. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.
- Úřad pro ochranu osobních údajů. 2013.** Úřad. *Úřad pro ochranu osobních údajů*. [Online] 2013. [Citace: 12. 5. 2017]. <https://www.uoou.cz/urad/ds-1059/p1=1059>.
- Warren, Samuel a Brandeis, Louis. 1890.** The Right to Privacy. [Online] 15. Prosinec 1890. [Citace: 13. 5. 2017]. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
- Werro, Franz. 2009.** The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash. [Online] 2009. [Citace: 15. 7. 2017]. <http://ssrn.com/abstract=1401357>.
- Westin, Alan F. 1968.** Privacy And Freedom. *Washington & Lee University School of Law*. [Online] 1968. [Citace: 13. 5. 2017]. <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.