

4 OCHRANA SOUKROMÍ A OSOBNÍCH ÚDAJŮ V KONCOVÉM ZAŘÍZENÍ

Na základě předchozích závěrů jsou dále zkoumány metody, jakými data o uživateli opouštějí koncové zařízení a jsou sdílena mimo faktickou kontrolu uživatele. V předchozí kapitole bylo argumentováno, že interní data vznikající v dispozici uživatele uvnitř koncového zařízení, je možné chránit proti cizím subjektům lépe než data externí. Vedle toho externí data o aktivitě uživatele jsou vytvářena primárně v softwaru třetích stran, jakými jsou zejména provozovatelé aplikací a webových stránek, a hrozí daleko vyšší riziko jejich zneužití. Fakticky totiž s nimi disponují právě subjekty odlišné od uživatele, kteří mají tendenci data využívat pro vlastní účely a sdílet je i s dalšími subjekty. V případě zpracování dat provozovateli aplikace jsou data vázána režimem, který je stranami smluvně sjednán, přičemž tento se bude lišit *ad hoc*.

Uživatel se měl se smluvními podmínkami a dalšími dokumenty pro uživatele seznámit a musel je v minulosti přijmout (příp. je sjednat). Navíc se s nimi v případě zájmu může kdykoliv podrobněji seznámit. Obdobně i údaje o nakládání s jeho osobními údaji musejí být dostupné v Politice soukromí. V tomto povinně zveřejňovaném dokumentu¹⁷⁵ popisují provozovatelé aplikací všechny podstatné informace o zpracování osobních údajů, včetně zákonných důvodů a účelů zpracování osobních údajů uživatelů.

V případě zpracování externích dat provozovateli webových stránek zpravidla neexistuje žádný kontrakt, kde by uživatel s provozovatelem webové stránky vymezili vzájemná práva a povinnosti nebo zpracování osobních údajů uživatele. Absenci dohody mezi stranami řeší právní úprava, která stanovuje podmínky a možnosti čtení a ukládání dat do koncového zařízení uživatele i obecné nakládání s daty, která by se mohla k uživateli ať již přímo či nepřímo vztáhnout. Aby mohla být právní úprava správně aplikována, je nezbytné vymezit faktické fungování jednotlivých metod identifikace koncových zařízení, prostřednictvím nichž jsou data uživatelů zpracovávána.

V praxi jsou internetové stránky standardně načítány prostřednictvím tradičního http protokolu, který je ze své podstaty anonymní. Jedná se totiž o bezstavový protokol, který neumí uchovávat stav komunikace a takto postupně identifikovat uživatele, kteří na stránku přistoupí. Přistoupivší uživatel je v tomto protokolu bez dalšího vždy nejprve neznámý. Aby mohli provozovatelé webových stránek své uživatele identifikovat a dále pracovat s daty o jejich aktivitě, přicházejí provozovatelé webových stránek s inovativními metodami, jak uživatele prostřednictvím koncového zařízení identifikovat a sbírat o nich osobní údaje. Pro pochopení a vyřešení

¹⁷⁵ *Privacy Laws for Apps: How to Protect User Data?* [online].

této problematiky, která má obrovský potenciál ovlivnit soukromí uživatele koncového zařízení, je nezbytné se těmito metodami identifikace a extrakce dat z koncového zařízení dále zabývat.

V této kapitole je proto pojednáno o konkrétních metodách a souvisejících datových tocích, které identifikují jednotlivce v kyberprostoru. Postupně jsou vymezeny způsoby, jakými jsou data z koncových zařízení získávána a jaký je legislativní rámec použití těchto identifikačních metod, stejně jako následného zpracování získaných dat.

