ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

Ochrana osobních, provozních a lokalizačních údajů v sítích elektronických komunikací

Jakub Šindelář

Plzeň 2022

ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PRÁVNICKÁ

KATEDRA OBCHODNÍHO PRÁVA

Studijní program: Právo a právní věda
Obor: Právo

Vedoucí práce: JUDr. Pavla Tloušťová, Ph.D., MBA
Katedra obchodního práva

Diplomová práce

Ochrana osobních, provozních a lokalizačních údajů v sítích elektronických komunikací

Jakub ŠINDELÁŘ

Plzeň 2022

"Prohlašuji, že jsem diplomovou práci na téma: ***Ochrana osobních, provozních a lokalizačních údajů v sítích elektronických komunikací zpracoval sám.*** *Veškeré prameny a zdroje informací, které jsem použil k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury."*

Podpis autora práce

…….

Poděkování

Rád bych na tomto místě poděkoval vedoucí diplomové práce **JUDr. Pavle Tloušťové, Ph.D., MBA**, za počáteční rady a velice vstřícný přístup.

Obsah

Seznam zkratek

ARPU – Average revenue per user (ukazatel průměrné tržby na jednoho uživatele)
GDPR – Obecné nařízení o ochraně osobních údajů
EU – Evropská unie
SFEU – Smlouva o fungování Evropské unie
SOOUSEK – Směrnice o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
ZEK – Zákon o elektronických komunikacích

Úvod

Jedním ze znaků moderní společnosti je potřeba neustále se vyvíjet na poli technologického výzkumu. Během několika uplynulých desetiletí se tento vývoj hnal nezadržitelnou, a především stále rostoucí rychlostí kupředu, a stejná tendence se dá očekávat i od let a desetiletí následujících. Ve většině případů měla myšlenka pro jistou technologickou inovaci ve svém zárodku touhu určitým způsobem pomoct lidské společnosti, někam jí posunout. Není naivní si myslet, že za vznikem nových technických prototypů stojí vznešený účel použít je pro dobro lidstva, ale jak známé přísloví říká, každá mince má dvě strany.

Na jedné straně máme technologický pokrok skrze neustále se rozvíjející se monetizace dat na sítích. Na straně druhé pak základní lidské právo na soukromí. Vezmeme-li v potaz drasticky se zrychlující technologický rozvoj komunikačních zařízení a platforem, a s ním spojený sběr všemožných dat, a podíváme se na zdlouhavé přijímání zákonů pro ochranu našeho soukromí, je na místě si myslet, že zákon musí být z povahy věci pozadu.

Komunikace je pro kohokoliv naprosto klíčová činnost a z mého pohledu vůbec základním stavebním prvkem pro přežití, dosahování cílů a budování společných věcí. Člověk v moderní době je schopen komunikovat prostřednictvím mnoha možných kanálů. Osobní komunikace jako by byla stále častěji nahrazována něčím rychlejším, efektivnějším, ač více neosobním. Komunikace skrze internet, zejména za použití chytrých telefonů prostřednictvím sociálních sítí, je čím dál tím více v rozkvětu.

Tento rozkvět efektivity a pohodlnosti však podrývá neosobnost vůči osobě, se kterou komunikujeme a paradoxně větší osobitost pro třetí stranu, která komunikaci zprostředkovává a sbírá o nás různorodé informace. Ač jsou tyto informace drobné a na první pohled nedůležité, zasazením do kontextu, doplněním do pomyslné mozaiky chcete-li, jím je dodáno důležitosti a rázem se stane z člověka plnohodnotná digitální osobnost, která stejně jako v reálnem životě má své zvyky, charakteristické rysy, oblíbené věci a slabosti. Do nedávna tyto střípky informací znala pouze druhá strana, se kterou jsme vedli konverzaci. V poslední době se však o tyto věci, nepřímo a mimovolně dělíme i s dalšími stranami. Tyto strany si díky pokročilým softwarům dokážou na rozdíl od mozku člověka daleko lépe zpracovat

jednotlivé dílky a vytvořit tak kompletní obrázek v řádu vteřin. Dokážou je také uchovat daleko déle a využít k všemožným účelům.

Tím hlavním však zůstává generování zisku. Představte si pokladní v obchodě, která o Vás ví vše a dokáže Vám nabídnout právě a jenom tu věc, kterou v danou chvíli potřebujete. Z mého pohledu ideální stav. Na tomto místě už je ale naivní si myslet, že obchod se točí pouze kolem potřeby. Do hry vstupují naše pocity, touhy a přání, které dokáže „paní pokladní“ podprahově použít a vyvolat v nás tak akci, určitou věc, či službu koupit, ačkoliv ji nutně nepotřebujeme. Ideálním stavem je pak dostat člověka do konzumního kolečka. Tedy konzumace reklam, které mu jsou specificky vybrány a následně zakoupení produktu nebo služby, přičemž příštím nákupem a kliknutím na reklamu se kolo roztáčí a přichází další dílek informace o osobě, která nakoupila.

Historicky byl obchod doménou pouze lidí, kteří svými znalostmi a dovednostmi dokázali svému zákazníkovi něco prodat. V současné době jsou to již čím dál častěji lidmi naprogramované stroje, které prostřednictvím pokročilých algoritmů sbírají a vyhodnocují naše data, která následně používají, aby nám nabídli co nejvhodnější produkt, jemuž nebude možné říci ne.

Pro tuto specifickou a nikdy nekončící formu hry tu máme ale naštěstí určitá pravidla, která by nás měla oproti negativním vlivům třetích stran efektivně chránit a pro nás jako koncové uživatelé přinášet pouze užitek. Zdali jsou aktuální právní normy efektní pro naši ochranu soukromí budu mimo jiné přibližovat v této diplomové práci.

První kapitola této diplomové práce se zaměřuje na definici základních pojmů patřících do tématu ochrany osobních, lokalizačních a provozních údajů. Dále nastiňuje pojmy úzce spojené s tématem, jako např. data retention. Základním údajům přiřazuje zákonnou definici a praktické příklady pro lepší představu pojmů. Jako hlavní zdroj pro první část slouží SOOUSEK a GDPR.

Druhá kapitola se věnuje specificky sítím elektronických komunikací. Obsahuje definice základních pojmů, při kterých se opírá převážně o Zákon o elektronických komunikacích. Postupně vymezuje samotnou síť elektronických komunikací až po elektronické komunikační zařízení. Poslední pododdíl jde více na povrch a pojednává o soukromí v těchto sítích.

Třetí kapitola pokrývá historii vývoje ochrany osobních údajů. Nejprve se zaměřuje na ochranu osobních údajů v obecném smyslu, následně vývojem ochrany

osobních údajů na území ČR a konečně historickým vývojem GDPR, přičemž bere na zřetel hlavní milníky a dokumenty.

Čtvrtá kapitola představuje ochranu osobních údajů v EU. Stěžejním dokumentem pro tuto část je Obecné nařízení o ochraně osobních údajů. Kapitola rozebírá předmět GDPR, principy a práva. V posledních podkapitolách přináší pohled na slabé stránky nařízení společně s regulačními přínosy pro firmy.

Pátá kapitola se zaměřuje na podnikání s osobními daty. Popisuje, jaká je hodnota dat v dnešní době, jak se s nimi nakládá, jak se analyzují a k čemu jsou firmám ku prospěchu. Dále pak vysvětluje pojem big data a ukazuje, jaké typy obsahu shromažďuje Facebook. Konec kapitoly se zabývá výhodami a nevýhodami obchodu s daty.

Šestá kapitola se věnuje počítačové kriminalitě. Definuje základní pojmy s ní spojené a finálně se zaměřuje na trestnou činnost úzce spojenou s osobními údaji, tedy na krádež identity a formy podvodného získávání osobních údajů.

Sedmá závěrečná kapitola plní úlohu lidskoprávní, přičemž se v převážné většině věnuje právu na soukromí, které rozebírá v několika rovinách. Na samotném konci se poté věnuje i svobodě projevu nebo právu na informace ve světle GDPR.

Cílem této diplomové práce je tedy zprvu definování základních pojmů pro následnou analýzu současného stavu ochrany osobních, lokalizačních a provozních údajů, poskytnutí historické perspektivy jejího vývoje a zprostředkování nového pohledu na efektivitu aktuálních norem v souvislosti s ochranou našeho soukromí.

Výzkumné otázky, na které budu prostřednictvím této práce hledat odpověď: Co jsou osobní, provozní a lokalizační údaje? Jaký je aktuální stav ochrany osobních, lokalizačních a provozních údajů? Jaký je historický vývoj ochrany osobních dat? Je současná právní úprava dostatečná pro účinnou ochranu našeho soukromí? Jakým způsobem se vydělává na těchto datech? Co je GDPR, k čemu slouží a jak se zvýšila ochrana dat od jejího zavedení? Co je to počítačová kriminalita a jak dochází k zneužívání našich osobních dat?

1 Osobní, provozní a lokalizační údaje

1.1 Osobní údaj

Abychom mohli problematiku ochrany údajů v sítích elektronických komunikací patřičně uchopit a v pozdější fázi práce se dostali i k úvahám o budoucnosti ochrany dat, začneme tím zásadním, tedy základním vymezením důležitých pojmů. Tím, z mého pohledu nejdůležitějším, je osobní údaj. Osobním údajem se rozumí *„veškeré informace o identifikované, nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“.[1]

Z výše uvedené definice tedy vyplývá, že osobní údaje se týkají pouze fyzických osob. Takovou fyzickou osobou, k níž se určité osobní údaje vztahují, označujeme pojmem *subjekt údajů*. Dále pak máme *identifikátory*, tedy informace, které mohou danou fyzickou osobu identifikovat. Důležitou roli pro to, abychom mohli v určitém případě mluvit o osobním údaji, je existence vazby mezi konkrétní osobou a identifikátorem. Zdali je určitá informace schopna nás identifikovat, záleží tedy zpravidla na kontextu. Třeba v případě samotného jména a příjmení Jakub Šindelář, se jedná o identifikátor, nikoliv však ještě o osobní údaj. V případě, kdy můj zaměstnavatel např. oznámí mým kolegům, že dostanu finanční bonus, a jsem ve firmě jediný s tímto jménem a příjmením, půjde o osobní údaj. Nejde pouze o Jakuba Šindeláře, ale o Jakuba Šindeláře pracujícího pro specifickou firmu. Máme zde tedy navíc informaci, která plyne z kontextu a je kompetentní identifikovat konkrétní osobu.[2]

1.2 Zvláštní osobní údaje

[1] Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 1.
[2] Fiala, O., Grepl J., Lichnovský, O. GDPR. Hmotné a procesní aspekty prakticky 1. vydání, Praha: C. H. Beck, 2019, str. 1-2.

Narozdíl od výše uvedených „klasických“ osobních údajů, které jsou definovány velice široce. To, co může představovat náš osobní údaj, je široká škála různých informací. U zvláštních osobních údajů tomu tak není a jako zvláštní označujeme jen údaje, *„které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.*“[3] Dalším rozdílem je pak vyšší ochrana těchto citlivých údajů oproti těm „klasickým“. Projevuje se zejména v přísném režimu jejich zpracování, jež lze provádět pouze na základě čl. 9 odst. 2 písm. a) až j) GDPR. V jiných případech než v těchto uvedených, se zpracování zvláštních kategorií osobních údajů zakazuje.[4]

1.3 Pseudonymizace

Za určitou formu kryptografie můžeme považovat proces „pseudonymizace“ osobních údajů, skrze který se kupříkladu jménu a příjmení přidělí určitá šifra, která sama o sobě nemá žádný význam a je nečitelná. Pouze za použití dodatečných informací, tzv. klíče, lze určitá informace přiřadit konkrétnímu subjektu. Tyto dodatečné informace jsou navíc uchovávány odděleně a pod technickými a organizačními opatřeními. Na rozdíl od anonymizace je tedy proces pseudonymizace procesem vratným.[5]

Pseudonymizace má za cíl zvýšit ochranu subjektů osobních údajů a celkově úroveň zabezpečení ochrany osobních údajů. Slouží tedy v zásadě k vyvažování rizika, které je v dnešní době, kvůli pokročilým technologiím, a kvůli lidem motivovaným data zneužít, a také kvůli stoupající hodnotě samotných dat, stále vyšší.[6]

[3] Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 1.
[4] Fiala, O., Grepl J., Lichnovský, O. GDPR. Hmotné a procesní aspekty prakticky 1. vydání, Praha: C. H. Beck, 2019, str. 2-3.
[5] Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 5.
[6] Obecné nařízení o ochraně osobních údajů, recitál 26, 28.