V současnosti existuje a používá se velké množství technických způsobů, jak koncové zařízení na webových stránkách identifikovat. Jednou z nejstarších a dlouhodobě nejrozšířenějších metod sledování uživatelů na internetu jsou tzv. http cookies.¹⁷⁶

4.1 Http cookies¹⁷⁷

Internet je zdrojem nepřehledného množství dat a informačních zdrojů, které lákají uživatele především pro jejich snadnou dostupnost a bezplatnost. Aktivita uživatelů, kteří v kyberprostoru prostřednictvím svých koncových zařízení vyhledávají informace, nebo přistupují k určitým službám, ale generuje také velké množství údajů o jejich aktivitě a sledovaných zájmech, které zase motivují poskytovatele služeb tato data sbírat a optimálně je i dále využívat ve svém podnikání. Tímto synergickým efektem dochází k obrovskému nárůstu objemu dat, kdy podle studie Dell Technologies Global Data Protection Index z roku 2021 spravují soukromé společnosti desetinásobný objem dat jen oproti roku 2016.¹⁷⁸

Lidé, kteří používají internetové služby, si často neuvědomují, že plátdlem v kyberprostoru již dávno nejsou pouze peníze, ale daleko častěji data včetně těch z digitální stopy, která za sebou uživatelé zanechávají.¹⁷⁹ Není proto divu, že správci webových stránek mají snahu shromažďovat o uživatelích jejich webu co možná nejvíce informací o jejich činnosti a předvolbách pomocí sledovacích zařízení, kterými mohou být i http cookies (dále jen „cookies“).¹⁸⁰

¹⁷⁶ Klodwig, J. Pokročilé metody identifikace koncových zařízení. In: Janovec, M. et al. (eds). *CO-FOLA 2020*. Brno: Muni Press, 2020, s. 1096; Roesner, F., Kohno, T., Wetherall, D. Detecting and Defending Against Third-Party Tracking on the Web [online]. *USENIX*. [cit. 2. 3. 2022]. Dostupné z: <https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner>.

¹⁷⁷ Tato kapitola vychází z Klodwig, J. *Aktuální otázky právní úpravy cookies*. 2018, studentská odborná vysokoškolská činnost, Masarykova univerzita, Právnická fakulta, s. 14–21.

¹⁷⁸ DELL Technologies. Global Data Protection Index 2021: Key Findings [online]. *delltechnologies.com*. [cit. 27. 9. 2023]. Dostupné z: www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-keyfindings.pdf.

¹⁷⁹ Donát, J., Tomíšek, J. *Právo v síti: průvodce právem na internetu*. Praha: C. H. Beck, 2018, s. 5; srov. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2018.

¹⁸⁰ Mo, J. Y. C. Cookies and Browser-Generated Information: The Challenge in Hong Kong Under the Personal Data (Privacy) Ordinance. *Statute Law Review*. 2017, roč. 38, č. 1, s. 2.

Cookies byly poprvé vytvořeny před zhruba 30 lety a postupně se staly základním kamenem pro online marketing a cílení reklamy v kyberprostoru.¹⁸¹ V současnosti jsou využívány téměř každou webovou stránkou¹⁸² a jejich hodnota spočívající ve sledování a ukládání dat o chování uživatelů online generovala již v roce 2017 téměř neuvěřitelných 35 miliard amerických dolarů.¹⁸³

Soubory cookies lze definovat jako malé textové soubory, jež navštívený webový server pošle prohlížeči uživatele k uložení přímo do koncového zařízení, např. notebooku nebo smartphonu. Při každém dalším navštívení této stránky se pak server prohlížeče ptá, zda nemá takový soubor u sebe uložený. Podle odpovědi je pak uložená informace v textovém souboru zdrojovým serverem rozeznána a její uživatel identifikován. Tímto způsobem je překonáván charakteristický rys http protokolu, který nedokáže sám o sobě uživatele identifikovat. V praxi se to projevuje například tak, že když uživatel dvakrát během hodiny navštíví jednu webovou stránku, tak stránka pouze ví, že došlo ke dvěma připojením, ale už nedokáže bez dalšího rozeznat, kdo se k ní připojil. Zjistí tak, kolikrát se stránka načetla, ale už sama o sobě nezjistí, že to bylo z téhož mobilního telefonu. A přesně tuto nedokonalost lze pomocí cookies snadno překonat. Stačí pouze uživatele označit při prvním průchodu souborem cookies a při dalším pak soubor přečíst a snadno skrze něj zjistit, že zařízení s tímto označením už bylo k webové stránce dříve připojeno.