1.4 Data retention a komunikace

Pojem „data retention“ v jednoduchosti znamená shromažďování určitých metadat (provozních a lokalizačních údajů) o komunikaci skrze elektronické komunikační prostředky. Data retention si klade za cíl zajistit jejich zpětnou dostupnost v případě potřeby, kterou může být např. trestní řízení.[7] Na rozdíl od osobní komunikace ve fyzickém světě je komunikace v elektronických sítích specifická tím, že její průběh je realizován třetí stranou (provozovatelem určité služby, tedy tzv. operátorem, který přenese obsah zprávy skrze svoji technologii). Každá tato komunikace generuje data potřebná pro její samotnou realizaci (kdy, kde a jak někdo někomu něco komunikoval) a obsahuje i specifický obsah komunikace (co kdo komu komunikoval). Metadata potřebná pro zprostředkování komunikace může za určitých pravidel operátor zpracovávat, obsah komunikace nikoliv. Operátor musí tedy zajistit důvěrnost komunikace a postarat se o to, aby obsah komunikace nezpracoval nikdo jiný.[8]

1.5 Provozní údaje

Provozní údaje definuje zákon o elektronických komunikacích následovně: *„Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.“*[9] Co provozní údaje ale mohou zahrnovat se dozvíme v recitálu č.15 SOOUSEK[10] *„informace o názvech, číslech nebo adresách, které poskytuje odesílatel sdělení nebo uživatel spojení za účelem přenosu sdělení“*[11], jedná se tedy o *„jakýkoli převod těchto informací sítí, po které se sdělení přenáší, za účelem provedení přenosu.“* [12] Do provozních údajů lze tedy mimo jiné zahrnout: „*údaje vztahující se ke směrování, délce trvání, času nebo objemu sdělení, použitému protokolu, umístění koncového zařízení odesílatele či příjemce, síti, ze které sdělení pochází či na které končí, a*

[7] MYŠKA, Matěj. Právní aspekty uchovávání provozních a lokalizačních údajů. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2013, str. 17.
[8] Ibidem, 17-18.
[9] Zákon o elektronických komunikacích, §90 odst. 1.
[10] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). Dále jen SOOUSEK.
[11] SOOUSEK, recitál č.15.
[12] Ibidem, recitál č.15.

počátku, konci či délce trvání spojení. Mohou také zahrnovat formát, ve kterém je sdělení sítí přenášeno“[13]

Jak bylo zmíněno v minulé kapitole, není možné zpracovávat metadata o provozu komunikace a obsah komunikace, jelikož máme každý své právo na soukromí. V současné době je možné pouze na základě provozních dat spolehlivě zmapovat soukromý život subjektu, aniž by bylo zapotřebí nabourávat obsah komunikace. Lze zjistit, co a kdo navštěvuje za internetové stránky, s kým se kdo baví a kam kdo chodí. Na základě těchto na první pohled poněkud nezávažných dat lze na základě jejich historie zjistit vzorce chování, pravidelné zvyky a třeba i předpovídat jeho chování do budoucna.[14] Tyto a jiné problematiky týkající se sběru metadat o komunikaci si rozebereme ještě v dalších kapitolách.

1.6 Cookies

Jednou z technologií, která o nás sbírá informace na webových stránkách, jsou tzv. cookies. Přesněji řečeno jsou jedním z tzv. „*síťových identifikátorů“*. Webové stránky si postupem času, podle toho, jak se chováme na určité stránce, ukládají malé soubory do našeho počítače. Díky těmto souborům je uživatelům internetových stránek ulehčeno např. přihlašování nebo prohlížení, jelikož je již toto přednastavení uloženo v našem počítači.[15]

Patří k oprávněným nástrojům a jejich použití je povoleno za splnění podmínky: „že uživatelé jsou jasně a přesně informováni v souladu s ustanovením směrnice 95/46/ES o účelu "cookies" či podobných nástrojů a je zajištěno, aby uživatelům byly známy informace, které se ukládají do koncového zařízení, jež používají.“[16] V případě cookies platí možnost odmítnout používat tento nástroj.

Toto odmítnutí dává největší smysl zejména v případech, kdy ke koncovému zařízení má přístup vícero lidí, jako např. v internetové kavárně. Možnost odmítnout poté trochu ztrácí na vážnosti zejména v takových případech,

[13] Ibidem, recitál č.15.
[14] MYŠKA, Matěj. Právní aspekty uchovávání provozních a lokalizačních údajů. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2013, str. 22-23.
[15] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 11.
[16] SOOUSEK, recitál č. 25.

kdy je souhlas s použitím cookies spojen i se samotným přístupem k obsahu na určité webové stránce.[17]

1.7 Lokalizační údaje

Lokalizační údaje definuje opět SOOUSEK a sice jako *„jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací“*[18] Lokalizační údaje se pak mohou týkat věcí vymezených v recitálu č.14, konkrétně tedy *„zeměpisné šířky, délky a nadmořské výšky koncového zařízení účastníka, směru pohybu, úrovně přesnosti lokalizačních informací, identifikace síťové buňky, ve které je koncové zařízení umístěno v určitém časovém bodu, a časového úseku, ve kterém byla lokalizační informace zaznamenána“*[19]

1.8 Biometrické údaje

Biometrické údaje jsou definovány jako osobní údaje technického charakteru, které představují technické zpracování fyzických a fyziologických znaků fyzické osoby, čímž umožňují jeho identifikaci. Typickým příkladem biometrického údaje je např. otisk prstu, snímek obličeje, vzor oční duhovky či sítnice, geometrie ruky, vzorek genetického materiálů, anebo podpis.[20]

Pojem biometrický údaj pochází z řeckého slova „bios”, v překladu „život”, a „metron”, neboli „změřit”. Biometrické údaje tak představují určitým způsobem změřené biologické, anatomické, fyziologické, či behaviorální vlastnosti člověka. Od počátku věků patří mezi základní charakteristiku sloužící k rozpoznávání jednotlivců jejich obličeje. Ovšem s rostoucí populací bylo nutné nacházet nové způsoby sloužící k identifikaci. První biometrické údaje představovaly především otisky prstu, kterým si lidé dříve označovali autorství svých jeskynních maleb, jsou staré až několik desítek tisíc let. Otisky prstu ovšem hrály důležitou úlohu také ve

[17] SOOUSEK, recitál č. 25.
[18] Ibidem, čl. 2 písm c).
[19] Ibidem, recitál č.14.
[20] Biometrické údaje | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. [cit. 15.03.2022]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/biometricke-udaje/.

starověku, kdy se používaly jako forma stvrzení obchodní transakce na hliněných deskách.[21]

Jedinečnost biometrických údajů spočívá v tom, že s velmi vysokou přesností dokáže rozpoznat mezi jedním a druhým člověkem. V roce 1892 došlo k první kalkulaci pravděpodobnosti dvou shodných otisků prstů ve společnosti, kdy celosvětová populace čítala okolo 1.6 miliardy obyvatel. Závěr měření byl takový, že pravděpodobnost shody mezi dvěma jednotlivci se pohybuje okolo 1:64000000.[22]

Kromě klasického využití biometrických údajů v kriminalistice, kde mimo jiné slouží například k určení totožnosti neznámé osoby, se biometrické údaje používají také např. v docházkových systémech, a v posledních letech strmě roste také jejich využití na internetu. Tam biometrické údaje slouží k tzv. autentizaci, tedy prokázání totožnosti konkrétního uživatele. Mezi otisky prstů se také v posledních letech zařadilo snímání obličeje uživatele, který slouží jako ověření totožnosti, a užívá se kromě odemknutí telefonu také k verifikaci online plateb, stahování aplikací apod. Snímání biometrických údajů o našem podpisu se mimo jiné využívá také v některých bankách, či u jiných poskytovatelů služeb jako náhrada vlastnoručního podpisu. Při sjednávání nových smluv tedy není potřeba osobní přítomnost jednotlivce, ale stačí, aby banka náš biometrický údaj vlastnila.[23]

Používání biometrických údajů s sebou ovšem nese také určitá rizika, která mohou ohrozit ochranu našeho soukromí. Biometrická verifikace je totiž založená na vzorku předložení biometrických dat. Abychom tedy získali přístup do mobilních aplikací, mobilního telefonu, či jiných internetových služeb na základě vlastních biometrických údajů, musíme tyto údaje nahrát do nějakého systému, jako např. Do datové schránky. Problém nastává ve chvíli, kdy z takové databáze naše biometrické údaje uniknou, jelikož údaje se můžou stát předmětem zneužití, aniž bychom o tom sami věděli. Kromě toho mohou některé biometrické údaje, jako například genetické údaje, také vypovídat o našem zdravotním stavu.[24]

---

[21] Biometrics News, Companies and Explainers | Biometric Update [online]. [cit. 15.03.2022]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2.
[22] STIGLER, STEPHEN, M. Perspectives; Galton and Identification by Fingerprintes. Statistics Department, Chicago. [online]. [cit. 15.03.2022]. Dostupné z: http://www.genetics.org/content/140/3/857.
[23] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 20.
[24] Ibidem, str. 21.

Právní úprava biometrického údaje, respektive jeho definice je zakotvena v čl. 4 odst. 14 GDPR, který říká, že: *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje"*[25]

Biometrický údaj spadá do zvláštní kategorie osobních údajů, a vztahují se na něj tak trochu jiná pravidla. Například platí obecný zákaz zpracování biometrických údajů, ovšem GDPR stanovuje i některé výjimky. Zpracování biometrických údajů např. podléhá explicitnímu souhlasu subjektu se zpracováním těchto osobních údajů. Ke zpracování může dojít také například v případě plnění povinností a výkonu práv v oblasti sociálního zabezpečení a sociálního práva, či v případě ochrany životně důležitých zájmů.[26]

[25] Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Čl. 4 odst. 14.
[26] NULÍČEK, MICHAL. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 162-169.

2 Sítě elektronických komunikací

2.1 Zákon o elektronických komunikacích

Pro potřeby lepší právní regulace současného rozvinutého telekomunikačního odvětví nahrazuje k 1. 5. 2005 zákon o elektronických komunikacích, dále jen ZEK, zákon předešlý, tedy zákon č. 151/2000 o telekomunikacích. Jak název napovídá, tento zákon neupravuje pouze telekomunikace, ale nově zahrnuje i komunikace elektronické a zapracovává do českého právního řádu nový regulační rámec EU týkající se elektronických komunikací. ZEK přináší tedy značnou pojmovou změnu a sice termín elektronické komunikace, který nahrazuje termín „telekomunikace“.[27]

ZEK upravuje jen podmínky podnikání, výkon státní správy a regulace trhu elektronických komunikací. Neobsahuje tedy poskytování samotných služeb uskutečňovaných skrze elektronické komunikace.[28]

2.2 Síť elektronických komunikací

Podíváme-li se do ZEK, zjistíme, že zákon pod tímto pojmem nerozlišuje např. mezi mobilní sítí, nebo internetem. Zákonná definice hledí na tyto sítě jako na stejné. Sítě el. komunikace jsou tedy definované následovně: *„přenosové systémy, bez ohledu na to, zda jsou založeny na trvalé infrastruktuře nebo jsou centralizovaně kapacitně řízené, nebo nikoli, a popřípadě i spojovací nebo směrovací zařízení a jiné prostředky, včetně neaktivních síťových prvků, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí okruhově nebo paketově komutovaných včetně internetu, mobilních sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na typ přenášené informace“.*[29]

[27] MAISNER, M., VANÍČEK, Z. Odpovědnost za obsah přenosu v elektronických komunikacích. Praha: Wolters Kluwer ČR, 2021. str. 7-9.
[28] VANÍČEK, Z. Zákon o elektronických komunikacích: Komentář, Praha: Linde Praha a.s., 2008.
[29] ZEK paragraf 2, odstavec 2, písm. b)

2.3 Veřejná komunikační síť

ZEK dále definuje také veřejnou komunikační síť následovně: „*síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání*“.[30] Jedná se tedy o síť, která je zcela nebo převážně využívána k poskytování veřejných služeb. Z užívání těchto služeb není nikdo předem vyloučen.

2.4 Služba elektronických komunikací

Službou elektronických komunikací se rozumí dle ZEK: *„služba obvykle poskytovaná za úplatu prostřednictvím sítí elektronických komunikací, která s výjimkou služeb poskytujících obsah přenášený prostřednictvím sítí a služeb elektronických komunikací nebo vykonávajících redakční dohled nad tímto obsahem.“*[31] Dále dle ZEK zahrnuje tato služba interpersonální komunikační službu, službu přístupu k internetu a služby spočívající v přenosu signálů např. poskytování komunikace mezi stroji a pro rozhlasové a televizní vysílání.[32]

2.5 Elektronické komunikační zařízení

Posledním pojmem, který bude pro účely této práce důležitým, je pojem elektronické komunikační zařízení, které ZEK definuje následovně jako: *„technické zařízení pro vysílání, přenos, směrování, spojování nebo příjem signálů prostřednictvím elektromagnetických vln.“*[33] V praxi si lze takovéto zařízení představit jako mobilní telefon, počítač či televizi.

[30] ZEK paragraf 2, odstavec 2, písm. d).
[31] Ibidem, paragraf 2, odstavec 3, písm. a).
[32] Ibidem.
[33] Ibidem, paragraf 2, odstavec 2, písm. c).

2.6 Soukromí v elektronických komunikacích

Naše soukromí na internetu chrání kromě ochrany osobních údajů a ochrany osobnosti také právní úprava elektronických komunikacích, v rámci které je asi nejvýznamnějším předpisem již zmiňovaná směrnice o soukromí a elektronických komunikacích. Tato směrnice se zabývá riziky elektronické komunikace ve vztahu k ochraně osobních údajů a základních lidských práv a svobod. Směrnice nařizuje poskytovatelům veřejných služeb elektronických komunikací co nejvíce a nejlépe zabezpečit sítě elektronických komunikací a jejich důvěrnost.[34]

Český právní řád tyto povinnosti stanovuje v zákoně č. 127/2005 Sb., o elektronických komunikacích stanovuje v § 97 odst. 3 následovně: *„právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, je povinna uchovávat provozní a lokalizační údaje, a tyto údaje je na požádání povinna poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu. Rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců, a formu a způsob jejich předávání orgánům oprávněným k jejich využívání, stanoví prováděcí právní předpis.“*

Tato přijatá směrnice Evropského parlamentu a Evropské rady č. 2002/58 byla přijata v návaznosti na události 11. září 2001, kdy došlo k útoku na budovu Světového obchodního centra a Pentagonu. Tato situace urychlila diskuze o nutných právních změnách v oblasti uchovávání a poskytování provozních a lokalizačních údajů.[35] Nově přijatá směrnice členským státům deklarovala možnost zavedení legislativního opatření umožňujícího držet data po určitou dobu z následujících důvodů: *„zajištění národní bezpečnosti, obrany, veřejné bezpečnosti, a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému.“*[36] Právo, které směrnice stanovila, jak je už z uvedené citace očividné, je poměrně nekonkrétně formulováno, což později způsobovalo potíže zákonodárcům jednotlivých členských států.

[34] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 77.
[35] MYŠKA, Matěj. Právní aspekty uchovávání provozních a lokalizačních údajů. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2013, str. 34-35.
[36] SOOUSEK, článek 15, odst. 1.

Taková právní úprava je pro zajištění našeho soukromí na internetu ohromně důležitá, a to hlavně z toho důvodu, že velká část internetové komunikace probíhá v nezašifrované podobě, což by v nezabezpečené počítačové síti mohlo vést k zásahu třetí osoby, která by tak získala přístup k obsahu komunikace. Kromě toho také zákon o elektronických komunikacích zakazuje odposlech, ukládání zpráv, anebo jiné způsoby zachycení či sledování zpráv a spojení bez souhlasu dotčených uživatelů. Výjimku ze zákazu odposlechů ovšem stanovuje § 88 trestního řádu, který v případě vedení trestního řízení pro zločin, pro nějž zákon stanoví trest odnětí svobody v minimální délce osm let, říká, že: *„může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené."* Dále například v případě, že dojde ke spáchání trestného činu zneužití postavení úřední osoby dle § 329, může Policie České republiky sledovat určené telefonní číslo či IP adresu zařízení a to až po dobu čtyř měsíců.[37]

Další z povinností, kterou zákon o elektronických komunikacích ukládá poskytovatelům elektronických služeb, je informovat své zákazníky o ukládání dat na naše zařízení a o přístupu k těmto datům. K tomu slouží již dříve zmíněné cookies, které jsou upozorněním na různých internetových stránkách sloužící k tomu, aby poskytovatel dané služby od nás obdržel souhlas. Společně s tím je dalším projevem větší ochrany soukromí na internetu také zákaz zasílání tzv. spamů, neboli nevyžádaných obchodních sdělení, které vybízejí např. k návštěvě konkrétních internetových stránek. Zákaz zasílaní takových sdělení stanovuje opět zákon o elektronických komunikacích.[38]

V dubnu roku 2021 informoval Úřad pro ochranu osobních údajů České republiky o tom, že na půdě Evropského parlamentu, Rady Evropské unie a Evropské komise bude v následujícím roce probíhat trialog týkající se návrhu nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES. Nové nařízení Rady Evropské unie a Evropského parlamentu se týká určitých odchylek od znění původní směrnice 2002/58/ES, a to především v oblasti používání technologií poskytovateli interpersonálních komunikačních služeb

[37] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 78-79.
[38] Ibidem, strana 78-80.

nezávislých na číslech ke zpracování osobních a jiných údajů pro účely boje proti pohlavnímu zneužívání dětí na internetu. V novém návrhu směrnice je také obsaženo opětovné povolení výše zmíněných cookies, a to i přes negativní postoj Evropského sboru pro ochranu osobních údajů.[39]

[39] Úřad k návrhu nařízení o soukromí a elektronických komunikacích: Úřad pro ochranu osobních údajů: Titulní stránka [online]. [cit. 15.03.2022] Dostupné z: https://www.uoou.cz/urad-k-navrhu-narizeni-o-soukromi-a-elektronickych-komunikacich/d-49300.

3 Historický vývoj ochrany osobních údajů

Ochrana soukromí, včetně ochrany osobních údajů, je ve světě přítomna téměř od nepaměti. Těmi největšími impulsy, které vedly k větší ochraně osobních údajů a ke střežení si svého soukromí, byly různé náboženské války, rozsáhlé revoluce, jako např. Velká francouzská revoluce, a genocidy společně s uplatňováním různých rasových zákonů. Po takových událostech bylo jasné, že osobní údaje, jež jsou jakýmkoliv způsobem zneužity státem, můžou vést k ohrožení, ba dokonce ztrátě života vlastního i svých blízkých. Ukázalo se, že zneužití natolik citlivých údajů, jako jsou informace o např. etnické, náboženské, rasové příslušnosti, či sexuální orientaci, můžou být velmi snadno, a v podstatě beztrestně, zneužity.[40]

Ještě více hrozeb a rizik do ochrany osobních údajů však přináší rychlý, a nezastavitelný rozvoj výpočetní techniky, která se zhruba od 70. let 20. století stala součástí našeho každodenního života. Osobní údaje začaly být v obrovském množství shromažďovány různými podnikatelskými subjekty, státními institucemi, a v neposlední řadě také sociálními sítěmi. Existence výpočetní techniky, a hlavně internetu, pak začala pro ochranu osobních údajů znamenat velké nebezpečí, jelikož začalo docházet k nezákonnému obchodování s osobními údaji, anebo k vytváření falešných identit. To vše opět bez větší právní kontroly.[41]

První zákonná opatření, která nějakým způsobem omezovala přístup k osobním údajům, vznikla v druhé polovině 18. století ve Švédsku. O pár let později, v roce 1789, došlo v době právě propukající Velké francouzské revoluce k vytvoření dokumentu zvaného Deklarace práv člověka a občana, který se stal základem pro určení lidských práv, jež jsou dnes zakotvena téměř ve všech ústavách na evropském a americkém kontinentu. Ačkoliv nikdy nenabyla právní závaznosti, inspirovala důležitým dokument vzniklý v roce 1948 zvaný Všeobecná deklarace lidských práv, která podle článku 12 deklarovala každému jedinci zákonnou ochranu proti svévolnému zasahování do soukromého života a proti útokům na svou čest a pověst. Doslovný obsah článku 12 pak převzal Mezinárodní pakt o občanských a politických právech, jež nabyl účinnosti roku 1976.[42]

[40] NAVRÁTIL., J. a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018, strana 26.
[41] Ibidem, strana 26.
[42] TÝČ, Vladimír. Česká republika a současný svět: (sborník dokumentů), Praha: Linde, 1998, str. 59-61.

Na počátku evropské integrace byla v roce 1950 na půdě Rady Evropy sjednána Evropská úmluva o ochraně lidských práv a základních svobod, jejímž hlavním cílem je ochrana těchto práv. Právo na ochranu soukromí, a osobních údajů, je pak popsáno v článku 8, který říká, že: *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. 2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."* [43]

První dokument, který komplexně řeší ochranu osobních údajů, a který poprvé definuje hlavní zásady ochrany osobních údajů, je Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, známá také pod názvem Úmluva č. 108, jež vyšla v platnost roku 1981. Ta říká, že je nutné: *„zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují."* [44]

Hlavním dokumentem, který v rámci Evropské unie upravoval způsob ochrany osobních údajů, byla až do roku 2018 směrnice Evropského parlamentu a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Ta především stanovovala jednotnou úpravu ochrany osobních údajů a jejich pohybu na území Evropského společenství, což mělo za následek i svobodný pohyb po zemích, jež jsou součástí tzv. Schengenského prostoru.[45] Kromě toho také směrnice určila požadavky na bezpečnost zpracovávání dat po technické stránce, zavedla povinnost oznamovat zpracování osobních údajů a stanovila vytvoření nezávislého dozoru nad dodržováním výše popsaných zásad, které každý členský stát Evropské unie musel povinně do tří let zařadit do své legislativy.[46] Tuto směrnici pak v roce 2018 nahradilo GDPR.

[43] TÝČ, Vladimír. Česká republika a současný svět: (sborník dokumentů), Praha: Linde, 1998, str. 66-70.
[44] Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI, 2008, str. 2-3.
[45] NAVRÁTIL., J. a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018, str. 29.
[46] Kučerová, A. a kol. Zákon o ochraně osobních údajů: komentář, 1. vydání. Praha: C.H. Beck, 2003, str. 351.

3.1 Historický vývoj ochrany osobních údajů v ČR

V České republice byla problematika ochrany osobních údajů dlouho řešena pouze ve spojitosti s vydáváním a držením cestovních dokladů. Více komplexní řešení ochrany osobních údajů se dostalo do popředí až v 90. letech 20. století. Prvním předpisem, který řeší otázku ochrany osobních údajů je zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl reakcí na výše zmíněnou evropskou Úmluvu 108. Zákon obsahoval základní definici toho, co to je osobní údaj, informační systém, či provozovatel informačního systému.[47]

Základní vymezení ochrany soukromí a osobních údajů také upravuje Ústava České republiky, konkrétně tedy její součást Listina základních práv a svobod, jak bylo zmíněno výše. V rámci příprav vstupu České republiky do Evropské unie vstoupil v platnost zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl v souladu s výše zmíněnou evropskou směrnicí 95/46/ES. Jako dohlížitel byl zřízen Úřad pro ochranu osobních údajů. Ten dozoruje dodržování plnění tohoto zákona, konkrétně: *„vedení registru povolených zpracování osobních údajů, přijímání podnětů a stížností na porušení zákona, poskytování konzultací, legislativních aktivit a zajišťování plnění požadavků vyplývajících z mezinárodních smluv a v neposlední řadě také přednáškové a osvětové činnosti."*

Od května roku 2018 je pak v plném rozsahu v České republice platné Obecné nařízení o ochraně osobních údajů, tedy GDPR, na jehož základě byl v březnu roku 2019 schválen zákon č. 110/2019 Sb., o zpracování osobních údajů.[48]

3.2 Historický vývoj právní úpravy GDPR

Obecné nařízení o ochraně údajů, zkráceně GDPR, které vychází z původní směrnice Evropské unie o ochraně osobních údajů, bylo v rámci EU přijato v roce 2016, a od roku 2018 je platné ve všech dnes už 27 členských státech, kde se jím musí řídit každá organizace, obec, instituce, škola, či jakékoliv jiné zařízení a společnost, které ukládá nebo zpracovává osobní údaje. Zavedením GDPR se tak Evropská unie snažila reagovat na neustále postupující digitalizaci a kybernetizaci,

[47] Janečková, E., Bartík, V. Ochrana osobních údajů v pracovním právu: (Otázky a Odpovědi). 1. vydání. Praha: Wolters Kluwer Česká republika, 2016, str. 13.
[48] Ibidem, strana 9.

jelikož krádež osobních údajů je hlavním problémem kybernetické bezpečnosti, které nejen členské státy Evropské unie v posledních letech čelí stále výrazněji.[49]

V současnosti je GDPR nejvíce komplexní zákonná norma snažící se chránit soukromí občanů. Jak bylo zmíněno výše, vychází z původní směrnice EU o ochraně osobních údajů, jež existuje více než 20 let, a která zmiňovala minimální podobu zákona o ochraně údajů v členských státech EU. S rychlým vývojem technologií musí dojít také k úpravě právních norem. Debata o revizi stávající směrnice začala na půdě Evropské komise okolo roku 2009, kdy se konala konference věnovaná využití a ochraně osobních údajů a zkoumání nových trendů týkajících se ochrany soukromí. V návaznosti na to pak vzniká nová strategie Evropské unie týkající se ochrany dat jednotlivců, včetně právní vymahatelnosti. V listopadu roku 2011 pak člen německého sdružení pro ochranu údajů oznamuje, že Evropská komise má v plánu zavést nařízení, jež bude aplikovatelné ve všech členských státech EU, jejichž vlastní zákony na ochranu osobních údajů bude tak harmonizovat.[50]

Na počátku roku 2012 pak Evropská komise navrhla komplexní reformu pravidel EU ochrany osobních údajů, která byla nutná v rámci postupujícího technologického pokroku a globalizace. Na nutnost zlepšení směrnice a upozorňovala také studie zvaná „Reforming the Data Protection Package", kterou pro Evropský parlament vypracovala polská advokátní kancelář ve spolupráci s německými akademiky z Evropského institutu právních studií. Nový a jednotný zákon o ochraně osobních údajů pro členské státy Evropské unie je vyžadován také z důvodů vytvoření prostoru pro růst jednotného digitálního trhu, na kterém by pak mohli evropské podniky participovat bez toho, aby jakkoliv ohrožovali data o svých spotřebitelích.[51]

K částečné shodě na konkrétní podobě návrhu nařízení o ochraně osobních údajů se na půdě Evropského parlamentu rodí během roku 2014, kdy parlament vyjadřuje hlasováním novému GDPR silnou podporu, což otevírá cestu pokroku v reformě ochrany osobních údajů. Po počátečních neshodách mezi Německem, Spojeným královstvím a Francií to vypadá, že bude vypracování finální podoby GDPR zpomaleno, ale obecné shody nad GDPR pak Rada EU dosahuje už v červnu 2015. Nakonec 17. prosince 2015 schvaluje Výbor pro občanské svobody,

[49] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 13.
[50] Ibidem, strana 15.
[51] Ibidem, strana 16.