Standardní struktura souborů cookies je proměnlivá. Může se skládat z několika možných komponent. Jedinou obligatorní, tedy vždy nutně v cookies uloženou složkou, je jméno a hodnota. NAME=VALUE generuje přímo zdrojová stránka. Ta si jméno i unikátní hodnotu souboru uloží, a příště podle tohoto unikátního kódu v jí vytvořené cookie konkrétního uživatele rozezná. Kromě této základní složky se však rozlišuje ještě DATE, které označuje dobu, po kterou má být soubor v zařízení uložen, DOMAIN_NAME, tedy název domény, která soubor vytvořila a která si tudíž následně může vyžádat zaslání předešlých cookies a PATH jako pomocný atribut, který slouží k ověření, zda má daný server k souboru cookies přístup.¹⁸⁴ Můžeme se setkat také s velikostí souboru SIZE, nebo dalšími komponenty, které jsou někdy rozeznávány. Ty však nejsou z hlediska právní úpravy důležité.

V praxi zdrojová stránka uloží svoji cookie přímo do prohlížeče klienta při jeho prvním průchodu stránkou. Do NAME se uloží libovolný název cookie a do VALUE zakódovaná informace o libovolných skutečnostech. Pro lepší znázornění si lze pod těmito obecnými skutečnostmi představit například údaje o osobní konfiguraci stránky provedené uživatelem, jako je zvolený jazyk stránky, volba pozadí, ale také preference reklam, nebo údaje nutné k vícefázovému provedení platby. Počet

¹⁸¹ Ibid., s. 2.

¹⁸² Z obchodní analýzy společnosti consentmanager.net mapující pomocí crawleru 100 000 nejnavštěvovanějších webových stránek v Evropě vyplývá, že cookies používá 96 % z pozorovaných webových stránek. Viz Winker. *Competition Analysis of Consentmanager*.

¹⁸³ Ibid., s. 2.

¹⁸⁴ Debussere, F. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?. *International Journal of Law and Information Technology*. 2005, roč. 13, č. 1, s. 77.

údajů a jejich kódu je pak úměrný velikosti textového cookies souboru. Při dalším průchodu daného uživatele stránkou se stránka zeptá, zda je v prohlížeči uložena cookie jména, jež eviduje a následně kód uložený ve VALUE použije pro rozklíčování dříve uložených skutečností. Pole DOMAIN_NAME přitom zajišťuje, aby se k dané cookie nemohla připojit jiná třetí stránka.

Zjednodušeně je možné říci, že soubory cookies jsou to, co uživatelům umožňují opakovaně nezadávat přihlašovací údaje, pokud se uživatel k webové stránce již jednou v relaci přihlásil, předvyplňuje online formuláře, napomáhá ochraně webových stránek před DDoS útoky a usnadňuje náš průchod oblíbenými webovými stránkami z našich osobních zařízení. Cookies však stejně tak mohou sloužit i jako nástroj personifikace reklamy, který díky jednomu vyhledávání bonboniéry pro přítelkyni může další týden nabízet na různých třetích stránkách cukrovinky, anebo po hledání zubní náhrady pro babičku obtěžovat měsíce nabídkou výhodných zubních protéz. Je proto nutné rozlišovat v rámci cookies jejich různé druhy.

4.2 Právně významná členění cookies¹⁸⁵

Rozvoj online světa předznamenal i rozvoj cookies, jakožto jednoho z primárních způsobů identifikace uživatelů v kyberprostoru. Vzhledem k technické povaze souborů cookies a jejich významu pro právo je třeba hodnotit více rozlišovacích kategorií. Neustále nové technické možnosti a vynalézavost ze strany poskytovatelů cookies zavdali příčinu pro vznik třídění cookies do následujících kategorií.