spravedlnost a vnitřní věci Evropského parlamentu výsledek jednání o obecném nařízení o GDPR, jež bylo schválenou převážnou většinou se 48 hlasy pro. GDPR, tedy Nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, pak oficiálně vstupuje v platnost 27. dubna 2016, jež nabývá účinnosti v květnu roku 2018.[52]

[52] The History of the General Data Protection Regulation | European Data Protection Supervisor. Redirecting to https://edps.europa.eu/_en [online]. [cit. 20.03.2022]Dostupné z: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

4 Ochrana osobních údajů v EU

Fundamentálním základem GDPR, je právo na ochranu osobních údajů, jak je potvrzeno v preambuli. Právo na ochranu osobních údajů však není absolutním právem a musí být proporcionálně vyváženo s ostatními právy a zájmy. [53] GDPR v 6. bodě odůvodnění konstatuje nárůst zpracování údajů v důsledku rozšiřování technologií, ale zároveň zdůrazňuje potřebu. „silnějšího a soudržnějšího rámce ochrany údajů podpořeného důrazným prosazováním“.[54]

Ochrana osobních údajů je základním právem stanoveným v čl. 8 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“) a v čl. 16 odst. 1 Smlouvy o fungování Evropské unie (dále jen „SFEU“).[55] Dříve byla zavedena prostřednictvím směrnice o ochraně údajů.[56] V době rychlého a globálního rozvoje technologií se však objevily nové výzvy týkající se ochrany osobních údajů a vzrostla potřeba posílit ochranu integrity fyzických osob.[57] Výsledkem byla reforma ochrany osobních údajů, která zavedla GDPR, jež vstoupilo v platnost 25. května 2018. Cílem nařízení bylo posílit práva subjektů údajů ve vztahu ke správcům údajů, kteří zpracovávají jejich osobní údaje, ale také učinit krok vpřed v rámci strategie jednotného digitálního trhu - zvýšit důvěru v digitální služby a jejich bezpečnost v EU, aby se umožnil rozvoj digitální ekonomiky na celém vnitřním trhu.[58] Přechodem od směrnice k nařízení došlo k větší harmonizaci právních předpisů členských států v oblasti ochrany údajů a ke kodifikaci ustálené judikatury EU.[59]

4.1 Předmět GDPR

GDPR se vztahuje na osobu nebo skupinu osob, které zpracovávají osobní údaje. Správný termín používaný v GDPR je správce osobních údajů, což je ta

[53] Obecné nařízení o ochraně osobních údajů, recitál 1 a 4.
[54] Ibidem, recitál 7.
[55] Ibidem, recitál 1.
[56] 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.
[57] Obecné nařízení o ochraně osobních údajů, recitál 6.
[58] Ibidem, recitál 7.
[59] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 13-14.

fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.[60] Subjektem GDPR je také zpracovatel osobních údajů, což je osoba, která zpracovává osobní údaje jménem správce.[61] Pokud správce údajů využívá zpracovatele, například společnost pro průzkum trhu nebo mzdovou společnost, GDPR vyžaduje, aby mezi nimi byla uzavřena smlouva nebo jiný právní akt upravující předmět ochrany.[62] Proto je v každém případě nezbytné analyzovat vztah mezi správcem a potenciálním zpracovatelem, aby bylo možné určit, kdo bude odpovědný za dodržování GDPR, které vnitrostátní právo se použije a který orgán pro ochranu údajů bude dodržování sledovat. Role zúčastněných subjektů však mohou být složité, protože často existuje mnoho subjektů, které zpracovávají tytéž osobní údaje současně nebo společně. Za účelem vyjasnění definic a rolí přijala pracovní skupina podle článku 29 v roce 2010 stanovisko k pojmu správce a zpracovatel osobních údajů.[63] Ve stanovisku se uvádí, že pojem správce je autonomní, což znamená, že by měl být vykládán především podle práva na ochranu údajů a v tom smyslu, že má rozdělit odpovědnost tam, kde je faktický vliv, a to na základě věcné, nikoli formální analýzy. Koncept správce charakterizují tři hlavní stavební prvky, a to osobní aspekt, možnost pluralitního řízení a základní prvky, které správce odlišují od ostatních aktérů.[64]

Osobní aspekt („fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt“) se zaměřuje na to, kdo může být správcem ze subjektivního hlediska. Z široké definice, jako je „jakýkoli jiný subjekt“, lze vyčíst, že se snaží pokrýt všechny vlivné subjekty na trhu. Ve stanovisku se uvádí, že je důležité se co nejvíce přiblížit praxi zavedené ve veřejném i soukromém sektoru v jiných oblastech práva, jako je občanské, správní a trestní právo.[65]

Možnost pluralitní kontroly („která se provádí samostatně nebo společně s jinými subjekty“) má za cíl chránit osobní údaje v případech, kdy se na zpracování těchto údajů podílí více subjektů bez ohledu na to, zda tyto operace probíhají současně nebo v různých fázích.[66]

[60] Obecné nařízení o ochraně osobních údajů, článek 4, odstavec 1.
[61] Ibidem, článek 4, odstavec 8.
[62] Ibidem, článek 28, odstavec 3.
[63] NAVRÁTIL., J. a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018, strana 99-101.
[64] Ibidem.
[65] Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“, strana 15.
[66] Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“, strana 17 a násl.

Základní prvky, které odlišují správce od ostatních subjektů („určuje účely a prostředky zpracování osobních údajů“), určují, jaká osoba může být správcem. Účely zpracování se týkají konkrétních, výslovných a legitimních rozhodnutí učiněných v souvislosti se zpracováním údajů. Ten, kdo tato rozhodnutí přijímá, je de facto kontrolor. Způsob zpracování se týká spíše technických nebo organizačních otázek, jako je rozhodnutí o tom, které údaje budou zpracovávány, které třetí strany budou mít k údajům přístup, jak dlouho budou údaje uchovávány nebo jaký hardware či software bude použit. Celkově správce rozhoduje o tom, proč a jakým způsobem se jednotlivé činnosti zpracování provádějí. Při určování toho, kdo je kvalifikován jako správce, lze analyzovat otázky, jako například „zpracovávala by externí společnost údaje, kdyby ji o to správce nepožádal?“ nebo „měl by dodavatel vliv na účel a prováděl by zpracování také ve svůj prospěch?“ Z tohoto hlediska je dobře možné, že technické a organizační prostředky určuje výhradně zpracovatel údajů.[67]

4.2 Principy zpracování osobních údajů

Při určování toho, zda je činnost zpracování zákonná a v souladu s GDPR, je třeba vzít v úvahu několik kroků. Zaprvé, zpracovávané údaje musí být osobní.[68] Za druhé, zpracování musí být zákonné.[69] Za třetí, zásady týkající se zpracování musí být splněno.[70] Za čtvrté, musí být splněna práva subjektu údajů (včetně povinností, které vyplývají pro správce a zpracovatele).[71] Konečně za páté je třeba zajistit bezpečnost osobních údajů.[72]

4.2.1 Zásada zákonnosti

Při zpracování osobních údajů je správce odpovědný za to, že tak činí alespoň na základě jednoho zákonného důvodu. Zpracování je zákonné, pokud a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden nebo

[67] Stanovisko 1/2010, strana 12 a násl.
[68] Obecné nařízení o ochraně osobních údajů, článek 4, odstavec 1.
[69] Ibidem, článek 6.
[70] Ibidem, článek 5.
[71] Ibidem, články 12-23.
[72] Ibidem, článek 32.

více konkrétních účelů (souhlas), b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro přijetí opatření na žádost subjektu údajů před uzavřením smlouvy (smlouva), (c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje (právní povinnost), d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (životně důležité zájmy), (e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce (veřejný zájem), nebo f) zpracování je nezbytné pro účely oprávněných zájmů správce nebo třetí strany, s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů, zejména pokud je subjektem údajů dítě (oprávněné zájmy).[73]

4.2.2 Principy transparentnosti a účelnosti

Článek 5 GDPR objasňuje zásady zpracování osobních údajů. GDPR vyžaduje, aby zpracování probíhalo transparentním způsobem.[74] Za druhé omezuje uchovávání osobních údajů „v identifikovatelné podobě po dobu ne delší, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány“, s výjimkou archivace ve veřejném zájmu, pro výzkum a pro statistické záznamy, pokud jsou náležitě zabezpečeny.[75] Zatřetí je správci uložena povinnost odpovědnosti, aby zajistil a prokázal dodržování všech zásad zpracování osobních údajů.[76] Správce je osoba nebo subjekt, který má pravomoc rozhodovat o účelu a „prostředcích zpracování osobních údajů“, a to sám nebo s jinými osobami.[77] V 39. bodě odůvodnění se rovněž dodává, že osobní údaje by měly být zpracovávány pouze tehdy, „pokud účel zpracování nelze rozumně splnit jinými prostředky“.

[73] Obecné nařízení o ochraně osobních údajů, článek 6, odstavec 1.
[74] Ibidem, článek 5, odstavec 1, písm. a).
[75] Ibidem, článek 5, odstavec 1, písm. e).
[76] Ibidem, článek 5, odstavec 2.
[77] Ibidem, článek 4, odstavec 7.

4.3 Práva subjektů GDPR

Tyto zásady se odrážejí a jsou konkrétněji vyjádřeny v následujícím souboru práv subjektu údajů. Subjekt údajů má právo získat informace o zpracování svých osobních údajů bez ohledu na to, odkud byly tyto údaje získány.[78] Toto právo odráží zásadu transparentnosti a poskytuje subjektu údajů větší kontrolu nad jeho údaji. Subjekt údajů má rovněž právo na přístup k těmto údajům, a to tak, že získá kopii zpracovávaných osobních údajů.[79] Pokud jsou osobní údaje nepřesné, má subjekt údajů právo na opravu, což znamená, že tyto údaje musí být doplněny.[80] Právo na omezení zpracování umožňuje subjektu údajů v některých případech omezit zpracování jeho osobních údajů.[81] Subjekt údajů má také právo na výmaz, označované také jako právo být zapomenut, což znamená, že správce musí v některých případech vymazat osobní údaje, například pokud již nejsou potřebné ve vztahu k účelům nebo pokud subjekt údajů odvolá svůj souhlas.[82] Právo být zapomenut je jasným vyjádřením důležitosti zásad minimalizace a omezení ukládání údajů. Byla obsažena již ve směrnici o ochraně osobních údajů, kterou stanovil Soudní dvůr EU ve věci Google Spain, ale později byla kodifikována v GDPR.[83]

Pokud je zpracování založeno na souhlasu a prováděno automatizovanými prostředky, má subjekt údajů rovněž právo na přenositelnost údajů, což znamená, že správce je povinen poskytnout údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a předat tyto údaje jinému správci, a to přímo od jednoho správce k druhému, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.[84] A konečně, pokud jde o automatizované individuální rozhodování, profilování a přímý marketing, má subjekt údajů právo kdykoli vznést námitku proti takovému zpracování z důvodů týkajících se jeho konkrétní situace a nepodléhat rozhodnutí založenému výhradně na automatizovaném zpracování, které má pro něj právní účinky. Správce pak takové zpracování zastaví, pokud se neprokážou

[78] Obecné nařízení o ochraně osobních údajů, článek 12-14.
[79] Ibidem, článek 15.
[80] Ibidem, článek 16.
[81] Ibidem, článek 18.
[82] Ibidem, článek 17.
[83] C-131/12, Google Španělsko, 13. května 2014.
[84] Obecné nařízení o ochraně osobních údajů, článek 20.

oprávněné důvody pro zpracování, které převažují nad zájmy, právy a svobodami subjektu údajů.[85]

4.4 Slabé stránky GDPR

Přestože je GDPR chváleno jako komplexní a poskytující dostatečnou ochranu soukromí, byly zjištěny některé nedostatky. Kritizováno je především to, že je příliš složité, nesnadno srozumitelné, příliš zdlouhavé, těžkopádné a má vysoké náklady na dodržování předpisů a administrativu.[86] Uvádí se, že společnosti měly problémy s dodržováním složitých požadavků, protože nedokázaly plně porozumět pravidlům a výjimkám.[87] To je problematické, neboť nedodržení požadavků z důvodu složitosti pravidel by bylo v rozporu s cíli nařízení GDPR.

4.5 Přínos pro firmy a sankce

Když přemýšlíme o regulačních přínosech, většinou je spojujeme s makroekonomickými, sociálními přínosy a označujeme je za hlavní účel nebo cíl vládních zásahů na trhu. Společnost se domnívá, že existují oblasti, kde firmy musí změnit způsob své práce, aby dodržely regulační požadavky a přizpůsobily se vyššímu prospěchu. Obecně panuje také přesvědčení, že regulace je nezbytná pro správné fungování trhů.[88]

První intuitivní reakcí, když se zamyslíme nad tím, co regulace přináší podnikům, jsou náklady. Na druhý pohled však zjistíme, že GDPR může mít z pohledu firmy i mnoho pozitivních stránek. Sirota, generální ředitel společnosti BigID, píše: *„Je chybou, že firmy vnímají soulad s GDPR pouze jako finanční zátěž.*

[85] Obecné nařízení o ochraně osobních údajů, článek 21-22.
[86] EMOTA, „Lessons from Europe and Data Protection“ (Konference OSN o obchodu a rozvoji 2017) [online]. [cit. 23.03.2022]. Dostupné z: https://unctad.org/system/files/non-official-document/dtl_eWeek2017p13_OliverHateley_en.pdf.
[87] Philip Heijmans, „Getting the Business Over Data Privacy“ (US News, 1. srpna 2018) [online]. [cit. 23.03.2022]. Dostupné z: https://www.usnews.com/news/best-countries/articles/2018-08-01/across-europe-new-data-privacy-law-still-leaves-confusion.
[88] Ambler, T., Chittenden, F. & Bashir, A. (2019). Counting the Cost of EU Regulation to Business (Počítání nákladů na regulaci EU pro podniky). Evropský hospodářský a sociální výbor. [online]. [cit. 23.03.2022]. Dostupné z https://www.eesc.europa.eu/en/documents/counting-cost-eu-regulation-business.

Pochopení a ochrana dat zákazníků přináší skutečné výhody".[89] Zmiňuje mimo jiné výhody, jako je porozumění zákazníkovi, úspory z kybernetického pojištění a občanskoprávních žalob a ochrana pověsti značky.[90]

Jako hlavní přínos můžeme určitě zařadit vyhnutí se případným sankcím GDPR předepsaným pro firmy, které se požadavky nařízení neřídí.

Od samého počátku, kdy se GDPR dostalo do médií, byly sankce, které čekají na firmy, které nebudou GDPR dodržovat, označovány za klíčovou změnu GDPR oproti (v té době) stávající legislativě a za jeden z hlavních důvodů, proč se GDPR dostalo tolik pozornosti ze strany firem. Sankce jsou rozděleny do dvou skupin. Kritéria pro rozdělení vycházejí z nesouladu s ustanoveními nebo požadavky GDPR, které společnost neprovádí nebo neprovádí řádně. Pokuty jsou stanoveny pouze z hlediska jejich maximální výše, která činí: „správní pokuty až do výše 10 000 000 EUR, nebo v případě podniku až do výše 2 % celkového celosvětového ročního obratu za předchozí účetní období, podle toho, která částka je vyšší" a „správní pokuty až do výše 20 000 000 EUR nebo v případě podniku až do výše 4 % celkového celosvětového ročního obratu za předchozí účetní období, podle toho, která částka je vyšší".[91]

[89] Sirota, D. (2018, April 23). GDPR: Analýza nákladů a přínosů. [online]. [cit. 23.03.2022]. Dostupné z: https://www.informationweek.com/strategic-cio/security-and-risk-strategy/gdpr-a-cost-vs-benefit-analysis/a/d-id/1331616.
[90] Ibidem.
[91] Obecné nařízení o ochraně osobních údajů, článek 83, odstavec 5 a 6.

5 Data v podnikání

5.1 Hodnota osobních dat

Osobní údaje jsou dnes považovány za „zlato“ našeho digitálního věku, ve kterém vládnou nuly a jedničky.[92] Tuto skutečnost nelze popřít, protože firmy mezi sebou soutěží o to, která získá více osobních údajů. Čím více údajů společnost vlastní, tím větší moc získává. Proto více než kdykoli předtím získala online anonymita a zajišťování anonymity na významu.

Informace nebo údaje, které jsou předmětem boje o moc, se liší od údajů o chování spotřebitelů, jejich zájmech, zvyklostech při utrácení peněz, jako jsou typy produktů, které si lidé prohlížejí na internetu, nebo co kupují a čtou, o co se obecně zajímají, až po údaje o zdravotním stavu a politickém přesvědčení jednotlivce.[93] Tyto informace mohou být využity ve prospěch firem a k vypracování lépe přizpůsobených marketingových strategií nebo strategií rozvoje podnikání.

Informace o výdajových zvyklostech nebo zájmech mohou podnikům poskytnout jasnější představu o tom, na které lidi mají zaměřit své služby nebo produkty, stejně tak se mohou stát přínosnými i další informace. Dalším typem údajů, které lze pro tyto účely využít a které jsou poměrně oblíbené, jsou kontaktní údaje o osobě, například e-mail, telefonní číslo, jméno a příjmení.[94]

Výše uvedené údaje umožňují individuální zacílení prostřednictvím zasílání individuálních nabídek a nevyžádaných e-mailů za účelem prodeje produktů a služeb. „Odhadovaný ARPU[95] (průměrný příjem na uživatele) v digitální reklamě, kterou ovládají především společnosti Google a Facebook, dosáhl v roce 2017, 59 dolarů na osobu“[96], proto není divu, že existuje mnoho firem, které se spoléhají výhradně na shromažďování údajů a jejich prodej jiným společnostem, které je potřebují pro svůj rozvoj.

---

[92] Agentura Evropské unie pro kybernetickou bezpečnost, Hodnota osobních údajů. [online]. [cit. 23.03.2022]. https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data.
[93] Ibidem.
[94] Ibidem.
[95] Pozn. Average revenue per user.
[96] Agentura Evropské unie pro kybernetickou bezpečnost, Hodnota osobních údajů. [online]. [cit. 23.03.2022]. https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data.

Osobní údaje jsou velmi vzácným artiklem, který vytváří ekonomickou a ve výsledku finanční hodnotu pro celý digitální trh, konkrétně především pro různé online platformy. Díky tomu, že nadnárodní společnosti získávají takto zcela bezplatně, a kvůli našemu přičinění, naše osobní údaje, zvládají pomocí různých algoritmů cílit personalizované reklamy na naše konkrétní potřeby, což firmám umožňuje efektivně propagovat konkrétní výrobky, jež odpovídají našim zájmům. Pro firmy je tedy zisk osobních údajů důležitý pro maximalizaci svých online transakcí a zvýšení tržeb.[97]

Nařízení Evropské unie GDPR definuje osobní data jako všechny informace o identifikované nebo identifikovatelné fyzické osobě. Množství osobních dat, které lze považovat za ekonomické aktivum, každým rokem rapidně roste. Klíčovým problémem takto využívaných dat je především v tom, že jeho spotřebitelé si nejsou vědomi, jakým způsobem jsou informace o jejich osobě využívány. Nedostatečná ochrana osobních dat může vést k nerovnoměrné ekonomické výměně.[98]

Jedním z největších takových obchodníků s osobními daty jsou gigantické online platformy jako Facebook a Google. Za využívání obou těchto platforem, ostatně jako drtivé většiny dalších sociálních sítí a vyhledávačů, nemusí jejich spotřebitel nic platit, jejich zisky tedy plynou výhradně poskytování reklamy. Takové online platformy pak díky využívání online reklam umožňují firmám jejich výrobky nabízet pouze konkrétnímu publiku, které jim skrze jejich využívání poskytují osobní údaje týkající se věku, pohlaví, zájmů, anebo vlastní rodiny. V roce 2016 znamenala reklama pro firmu Google téměř 90 % veškerých příjmů.[99]

Pro to, aby online platformy byly schopné optimalizovat svou reklamu, je nutné, aby data poskytovaná jejich uživateli správně analyzovaly. Postupné zlepšování analýzy osobních dat, a vývoj nových a stále lepších a přesnějších algoritmů, vede ke zvyšování hodnoty našich údajů na internetu. Například v roce 2016 dosahovala finanční hodnota osobních údajů na Google zhruba 7 dolarů.[100]

[97] GDPR | Obecné nařízení o ochraně osobních údajů — prakticky. [online]. [cit. 23.03.2022] Dostupné z: https://www.gdpr.cz/blog/osobni-data-jako-vzacny-artikl/.
[98] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 20-21.
[99] Ibidem, strana 21.
[100] Ibidem, strana 21.

5.2 Big data

Termín „Big Data“ nevznikl v komunikačních nebo politických studiích, ale stále častěji se používá pro analýzu velkých datových souborů v těchto a mnoha dalších oborech. Jedná se tedy o data, která svojí velikostí a složitostí nelze jednoduše procesovat.[101]

V současné době je silně spojován zejména s analýzou sociálních médií, neboť datové soubory se neustále zvětšují. Spolu s rostoucím přístupem k nástrojům pro zachycování, ukládání a zpracování většího množství dat a jejich dostupností. To samozřejmě odráží i trendy týkající se využívání sociálních médií, neboť na platformách, jako jsou Facebook, Twitter, YouTube nebo Instagram, se zaregistrovalo více uživatelů, a tím i více přispívajících dat.[102]

Jedním z předpokladů používání sociálních médií je vytvoření účtu s použitím našich osobních údajů, jako je jméno, datum narození, věk atd. Do dnešního dne neexistuje sociální médium, které by svým uživatelům umožňovalo anonymní používání. Facebook, gigant mezi sociálními médii, otevřeně přiznává, že shromažďuje naše osobní údaje pro různé účely: *„Shromažďujeme také informace o tom, jak naše produkty využíváte, například typy obsahu, který si prohlížíte nebo se kterým jste nějakým způsobem propojeni, funkce, které používáte, akce, které provádíte, lidé nebo účty, se kterými komunikujete, a frekvence nebo doba trvání vašich aktivit. Například zaznamenáme, kdy používáte a kdy jste naposledy použili naše produkty, a jaké příspěvky, videa nebo další obsah v našich produktech zobrazujete. Také shromažďujeme informace o tom, jakým způsobem používáte naše funkce, jako je například náš fotoaparát.“*[103]

Navzdory debatám o legálnosti a oprávnění sociálních médií zpracovávat osobní údaje nelze přehlížet, že sociální média jsou největším zdrojem velkých dat. Gigant mezi sociálními médii, společnost Facebook, se v současné době může

[101] Boyd, D., Crawford, K. Six Provocations for Big Data, 2011. [online]. [cit. 26.03.2022] Dostupné z: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1926431_code1210838.pdf?abstractid=1926431&mirid=1.
[102] Bruns, A. Compromised Data: From Social Media to Big Data, 1. vydání. Bloomsbury Academic, 2015, strana 175.
[103] [online]. [cit. 26.03.2022] Dostupné z: https://www.facebook.com/about/privacy/.

pochlubit přibližně 2,9 [104] miliardami aktivních uživatelů, což z něj činí největší zdroj velkých dat. Bez debat v této oblasti nezůstávají ani další aplikace spojené s Facebookem, jako jsou WhatsApp a Instagram.

Shromažďování dat na sociálních médiích mělo velký vliv na výzkum sociálních hnutí. *„Výzkumy různých trendů ukazují, že získávání a analýza velkých dat o sociálních hnutích ze sociálních médií se neomezují pouze na velké výzkumné projekty s napojením na poskytovatele dat, vysoce výkonnou výpočetní techniku a rozsáhlou technickou literaturu.“*[105] Nejvýrazněji se trend projevil od roku 2011 v souvislosti s velkými revolucemi na Blízkém východě a v severní Africe. Hlavním důvodem byla nejen vnitřní rychlá komunikace, kterou sociální média umožnila, ale také rozsáhlé vnější pokrytí z vnějšího světa, konkrétně ze západního světa díky využívání sociálních médií a sítí. Při výzkumu nebo sběru velkých objemů dat na sociálních sítích se výzkumní pracovníci ve velké míře spoléhají na hashtagy. S příchodem Twitteru se hashtagy začaly hojně využívat ke sledování náhlých událostí.[106]

Například průzkumná analýza 5,88 milionu tweetů (obsahující sedm hashtagů, včetně #egypt #libya #sidibouzid a #feb14), poskytla prvotní informace o vzorcích tweetování pro každé z těchto hnutí, včetně denní aktivity a umístění uživatelů.[107]

Analýza polohy a denní aktivity uživatelů sice poukazuje na možné narušení soukromí uživatelů a analýzu jejich osobních údajů bez jejich souhlasu, ale nelze popřít, že tyto analýzy mají i svou prospěšnou stránku. Takové analýzy nejsou jen minovými poli mnohostranných informací, ale také analýzou a shromažďováním informací v různých oblastech kromě ústředního tématu, jako je jazyková a interakční oblast. Proces využívání technik velkých dat ve výzkumu sociálních hnutí zvyšuje stávající složitost a vyžaduje revizi a přehodnocení stávajících etických modelů pro výzkum sociálních hnutí.[108]

---

[104] Facebook users by country 2021, Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. [cit. 26.03.2022]. Dostupné z: https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/#:~:text=With%20around%202.9%20billion%20monthly,most%20popular%20social%20media%20worldwide.

[105] Bruns, A. Compromised Data: From Social Media to Big Data, 1. vydání. Bloomsbury Academic, 2015, strana 175.

[106] Ibidem, strana 176.

[107] Freelon, D. Online Fragmentation in Wartime: A Longitudinal Analysis of Tweets about Syria, 2011–2013. The ANNALS of the American Academy of Political and Social Science 2015, strana 166-179.

[108] Ibidem, strana 178.

5.3 Hodnota dat pro firmy

Hodnota osobních dat pro firmy je obrovská. Díky využívání osobních dat skrze online reklamy a její následné analýzy jsou firmy schopné optimalizovat své služby a produkty tak, aby odpovídaly poptávce a byly na míru ušité širšímu publiku spotřebitelů. Příklady efektů plynoucích z využívání osobních dat, které vedou ke zlepšování nabídky jednotlivých firem jsou např. recenze produktů, komentáře spotřebitelů na sociálních sítích, či jiné konkrétní údaje o používání produktů. Osobní údaje také pomáhají firmám k udržení stávajících zákazníků, kteří jim skrze různé formuláře a další poskytují informace o tom, jak jsou v využíváním daných produktů či služeb spokojeni. Pro firmy je tak poměrně jednoduché si skrze podobné marketingové aktivity zákazníky udržet, a tím samozřejmě znovu maximalizovat svůj zisk.[109]

Jednou z možností, jak finanční hodnotu, kterou naše osobní údajů pro firmy mají, je takové příjmy v malé míře zdanit tak, aby jejich používání vedlo k našemu opětovnému prospěchu. Ovšem v otázce zdanění osobních údajů je několik nezodpovězených otázek, ačkoliv samotná daň z prodeje je zcela běžnou, a jednou z nejstarších daní. Není jednoduché osobní údaje ohodnotit, protože jsou uchovávána v soukromí firem, a my tak ani nemáme úplný přehled o tom, jaká data jsou získávána a jaká mají větší hodnotu než jiná. Navíc různé osobní údaje jsou důležité pro různá odvětví. Kromě toho také záleží na tom, jakým způsobem jsou data analyzována, protože správná analýza může hodnotu dat enormně zvýšit.[110]

5.4 Výhody a nevýhody obchodování s osobními daty

Obchodování s osobními údaji s sebou nese několik výhod a nevýhod. Hodnota, kterou osobní data pro firmy a online platformy mají, neustále roste. Ovšem užívání osobních dat k obchodování může mít určité výhody také pro samotné spotřebitele.