Prvním kritériem významným pro právní klasifikaci cookies je doba jejich trvání. Tím rozumíme nikoliv nutně časový úsek stanovený délkou časové jednotky, ale také skutečnost, na kterou se zánik cookies váže. Z tohoto pohledu rozlišujeme „Session cookies“ neboli cookies pro relaci a tzv. perzistentní cookies.¹⁸⁶

- **Cookies pro relaci** je krátkodobější forma cookies, která je funkční pouze pro danou relaci,¹⁸⁷ ve které byla vytvořena. Po skončení relace, tedy po zavření prohlížeče, se cookies pro relaci automaticky smaže. Z důvodu nesvázanosti životnosti u tohoto typu cookies s časovou jednotkou absentuje pole DATE.
- **Perzistentní cookies** mají podstatně delší životnost. Jejich zánik není již vázán toliko na zavření prohlížeče, a v prohlížeči zůstávají i při jeho dalším spuštění.¹⁸⁸ U tohoto typu je tak zánik vázán na časovou hodnotu definovanou v poli DATE.

¹⁸⁵ Tato podkapitola vychází z Klodwig, J. *Aktuální otázky právní úpravy cookies*, s. 14–21.

¹⁸⁶ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies [online]. *Europa.eu*. 7. 6. 2012. [cit. 16. 4. 2021], s. 4. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf.

¹⁸⁷ Relaci rozumíme trvání spojení prohlížeče s danou stránkou, která začíná otevřením stránky a končí jejím zavřením. Jinými slovy je to průchod uživatele webovou stránkou.

¹⁸⁸ Article 29 Data Protection Working Party. Opinion 1/2008 on data protection issues related to search engines [online]. *Europa.eu*. [cit. 13. 2. 2019], s. 19. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

Z výše uvedeného lze snadno vyvodit, proč je nutné provést tuto distinkci. Zatímco cookies pro relaci jsou spíše praktickým nástrojem pro jednorázové použití stránky, perzistentní cookies jsou pro svůj dlouhodobý charakter daleko vhodnější k monitorování uživatelských preferencí. To dokazuje i analýza WP29, jež v roce 2015 naměřila, že z celkového počtu 16 555 zaznamenaných cookies bylo pouhých 2 302 cookies pro relaci. Zajímavostí je, že ČR se z osmičky států, v nichž průzkum probíhal, umístila na prvním místě s počtem perzistentních cookies, kdy oproti 124 cookies pro relaci bylo naměřeno 1 144 cookies perzistentního charakteru.¹⁸⁹

Dalším důležitým kritériem z hlediska práva je **původ cookies**. Zde rozlišujeme:

- **Cookies prvních stran** pocházejí přímo od provozovatele internetové stránky, kterou uživatel navštívil. Adresa URL navštívené stránky je tedy shodná s polem DOMAIN_NAME.
- **Cookie třetích stran** je oproti tomu nastavena internetovou stránkou s doménou, která se liší od domény internetové stránky, kterou uživatel navštívil. Adresa zobrazená v poli prohlížeče pro adresu se liší od adresy, jež cookie spravuje.¹⁹⁰ V praxi se jedná zejména o cookies vytvořené ostatními weby, které na navštívené stránce publikují nějaký obsah, jakým je typicky obrázek, video nebo například reklamní pole.

Termín cookies třetích stran přitom může při hlubším poznání působit potíže, a to zejména vzhledem k definici v GDPR, kde je třetí osoba definována jako:

„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů“.