[109] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 24-26.
[110] GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. [cit. 26.03.2022]. Dostupné z: https://www.gdpr.cz/blog/osobni-data-jako-vzacny-artikl/.

Kromě cílené internetové reklamy, která umožňuje spotřebitelům nakupovat produkty a služby šité na míru velmi bez zdlouhavého a složitého hledání, mohou spotřebitelé využívat svá osobní data, která online platformy denně generují, k vlastním účelům, např. za účelem zisku. Existují společnosti, jako např. bývalá start-upová společnost Datacoup, která do roku 2019 platila uživatelům měsíční poplatek za přístup k jejich osobním datům, ke kterým v neidentifikovatelné, a anonymní podobě měli přístup inzerenti, kteří nashromážděná data mohli používat k vlastní analýze a optimalizaci jejich nabídky.[111] Jiné společnosti provozující stejné podnikání založené na osobních datech tak denně sbírají informace o tom, jaké stránky uživatel navštěvuje, jaké používá aplikace, kolik na nich tráví času a jaké informace do nich ukládá. Za to daným spotřebitelům firmy určitý peněžní přínos, můžeme tedy hovořit o tom, že osobní data opravdu mají ekonomickou hodnotu, kterou se právě takové společnosti snaží nastavit.[112]

Hlavními důvody, kromě malého finančního bonusu, proč jsou spotřebitelé ochotni sdílet své osobní údaje jsou personalizované služby v podobě více relevantních reklam. Průzkum, který společnost Microsoft provedla v roce 2017, bylo zjištěno, že celkem 56 % respondentů z celkových 13 200 osob uvedlo, že raději nakupují u společností, které jim nabízejí výrobky a služby šité na míru, a mají tedy možnost do samotného procesu vytváření vstupovat výměnou za poskytnutí svých vlastních dat. Bezesporu to ovšem není cesta pro všechny internetové uživatele. Přístup spotřebitelů se také dle průzkumu liší i v otázce národnosti, kdy např. obyvatelé USA byli sdílení svých osobních dat mnohem více nakloněni, než spotřebitelé z Francie, kteří mají větší potřebu si svá osobní data chránit.[113]

Obchodování s osobními daty znamená pro dnešní trh obrovskou změnu. Umožňuje totiž poskytování více kvalitních služeb a personalizaci nabídky, která tak více odpovídá poptávce, což úměrně tomu zvyšuje zisk jednotlivých firem. Ještě k větší maximalizaci hodnoty získávané z osobních údajů uživatelů lze dosáhnout v případě, že se spotřebitelé budou cítit bezpečně svá osobní data sdílet. Pro to je nutné, aby bylo užívání osobních dat online platformami dostatečně chráněné

[111] Sell Your Personal Data for $8 a Month | MIT Technology Review. MIT Technology Review [online]. [cit. 26.03.2022]. Dostupné z: https://www.technologyreview.com/2014/02/12/174259/sell-your-personal-data-for-8-a-month/.
[112] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 24-25.
[113] Ibidem, strana 25.

právními předpisy, a aby bylo jejich zpracování transparentní, a neporušovalo tak práva a svobody jednotlivců.[114]

[114] Nezmar, L. GDPR praktický průvodce implementací, Praha: Grada Publishing, 2017, strana 25-26.

6 Osobní data a kriminalita

6.1 Pojem počítačová kriminalita

„Kyberprostor, amorfní, domněle „virtuální“ svět stvořený propojením počítačů, internetových zařízení, serverů, routerů a ostatních komponentů internetové infrastruktury.“[115] Tento svět plný nul a jedniček, předvídatelných hesel, nezabezpečených počítačových zařízení a jejich neznalých uživatelů je stejně, ne-li více, zneužitelný pro páchání trestné činnosti, jako ten svět normálnímu člověku o něco bližší, fyzický. Naštěstí, stejně jako za sebou pachatel ve většině případů po spáchání trestného činu nechá fyzické stopy (otisky prstů, vzorky DNA, osobní předměty apod.), tak je nechá (v podobě digitální) i po spáchaní tzv. kyberzločinu. Tyto stopy jsou ovšem často velmi složitě objevitelné, dopátrání se pachatele trvá mnohem déle a je zapotřebí mít k dispozici odborníky pracující pro správnou stranu zákona, kteří jsou alespoň stejně zdatní jako jejich zákon porušující „kolegové“.

„Kyberzločin, také známý jako „počítačový zločin“, je použití počítače jakožto nástroje pro páchání trestné činnosti, jako dopouštění se podvodu, obchodování s dětskou pornografií a duchovním vlastnictvím, krádež identity či zneužívání soukromí.“[116] Vzhledem k tomu, jaké množství informací se v dnešní době nalézá na internetových serverech, dosahuje potenciál jejich zneužití jen těžko uchopitelných hodnot. Nebavíme se však „jen“ o osobních datech, peněžních účtech, firemních záznamech apod. Na internetu jsou schraňována data, která přímo souvisí s národní bezpečností, a jejich zneužití může mít přímý vliv na ekonomickou a politickou rovnováhu světa.

6.2 Kyberzločinec

Stejně jako se dá relativně jednoduše porovnávat trestná činnost ve světě virtuálním a fyzickém, tak je možné vedle sebe postavit zločince internetového, a

[115] BUSSELL, Jennifer. Cyberspace. britannica.com [online]. [cit. 27.03.2022]. Dostupné z: https://www.britannica.com/topic/cyberspace.
[116] DENNIS, Michael Aaron. Cybercrime. britannica.com [online]. [cit. 27.03.2022]. Dostupné z: https://www.britannica.com/topic/cybercrime.

zločince, který člověku v obchodě ukradne kabelku. Tento příklad byl vybrán záměrně, nýbrž existuje fenomén, kdy si člověk pod typickým zločincem spíše představí jisté zkrachovalé individuum, které se v důsledku tíživé životní situace, mentální nestability či jiných faktorů uchýlí k nekalé činnosti, i za cenu možného ohrožení zdraví a života jiné osoby. Na druhou stranu, když se zmíní pojem „kyberzločinec", člověk má tendenci si představit geniálního mladíka s kapucí, sedícího za obrazovkou, a schopného se během několika vteřin nabourat do těch nejzabezpečenějších serverů světa. Realita však může být zcela jiná. Takto vystihl zmíněný fenomén Ian Lloyd ve své knize o právu informačních technologií: *„Je typické považovat počítačové zločince za sofistikované a expertní odborníky. Ne vždy to však realita potvrzuje. I tam, kde se trestné činy zdají být přímo napojeny na počítačovou technologii – jako v případě hackování a vytváření a šíření počítačových virů – je příslušný prvek dovednosti často omezen."*[117]

Jinak řečeno, stejně jako klasický zločinec může být opravdu jen obyčejný člověk okrádající staré lidi, nebo geniální mozek rozsáhle zločinecké organizace, tak i kyberzločinec může mít dvě tváře. Na jednu stranu tvář již zmíněného mladíka za obrazovkou s rychlými prsty a obrovskou dovedností, na stranu druhou tvář naprostého počítačového amatéra, který využil nepozornosti svého kolegy z práce, jenž nechal v prohlížeči otevřené internetové bankovnictví, a z jehož účtu si na ten svůj přeposlal finanční prostředky.

6.3 Počítačový podvod

Podvod obecně je jeden z nejrozšířenějších typů trestné činnosti, a ve světě počítačů tomu není jinak. Stručně řečeno, jedná se o „pokus zajistit určitou formu neoprávněného finančního prospěchu."[118] Jeden z prvních cílů podvodu, který člověka přirozeně napadne, jsou finanční instituce (banky, pojišťovny apod.) coby operátoři s gigantickými finančními částkami. I když na počátku rozmachu počítačových sítí (80., 90. léta 20. století) tomu tak většinou bývalo, v dnešní době, vzhledem k obrovskému úsilí fin. institucí vynaloženému na ochranu před

[117] LLOYD, Ian J. Information Technology Law. Vyd. 8. Oxford, UK: Oxford University Press, 2017, str. 209.
[118] Ibidem, 212.

podvodnými útoky, není tím nejsnazším cílem nikdo jiný, než jejich důvěřující zákazník.

Nejčastější typ podvodu v této oblasti je zneužití debetních a kreditních karet. *„Podvod s debetní kartou nastává ve chvíli, kdy zločinec získá přístup k číslu cizí debetní karty (v nějakých případech i k PIN kódu) a udělá s ní neoprávněný nákup, či vybere hotovost z daného účtu.*“[119] Obecně se takový typ jednání považuje za krádež identity, což je v současnosti ve sféře informačních technologií často diskutovaný pojem. Vzhledem k existenci sociálních sítí (Facebook, Twitter, Instagram atd.), na kterých jejich uživatelé vědomě a svévolně sdílejí velká množství osobních informací, je krádež a zneužití cizí identity jednodušší a přístupnější než kdykoliv předtím.

Dalším faktorem přispívajícím k rostoucímu množství podvodů je všudypřítomná neopatrnost uživatelů při volbě hesel, přihlašování se v rámci otevřených sítí a do jisté míry ignorantskému přístupu typu „mě se to stát nemůže“. *„Velmi často jsou jako hesla užívána jména mazlíčku nebo dětí i pro velmi citlivé účely a i bleskové pročtení sociální sítě může podvodníkovi poskytnout dostačující množství materiálu potřebného k získání neoprávněného přístupu. “*[120]

Co se trestu za podvod s kreditní/debetní kartou týče, za ty nejzávažnější případy může být uložen trest vězení přesahující i 10 let. Další možností je podmínka, nebo pokuta, jež může přesahovat částku $10000 (americký dolar). Nedílnou součástí trestu je i kompenzace v podobě odškodnění.[121] Nutno podotknout, že zmíněné tresty jsou platné ve Spojených státech amerických.

6.4 Hacking

Termín „hacking“ je typický tím, že si ho většina lidí vykládá čistě v negativním slova smyslu. „Hacker je člověk, který využívá počítačových, síťových a jiných dovedností k překonání technického problému.“[122] Ač z této definice

[119] FONTINELLE, Amy. Debit Card Fraud: Is Your Money At Risk? investopedia.com [online]. [cit. 27.3.2022]. Dostupné z: https://www.investopedia.com/articles/pf/09/debit-card-fraud-at-risk.asp.
[120] LLOYD, Ian J. Information Technology Law. Vyd. 8. Oxford, UK: Oxford University Press, 2017, str. 213.
[121] THEOHARIS, Mark. Laws on Fraud. criminaldefenselawyer.com [online]. [cit. 27.3.2022]. Dostupné z: https://www.criminaldefenselawyer.com/crime-penalties/federal/Fraud.htm.
[122] ROUSE, Margaret. Hacker. searchsecurity.techtarget.com [online]. [cit. 27.3.2022]. Dostupné z: https://searchsecurity.techtarget.com/definition/hacker.

žádným způsobem nevyplývá, že se musí nutně jednat o trestnou činnost, vyskytuje se pojem „hacker“ nejčastěji právě ve spojení s kyberzločinem.

Jedná-li se tedy o trestnou činnost, je příhodná definice hackování dle Lloyda: *„Akt získání neoprávněného přístupu k počítačovému systému, a to způsobem telekomunikačního propojení z jiného počítače.“*[123] Ve své podstatě se tedy bude jednat o formu podvodu, kterého se pachatel dopustí pomocí dálkově řízené komunikace, s využitím velice pokročilých znalostí informačních technologií, případně programů vytvořených počítačovým kódem.

6.5 Detekce kyberzločinu a získávání důkazů

Proces detekování a stíhání protizákonné aktivity spojené s počítačovými zařízeními se jen těžko dá popsat jako jednoduchý. Naopak, složitost tohoto procesu je jedním z hlavních důvodů, ne-li ten vůbec nejzásadnější, proč se kyberzločin nachází v rozmachu a proč je nezbytné mu věnovat zvýšenou pozornost. „Náš právní systém, vylepšovaný v průběhu staletí, byl stvořen ve fyzickém světě pro fyzické zločiny.“ [124] Svět virtuální, o poznání mladší, se ovšem stále více probíjí do všedních životů lidí na této planetě, a je nutné s ním držet krok i v oblasti práva.

Samotná detekce je zpravidla tou nejsnazší částí. Naneštěstí, podobně jako ve světě fyzickém, k ní dojde až ve chvíli, kdy zločin již proběhl. Vybraný účet, smazaná, upravená či jinak zkompromitovaná data, zablokovaný počítač či serverový výpadek, to vše může indikovat již proběhlou protizákonnou aktivitu. V této chvíli nezbývá nic jiného, než začít detektivní práci za účelem najít virtuální stopy, které by potencionálně mohli vézt k pachateli. Detekování zločinu v jeho průběhu je samozřejmě ideálnější situací, vzhledem k možnosti aktivitu sledovat v reálném čase a případně i zasáhnout. Taková situace se výrazně liší ve světě fyzickém, a v kyberprostoru. Zatímco „běžně“ probíhající zločin je možné přerušit fyzickou konfrontací s pachatelem, a v ten moment jej i zadržet, v případě např. sledovaného, právě probíhajícího hackerského útoku je sice pokus o jeho zastavení možný, ale vzhledem k mnoha obranným mechanismům je jeho úspěšnost

[123] LLOYD, Ian J. Information Technology Law. Vyd. 8. Oxford, UK: Oxford University Press, 2017, str. 215.
[124] GRIMES, Roger A. Why it's so hard to prosecute cyber criminals. csoonline.com [online]. [cit. 27.3.2022]. Dostupné z: https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html.

přinejmenším nepravděpodobná. Navíc i v případě úspěchu zde není možnost okamžitě konfrontovat pachatele, jemuž se naskýtá možnost zahladit stopy a ztratit se.

Získání relevantních důkazů je v mnoha případech náročnější, než by se mohlo čekat. Jako příklad je možné uvézt běžný e-mail (elektronická pošta). Jedna z možností, jak zprávu zachytit, je její zachycení během přenosu, např. z počítače A do počítače B. Tomu však do značné míry zabraňuje tzv. „přepojování paketů", proces, kterým jsou zprávy rozděleny do velkého množství segmentů, z nichž si každý najde jinou cestu do své destinace. Zpráva se složí v celek až v poslední fázi."[125] Zachycení celé zprávy v jeden určitý okamžik je tedy téměř nereálné. Dá se předpokládat, že zpráva bude z obou počítačových zařízení okamžitě smazána, znemožňujíc její získání fyzickým přístupem. Poslední možností je získání oné zprávy ze zařízení poskytovatele internetových služeb, který má právo pro bezpečnostní účely taková data shromažďovat. *„Tomu však zabraňuje vznik kryptografických systémů, jakožto nástrojů, jež může používat i průměrný uživatel"*[126] Pomocí kryptografie je možné zprávu zašifrovat, tak aby jí i při případném zachycení třetí stranou nebylo možné srozumitelně interpretovat (k jejímu přečtení je nutný určitý klíč známý pouze odesílateli a adresátovi).

6.6 Krádež identity

Krádež identity jako trestný čin se objevuje již od 30. let 20. století, kdy byly identity kradeny pro účely hlasování. Kromě toho se vytváření falešných identit a krádeže identity rozšířily v roce 1956, kdy byly identity vytvářeny za účelem nelegálního přistěhovalectví.[127] V důsledku technologických trendů 21st století však krádeže identit nabyly nové podoby a vyvinuly se - krádeže identit se staly složitějšími ve své podstatě, a proto je obtížnější je vystopovat. Používání internetu se stalo každodenním zvykem společnosti a většina se nestává předmětem krádeže identity, proto se vyvinulo mylné přesvědčení, že se člověk nikdy nestane

[125] LLOYD, Ian J. Information Technology Law. Vyd. 8. Oxford, UK: Oxford University Press, 2017, str. 264.
[126] Ibidem, str. 264.
[127] Jake Stroup, A Brief History of Identity Theft, The Balance. [online]. [cit. 27.3.2022]. Dostupné z: https://www.thebalance.com/a-brief- history-of-identity-theft-1947514.

obětí tohoto trestného činu. Nedbalost je však hlavním důvodem, proč je pro kyberzločince snadné provádět výše uvedené trestné činy.

Zatímco ukradená data může zloděj využít osobně, existují i kyberzločinci, kteří kradou obrovské množství osobních údajů a dále je prodávají dalším stranám. Většina transakcí probíhá na dark webu, který je jakousi podúrovní „internetu“ dark web není indexován a je k němu omezený přístup, proto je přístupný pouze pomocí softwaru s otevřeným zdrojovým kódem nebo proxy, jako je například Tor.[128] Dark web lze sice využívat k nekalým účelům, ale jak bylo uvedeno výše, dochází zde k mnoha nelegálním transakcím, včetně krádeží identity a prodeje ukradených identit. Jak v roce 2018 zjistil deník The Independent, „ukradené osobní údaje občanů Spojeného království se na dark webu prodávají za pouhých 10 liber a nabízejí hackerům veškeré informace potřebné k provádění online podvodů.“[129] Jaké jsou ale nejčastější osobní údaje, které se kradou a před kterými se snaží ochrana osobních údajů chránit? Odpověď je následující: 35 % ukradených údajů tvoří čísla sociálního pojištění, následuje 30 % ukradených údajů o kreditních kartách, díky čemuž je krádež finanční identity jednou z nejčastějších.[130]

Jak bylo uvedeno výše, krádeže identity a podvody ve finančním sektoru jsou běžným problémem. Nejoblíbenějšími typy bankovních operací, které jsou terčem útoků, jsou - online platby, nebo karetní transakce. Protože však bankovní sektor nestojí na místě a jako každé jiné odvětví se neustále vyvíjí a směřuje k digitalizaci, přináší to své vlastní výzvy. Krádeže identity se rozšířily konkrétně po zavedení internetového bankovnictví, což následně poskytuje více příležitostí a možných slabých míst pro kyberzločince. Čím je služba složitější, tím větší je možnost slabého místa, na které se lze zaměřit.[131]

Běžným způsobem získávání osobních údajů je tzv. phishing. Phishing je krádež identity prostřednictvím rozesílání falešných e-mailových adres, které se svým charakterem podobají e-mailovým adresám bank nebo finančních institucí,

---

[128] John Stevenson, All you need to know about Darkweb. [online]. [cit. 27.3.2022]. Dostupné z: https://books.google.lv/books?id=OAZuDAAAQBAJ&printsec=frontcover&hl=lv#v=onepage&q&f=false.

[129] Anthony Cuthbertson, Stolen UK identities selling for as low £10 on, The Independent. [online]. [cit. 27.3.2022]. Dostupné z: https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-id-value-hackers-cyber-crime-a8683821.html.

[130] Doug Shadel, Is My Identity on the Dark Web?, AARP. [online]. [cit. 27.3.2022]. Dostupné z: https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-we.

[131] MAISNER, M., a kol. Základy softwarového práva. Praha: Wolters Kluwer ČR, a. s., 2011, strana 272.

nebo pomocí falešných webových stránek, které požadují, aby jim jednotlivec poskytl osobní údaje, jako jsou údaje o kreditních kartách, kódy PIN, přístupové údaje do různých systémů nebo údaje o bankovních kartách apod.[132] Kromě toho lze krádež identity provést a informace získat pomocí „pharmingu“ - používání různého nelegálního softwaru, který lze nainstalovat do zařízení uživatele a který bez jeho vědomí provádí na zařízení různé úkoly - takový software je jinak známý jako počítačové viry. Mezi populárně známé počítačové viry tohoto typu patří „trojský kůň“, různé viry typu „keylogger“, které se instalují do zařízení a ukládají hesla, uživatelská jména, bankovní údaje, které se zadávají pomocí klávesnice.[133]

„*Některé z těchto virových technologií napadají adresní řádek internetového prohlížeče a jsou pokročilejší než phishing. Když zákazníci zadají platnou adresu URL, místo na platné stránky jsou přesměrováni na kriminální webové stránky*.“[134]

Celkově lze říci, že krádež identity jako trestný čin je nejvíce rozšířena v USA, Austrálii, Jihoafrické republice, Kanadě a Evropské unii. V roce 2009 byla nejkritičtější situace v Evropské unii pozorována ve Spojeném království, neboť podle údajů Asociace komerčních bank ve Spojeném království vzrostly v první polovině roku 2006 ztráty způsobené podvodnými transakcemi v internetovém bankovnictví o 55 %, což v porovnání s předchozím rokem přispělo ke ztrátám ve výši 22,5 milionu liber.[135] Podle informací poskytnutých sdružením CIFAS, které působí ve Spojeném království boj proti podvodům a prevence podvodů, mezi lety 2000 a 2006 vzrostl počet krádeží identity online o 500 %.[136]

Přestože prezentované údaje pocházejí z roku 2006, a nikoli z aktuální doby, podtrhují význam, rychlý růst a aktuálnost této problematiky v internetovém bankovnictví. Krádeže identity v online sféře představují pro finanční instituce velkou hrozbu, které je třeba neustále čelit.

V současné době byla zavedena různá řešení s cílem zabránit podvodným činnostem, například zavedením bezpečnějších způsobů ověřování v internetovém

[132] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016, strana 395.
[133] Prof. Silvia Parusheva, Identity Theft and Internet Banking Protection, Ekonomická univerzita - Varna, Economic Alternatives, Issue 1, 2009, strana 44.
[134] MAISNER, M., a kol. Základy softwarového práva. Praha: Wolters Kluwer ČR, a. s., 2011, strana 272.
[135] Prof. Silvia Parusheva, Identity Theft and Internet Banking Protection, Ekonomická univerzita - Varna, Economic Alternatives, Issue 1, 2009, strana 45.
[136] Ibidem.

bankovnictví, jako je zavedení více faktorového ověřování, s použitím PIN kalkulátorů, karet nebo doplněním procesu ověřování službou poskytovatele důvěryhodných služeb. Změnám v bankovnictví se samozřejmě musí přizpůsobit i proces identifikace, který se musí stát jednodušším, efektivnějším a také bezpečnějším, nicméně vystaven digitalizaci se i proces autentizace může stát předmětem ohrožení.

I když je zajištění online anonymity zásadní, je třeba poznamenat, že stejně zásadní je i zajištění online identity pro určité činnosti, aby se zabránilo neoprávněnému přístupu k údajům, aby nedošlo ke krádeži identity a z mnoha dalších důvodů. Online anonymita i identita mají společnou tenkou hranici, po které je třeba opatrně kráčet - obě jsou zásadně potřebné, nicméně v některých případech se střetávají a způsobují mírný zmatek.

7 Osobní data a lidská práva

7.1 Právo na soukromí

7.1.1 Soukromí jako koncept

Pojem soukromí a soukromé sféry je poměrně obtížně definovatelný pojem, který, ačkoliv prostupuje všemi aspekty našeho života, není univerzálně definován. Z logicky věci je zřejmé, že soukromí je založeno na vztahu jedince vůči společnosti, která svou existencí a specifickým fungováním vytváří určitý veřejný prostor, ve kterém jednotlivci vymezují svou sféru soukromou.[137]

Soukromí, jakožto součást základních lidských práv, je ve Všeobecné deklaraci lidských práv definováno v článku 12, který říká, že: *„Nikdo nesmí být 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.“*[138] V rámci Listiny základních práv a svobod, jež je součástí ústavního pořádku České republiky, je ochrana soukromí součástí obecné ochrany osobnosti v článcích 7 a 10, které mimo jiné říkají, že nedotknutelnost soukromí osoby je zaručena, a že každý má právo na ochranu před neoprávněným zveřejňováním, či jiným zneužíváním údajů o své osobě.[139] Ústavou je nám tedy zaručeno právo na ochranu lidské důstojnosti, dobré pověsti a jména, osobní cti, a také právo před neoprávněným zasahováním do rodinného života, který je vnímán jako součást soukromí každého jednotlivce.[140] Občanský zákoník České republiky vymezuje základní úpravu ochrany soukromí v zákoně č. 89/2012 Sb., který uvádí, že chráněna je našeho osobnost včetně všech našich přirozených práv, jakožto také projevy naší osobní povahy.[141]

Soukromí lze tedy dle této definice chápat jako právo každého jedince jak na ochranu informací o vlastní osobě, tak na ochranu osobního prostoru týkajícího

[137] Wacks, Raymond. Law, Mortality and the Public Domain, Hong Kong: Hong Kong University Press, 2000, str. 235-236.
[138] Všeobecná deklarace lidských práv, článek 12.
[139] Listina základních práv a svobod, článek 7, 10.
[140] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 23.
[141] Ibidem, str. 24.

se vlastního těla, prožitků, myšlenek a také vlastní rodiny před zveřejněním a možným zneužitím v prostoru veřejné sféry.