Je třeba podotknout, že třetí stranu definujeme v kontextu cookies pouze podle struktury URL tak, jak je zobrazena v adresovém řádku prohlížeče.¹⁹¹

Rozlišení cookies prvních a třetích stran je důležité zejména při posuzování nezbytnosti cookies pro službu poskytovanou uživateli neboli zda se zakázáním používání cookies neohrozí samotný chod poskytované služby. Cookies třetích stran se často používají pro remarketing¹⁹² a podobné reklamní účely, a tedy obvykle nejsou nezbytně nutné pro uživatele, jež stránku navštíví.

Uvedené skutečnosti těsně souvisejí s potřebou členit cookies také podle účelu, ke kterému slouží. Pro toto dělení vytvořila Mezinárodní obchodní komora v Paříži

¹⁸⁹ Article 29 Data Protection Working Party. Cookie sweep combined analysis – report. [online]. *Europa.eu*. [cit. 13. 2. 2019], s. 7. Dostupné z: <https://ec.europa.eu/newsroom/article29/redirection/document/56123>.

¹⁹⁰ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies.

¹⁹¹ *Ibid.*, s. 5.

¹⁹² Remarketing je metoda cílení internetové reklamy, která spočívá v zacílení na uživatele, kteří někdy v minulosti již navštívili web poskytovatele pomocí souborů cookies.

(dále jen „**Komora**“) praktické členění do čtyř kategorií vhodné pro další právní klasifikaci.¹⁹³

1. **Nezbytně nutné cookies** jsou specifickou kategorií a jsou nutné pro správné fungování některých funkcí webových stránek. Na jejich uložení závisí správné fungování například rozhraní nákupního košíku na e-shopu či platby přes internet. Půjde zejména o služby, o něž si uživatel sám zažádal, přičemž pojem „nezbytně nutné“ je podle Komory nutné vykládat restriktivně.
2. **Výkonnostní cookies** jsou cookies, jež slouží ke zlepšování výkonu daných stránek, přičemž se jejich použitím téměř nenaruší soukromí uživatele, neboť sbírané informace jsou převážně anonymní. Tento typ cookies nespadá pod kategorii osobních údajů (jak je podrobněji popsáno níže) a je nejčastěji využíván k měření návštěvnosti stránek, informování partnerských subjektů o tom, že uživatel přešel na dané stránky ze stránek partnera, nebo zda takový přechod vedl k nákupu inzerované služby či produktu.
3. **Funkční cookies** slouží k modifikaci uživatelského rozhraní webové stránky. V cookies jsou v tomto případě uloženy informace o přizpůsobení stránky potřebám uživatele jako je velikost textu, písma, nebo jiné variabilní prvky. Časté je také ukládání informací, o již prohlédnutých produktech či zhlédnutých videích, aby v dalších průchodech uživatele nedošlo k opakování téže nabídky. Byť funkční cookies mohou obsahovat např. informaci o geografické poloze uživatele a zobrazovat mu denně relevantní předpovědi počasí, pro řadu uživatelů už se může jednat o příliš osobní informace, a tedy se zde mohou rozcházet názory na přiměřenost zpracování údajů na ose komfortu a ochrany soukromí uživatele.
4. **Reklamní cookies** jsou záměrně uváděné až čtvrté, a toto místo jim náleží také z pohledu testu proporcionality mezi jejich potřebností a mírou narušení soukromí jejich subjektu. Jak totiž jejich název napovídá, používají se k cílení reklamy. Jejich obsahem je, kromě počtu zobrazení stránek, zejména počet zobrazení reklamy a její úspěšnost z hlediska prokliku.¹⁹⁴ Jsou to právě reklamní cookies, na kterých doposud stojí drtivá část online reklamního průmyslu.¹⁹⁵

Sama Komora ovšem přiznává, že výše uvedené dělení není vždy jednoznačné. Často se může stát, že jeden z typů splývá s jiným.¹⁹⁶ Ve skutečnosti je naprosto

¹⁹³ International Chamber of Commerce. ICC UK Cookie guide [online]. *cookielaw.org*. 2012. [cit. 17. 2. 2020]. Dostupné z: https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookies_guide_revnov.pdf. Případně lze použít také v praxi oblíbené a zjednodušené členění rozlišující pouze nezbytně nutné cookies, reklamní cookies, a pak středovou kategorii analytických cookies.

¹⁹⁴ Jako proklik se označuje takové kliknutí na reklamu, které uživatele dovede až na cílovou stránku. Může se totiž stát, že byť uživatel na odkaz klikne, nedostane se na cílovou stránku z různých důvodů. Proklik se nejčastěji používá při používání internetové reklamy.

¹⁹⁵ Krčmář, P. Cookies umírají, reklamní branže si ale najde náhradu [online]. *root.cz*. 13. 2. 2014. [cit. 11. 2. 2018]. Dostupné z: <https://www.root.cz/clanky/cookies-umiraji-reklamni-branze-si-ale-najde-nahradu/>.

¹⁹⁶ Toto neplatí pouze pro nezbytně nutné cookies, které jsou přímo definovány v článku 5 odst. 3 směrnice o soukromí a elektronických komunikacích a do českého právního řádu promítnuty v § 89 odst. 3 zák. o elektronických komunikacích.

běžná „symbióza“ například funkčních a reklamních cookies. Pokud dojde k podřazení pod více kategorií, mělo by se se souborem pracovat tak, jako by byl zároveň všemi z výše podřazených.¹⁹⁷ Bez ohledu na jednotlivá dělení lze z hlediska vývoje identifikačních metod všechna výše zmíněná dělení cookies pojednávající o základních http cookies souhrnně označit jako „**identifikační metody první generace**“.

4.3 Ochrana osobních údajů v kontextu koncových zařízení

Výše bylo v kapitole č. 3 pojednáno o datech, informacích a osobních údajích, které se v koncových zařízeních vytvářejí ať již jejich vložením samotným uživatelem, během jeho činností na koncovém zařízení, nebo ve spolupráci s třetími stranami prostřednictvím aplikací nebo webových stránek. Vzhledem k oblíbenosti surfování na internetu jsou to však zejména provozovatelé webových stránek, kteří vytvářejí díky identifikačním metodám první generace (představených v předchozí kapitole č. 4.1) rozsáhlá behaviorální data, která zůstávají v jejich dispozici. V tomto kontextu **je potřeba rozlišit ochranu osobních údajů a ochranu soukromí uživatele v koncovém zařízení**, jelikož obě tyto oblasti jsou regulovány svébytnou právní úpravou.

Ochrana soukromí může být ohrožena zejména svévolnými přístupy do koncového zařízení stran provozovatelů aplikací a webových stránek, kteří se ve větší či menší míře mohou dostávat do koncového zařízení a přistupovat k některým datům uloženým v koncovém zařízení, číst je anebo do něj také ukládat data vlastní. Vedle toho ochrana osobních údajů řeší nakládání s těmi daty, která jsou ať již přímo či nepřímo přiřaditelná ke konkrétní fyzické osobě, přičemž se může jednat o zpracování těch dat, která jsou z koncového zařízení čtena nebo do koncového zařízení ukládána. Ochrana osobních údajů a ochrana soukromí jsou tedy jako dvojčata, která je nutno vzít v úvahu vždy obě. To znamená že pokaždé, když se řeší ochrana osobních údajů v koncových zařízeních, mělo by se myslet i na ochranu soukromí a naopak.

Ochranu osobních údajů někteří autoři v minulosti označovali jako součást práva na ochranu soukromí,¹⁹⁸ a jiní je považují za dvě samostatná rovnocenná práva.¹⁹⁹ Souhlasit lze dle mého názoru s oběma těmito názory, jelikož se vztah těchto dvou právních odvětví vyvíjel. Ochrana osobních údajů se totiž v minulosti vyvinula z ochrany soukromí.²⁰⁰

¹⁹⁷ International Chamber of Commerce. *ICC UK Cookie guide*, 2012, s. 8–10.

¹⁹⁸ Molek, P. *Základní práva. Svazek první – Důstojnost*. Praha: Wolters Kluwer, 2017, s. 368.

¹⁹⁹ Polčák, R., Svantesson, D. J. B. *Information Sovereignty*. UK: Edward Elgar Publishing, 2017, s. 111.

²⁰⁰ Obě práva na ochranu soukromí a na ochranu osobních údajů totiž vycházejí ze stejného základu a lze je uchopit v rámci širšího konceptu práva na informační sebeurčení, o kterém bylo podrobně pojednáno v kapitole 2.3.

V souvislosti s výše popsáním raketovým růstem dat, a tedy i osobních údajů v kyberprostoru, se zvyšovala i potřeba s těmito osobními údaji, které již byly v kyberprostoru přítomné, dále nakládat. Nestačilo již pouze stanovit, která data o své osobě zveřejnit a která nikoliv, ale objevila se celá řada otázek, jak nakládat s osobními údaji již jednou v kyberprostoru zveřejněnými, která stále rostla na důležitosti. Objevovaly se i otázky nové, jako jaký je vůbec obsah ochrany osobních údajů, jestli vůbec existuje právo na výmaz, nebo co všechno je osobním údajem. Tyto všechny otázky tlačené poptávkou praxe zapříčinily, že z ochrany osobních údajů se stala nejprve jedna z nejrychleji se rozvíjejících oblastí ochrany soukromí,²⁰¹ a posléze i nejrychleji se rozvíjející samostatné právo, které se z ochrany soukromí vyčlenilo a etablovalo vlastní veřejnoprávní povahu, odlišnou od původní soukromoprávní povahy ochrany soukromí.

Právě kvůli své relativně nedlouhé existenci není ochrana osobních údajů zakotvena ve starších lidskoprávních dokumentech (na rozdíl od ochrany soukromí, viz podkapitulu 2.2) jako je Mezinárodní pakt o občanských a politických právech, nebo EÚLP. Původně nebyla ochrana osobních údajů obsažena ani v původním návrhu Listiny základních práv a svobod Evropské unie²⁰² vypracovaném na přelomu tisíciletí.

O jak moderní právo se jedná dokazuje fakt, že se ochrana osobních údajů do Listiny základních práv Evropské unie²⁰³ dostala až během procesu jejího přijímání, a to „díky narůstajícímu povědomí potřeby speciálně ochránit některá základní práva, která jsou potenciálně ohrožena stále narůstající technologickou revolucí.“²⁰⁴ Až judikatura ESLP začala ochranu osobních údajů jako specifický aspekt ochrany soukromí postupně rozeznávat a následně podřazovat pod článek 8 EÚLP.²⁰⁵ Naproti tomu v české legislativě máme ochranu osobních údajů zakotvenou již v ústavním pořádku, a sice článkem 10 odst. 3 LZPS, který stanoví, že: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“²⁰⁶ To pak v české legislativě specifikoval od roku 1992 samostatný zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, a následně pak i zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. I druhý zmíněný zákon je však v současnosti již derogován novějšími předpisy, a sice evropským nařízením GDPR a implementačním zákonem – ZZOU.

GDPR společně se směrnicí Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním

²⁰¹ Molek, P. *Základní práva. Svazek první – Důstojnost.*, s. 368.

²⁰² Listina základních práv Evropské unie (Úř. Věst. C 202, 7. června 2016).

²⁰³ Ibid.

²⁰⁴ Donati, F. Protection of Personal Data. In: Mock, W. B. T. et al. (eds). *Human Rights in Europe: Commentary on the Charter of Fundamental Rights of the European Union*. Durham, South Carolina: Carolina Academic Press, 2010, s. 53.

²⁰⁵ Molek, P. *Základní práva. Svazek první – Důstojnost.*, s. 362.

²⁰⁶ Článek 10 odst. 3 LZPS.