Takový koncept soukromí, jaký jsem vymezil v odstavci výše, je v souvislosti s neustále postupující digitalizací všech aspektů lidského života ne zcela reálný. Technologie, především ve spojitosti s internetem, totiž vymazávají hranice mezi veřejným a soukromým prostorem. V souvislosti s tímto poměrně mladým trendem vyspělých technologií a internetu se někteří odborníci domnívají, že pojem soukromí, tak jak ho po staletí chápeme a vnímáme, je zastaralý a bránící se jakékoliv inovaci.[142]

Ve známém článku „Právo na soukromí" soudců Louis D. Brandeise a Samuel D. Warrena, který vznikl v reakci na masivní rozvoj bulvární žurnalistiky a fotografického průmyslu, je právo na soukromí vymezeno jako právo být nechán na pokoji, tedy jako právo na nezasahování do vlastního soukromí.[143] Kritikou tohoto přístupu pak byl argument, který tvrdí, že právo být nechán na pokoji je v rozporu se společností, jež se vyznačuje svobodou projevu a veřejnou diskuzí.[144]

V teorii jsou vymezovány dva hlavní proudy vymezující pojem soukromí. Zástupci prvního proudu popisují soukromí jako shluk samostatných zájmů, jež spolu nemusejí vždy souviset, a mělo by tak být vyjadřováno skrze konkrétní příklady.[145] Dalším teoretickým výkladem soukromí je teze, že soukromí je jednotné, pojmově odlišné právo nebo zájem, která má zřetelnou morální hodnotu.[146]

Z hlediska technologií a internetu je právo na soukromí vyjadřováno právem na kontrolu informací o sobě. Takový obsah mu přisuzuje i Ústavní soud České republiky, který říká, že: *„Právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. V jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí*

[142] Julie E. Cohen "What Privacy is for" in "Synopsium: (2013) 126 Harvard Law Review 1879, kapitola IV.
[143] Samuel D. Warren a Louis D. Brandeis, "The Right to Privacy" (1890) 5 Harvard Law Review 1879, kapitola V.IV.
[144] Richards, Neil. Intellectual privacy rethinking civil liberties in the digital age, Oxford: Oxford University Press, 2015, str. 4.
[145] O'Callaghan, Patrik. Refining Privacy in Tort Law Heidelberg: Springer-Verlag Berlin, 2013, str. 25.
[146] Ibidem, 10.

zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení.“[147]

7.1.2 Soukromí jako ochrana osobních údajů

Ochrana osobních údajů, jež do jisté míry chrání také samotné soukromí, je popisována jako souhrnný termín pro řadu myšlenek, které se týkají ochrany osobních údajů a jejich zpracování.[148]

Mnohé ze základních úmluv o lidských právech jsou poměrně abstraktní, oproti tomu různé mezinárodní úmluvy, jako např. Evropská úmluva o lidských právech, či Listina základních práv Evropské unie v kombinaci se státními právními předpisy vytváří velmi rozsáhlý rámec norem týkající se ochrany soukromí a osobních údajů. Právní předpisy o ochraně soukromí a osobních údajů poskytují lidem práva na správu vlastních osobních údajů a na rozhodování o jejich použití. Na mezinárodní úrovni je ochrana osobních údajů upravena Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat, známá také jako tzv. Ústava 108, která vznikla v roce 1981 na půdě Rady Evropy.[149] Ta fyzickým osobám zaručuje na území smluvních stran ochranu soukromí ve vztahu k automatickému zpracování osobních údajů. Na základě této úmluvy pak byla problematika ochrany osobních údajů zpracována také v jednotlivých členských státech.[150]

Pod pojmem osobního údaje dle zákona 5 písm. a) rozumíme jakoukoliv informaci, která se týká určené nebo určitelné fyzické osoby přičemž *„subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*[151] Takovéto vymezení osobních údajů je ale velmi široké, a za osobní údaj tedy můžeme považovat dlouhou a různou řadu informací. Typicky

[147] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 24.
[148] Paul De Hert a Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Gutwirth S., Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (eds) Reinventing data protection? (Springer Science, Dordrecht 2009) 3- 44, 3.
[149] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 43.
[150] Ibidem, 42.
[151] Ibidem, 43.

mezi osobní údaje řadíme osobní jméno, příjmení, rodné číslo, v internetovém prostředí pak např. emailovou adresu, přezdívku na sociálních sítích, anebo v některých případech také IP adresu. Zpracováním osobních údajů pak podle zákona 4 písm. a) Ochrany osobních údajů rozumíme *„jakoukoliv operaci, nebo soustavu operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky"*, jako jejich *"shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace."*[152]

Podle amerického profesora práva Daniela J. Soloveho se tato práva skládají především z práva na oznámení, přístup a souhlas týkající se shromažďování, používání a zveřejňování osobních údajů. Solove tuto takzvanou kontrolu osobních údajů nazývá „samosprávou soukromí". Tento přístup však sám kritizuje, neboť vychází z předpokladu, že lidé jsou vždy plně informovaní a jednají zcela racionálně, což ovšem nelze považovat za stoprocentní pravdu.[153] Podobný názor sdílí také například americká právnička Julie E. Cohenová, která se domnívá, že ono liberální já, které je předmětem teorie ochrany soukromí a tvorby politiky ochrany soukromí, ve skutečnosti neexistuje". I ona kritizuje klasifikaci soukromí jako „kontroly" informací a tvrdí, že soukromí nelze redukovat na „kontrolu" informací.[154]

7.1.3 Právo na soukromí jako abstraktní a symbolický pojem

Jak již bylo uvedeno, soukromí má řadu významů. Při čtení argumentů různých teoretiků lze dojít k závěru, že soukromí může v praxi znamenat téměř cokoli. Pokud se o soukromí hovoří bez náležitých definic a bez přesnosti, celý pojem se pak rozmělňuje a je značně abstraktní. Lze tedy uvažovat, že pokud soukromí znamená téměř cokoliv, neznamená pak v praxi téměř nic?

Někteří vědci se domnívají, že takzvané abstraktní pojmy, jako je například svoboda projevu, nebo právě soukromí, nemají žádný přirozený obsah, ale jsou

[152] Donát, J., Tomíšek, J. Právo v síti. Průvodce právem na internetu. 1. vydání. Praha: C. H. Beck, 2016, str. 44.
[153] Solove, J. Daniel. Introduction: Privacy Self-Management and the Consent Dilemma, 2013 126 Harvard Law Review 1879, 1880
[154] Julie E. Cohen "What Privacy is for" in "Synopsium: (2013) 126 Harvard Law Review 1879, kapitola IV.

naplněny v podstatě jakýmkoliv obsahem, který se do nich podaří vložit.[155] Panuje určitý obecný předpoklad a vědomí toho, co tyto abstraktní pojmy znamenají. Jejich definice jsou nicméně natolik vágní, že nechávají prostor pro nesouhlas s tím, jak jsou obvykle vnímány, a tak se otevírá prostor pro rozlišné definice a chápání. Tím, co určuje všeobecné vědomí o obsahu těchto pojmů, je pak tzv. sdílená zkušenost, která je ale založena na odlišném kulturním vnímání.[156]

Na soukromí lze nahlížet jako na fenomén, který představuje určité zvyky a praktiky, které tak vlivem nějaké společenské zkušenosti vnímáme, anebo na něj lze nahlížet také jako na právo. Oproti fenoménu, který je málokdy jasně definován, je právo jasně stanoveno. Pro zajištění právní jistoty je tak třeba na pojem soukromí vnímat jako právo. Jedním ze způsobů, jak na to nahlížet, je vnímat soukromí jako hodnotu, kterou je třeba chránit pomocí určitých právních nástrojů. Zákon pak definuje, na jaká práva a ochranu má každý z nás nárok.[157]

Ochrana soukromí je celosvětovou záležitostí. Téměř každý stát má přímé či nepřímé právní předpisy nebo pravidla, která chrání soukromí, jež obvykle bývá zakotvené v ústavě.[158] Existují také nadnárodní směrnice a rámce upravující ochranu soukromí. Kromě toho je soukromí lidským právem a potvrzením osobní svobody, ale není právem absolutním.[159] Někdy ale musí soukromí ustoupit jiným základním právům, anebo může být vyváženo veřejným zájmem, nebo jinými hodnotami. V dnešní digitalizované společnosti, kdy jsou informace a osobní údaje téměř neustále sdílena s velkým publikem, je ochrana soukromí ve značném ohrožení. V některých případech je obtížné, nebo možná dokonce nemožné, definovat, kdo data kontroluje, kdo k nim má přístup, a kam až může sběr dat zajít.[160] To je však problém, který si GDPR klade za cíl vyřešit, nebo alespoň zlepšit.

---

[155] Stanley Fish, There's no such Thing as Free Speech and it's a Good Thing, Oxford University Press 1994) 90.
[156] O'Callaghan, Patrick. Refining Privacy in Tort Law , Heidelberg: Springer-Verlag Berlin, 2013, str. 25.
[157] Mireille Hildebrandt. "Privacy and Identity" Oxford - AntwerpPrivacy and the Criminal Law (2006) [online]. [cit. 15.03.2022]. Dostupné z: http://works.bepress.com/mireille_hildebrandt/6/ 61-104, 63.
[158] Solove, J. Daniel. Introduction: Privacy Self-Management and the Consent Dilemma, 2013 126 Harvard Law Review 1879, 1880, 2-3.
[159] Gregory J. Walters, *Human Rights in an Information Age: A philosophical Analysis*, University of Toronto Press, 2001, strana 133.
[160] Rodrigues, Ruben. Privacy on Social Networks: Norms, Markets, and Natural Monopoly' in Saul Levmore and Martha Nussbaum (eds) *The Offensive Internet, Speech Privacy and Reputation*, Harvard University Press, 2010, strana 237.

Ochrana osobních údajů je definována a upravena v mnoha mezinárodních a vnitrostátních právních předpisech. Tyto právní předpisy svým způsobem definují právo na soukromí a ochranu údajů. Dá se ovšem předpokládat, že ve chvíli, kdy by byly všechny zákony týkající se práva na soukromí a ochranu osobních údajů zrušeny, lidé by tato práva pravděpodobně stále, alespoň do určité míry, stále respektovali. To nejspíše vyplývá ze základní morální hodnoty, která je společností soukromí přisuzována. V takovém případě lze tedy citovat myšlenku amerického profesora Daniela J. Soloveho, že: „soukromí zahrnuje všechno, a proto se zdá, že samo o sobě není ničím." Abychom pochopili průnik technologií a soukromí, musíme analyzovat a konceptualizovat soukromí v novém digitalizovaném prostředí. Je důležité, aby právní vědci a další právníci měli na paměti, že v dnešní společnosti je pravděpodobné, že každý a všechno je neustále monitorováno pomocí technologie chytrých zařízení. Není možné vrátit čas. Je tedy nutné se této nové situaci přizpůsobit.

7.2 Svoboda projevu a GDPR

Právo na svobodu projevu je zakotveno ve Všeobecné deklaraci lidských práv, která říká, že: *„Každý má právo na svobodu přesvědčení a projevu; toto právo nepřipouští, aby někdo trpěl újmu pro své přesvědčení, a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a bez ohledu na hranice."*[161]

Tato deklarace inspirovala již závazný mezinárodní dokument zvaný Mezinárodní pakt o občanských a politických právech, který je platný od roku 1976, a který ve svém článku 19 upravuje svobodu projevu tak, že každý má právo zastávat svůj bez jakékoliv překážky, a stejně tak jako má každý jedinec právo na svobodu projevu, má také právo na hledání, přijímání a rozšiřování jakýchkoliv informací.[162] Nejdůležitějším mezinárodním dokumentem, jež upravuje právo jedince na svobodný projev, je pak Mezinárodní úmluva o ochraně lidských práv, která v České republice vešla v platnost v roce 1992. Svoboda projevu je pak také součástí ústavního pořádku České republiky, a upravuje ji Listina základních práv a svobod, která v článku 17 deklaruje následující:

[161] Všeobecná deklarace lidských práv, článek 19.
[162] Mezinárodní pakt o občanských a politických práv, článek 19.

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 nepřípustná.

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.[163]

Ovšem také svoboda projevu má určité meze, v rámci kterých se musí pohybovat. Podle článku 17 Listiny základních práv a svobod by právo na svobodu projevu nemělo ohrozit bezpečnost státu, veřejnou bezpečnost, veřejné zdraví a mravnost, a v neposlední řadě by svoboda projevu neměla narušovat práva a svobody druhých.[164]

Svoboda projevu může být také omezena v souvislosti s přístupem k informací a jejich šíření. Těmi hlavními důvody, proč svobodu projevu omezit bývají např. Ochrana soudnictví, anebo ochrana práv třetích osob především v souvislosti s různými citlivými údaji, mezi které také samozřejmě patří osobní údaje.[165]

Střet práva na ochranu osobních údajů a práva na svobodu projevu zřejmý, a v souvislosti se zavedením GDPR muselo dojít k jejich vyvážení. Problematika střetu ochrany osobních údajů a svobodného projevu je velmi častá, a také poměrně komplikovaná, především v oblasti médií, a dále například v akademickém, uměleckém, či literárním projevu. V těchto oblastech, a především právě v novinářském odvětví, dochází vlivem internetu a neustále se rozvíjejících technologií, k masovému zpracovávání osobních dat. V oblasti ochrany osobních údajů a jejich zpracování za novinářskými účely byla členským státům EU při zavádění GDPR umožněno dělání úprav. Členské státy EU mohly tedy stanovit

[163] Listina základních práv a svobod, článek 17.
[164] Ibidem, článek 17.
[165] BARTOŇ, Michal. Svoboda projevu: principy, garance, meze. Praha: Leges, 2010. Teoretik, s. 125.

odchylky na definici práva na ochranu osobních údajů společně s právy na svobodu projevu a informací, a to z důvodu odlišného pojetí těchto práv v různých státech.[166]

Při zpracovávání a zveřejňování osobních údajů, např. v médiích, by se měl daný subjekt řídit zásadou proporcionality, tedy měl by se snažit o přiměřené vyvážení všech práv, konkrétně tedy práva ochrany osobních údajů a práva na svobodu projevu. Při omezování práva na ochranu osobních údajů za účelem dosažení svobody projevu je důležité dbát na všechny relevantní skutečnosti týkající se toho, zdali je osoba, jejíž osobní údaje jsou zveřejňovány, mediálně či politiky činná, jelikož v příkladě především veřejných činitelů je právo na soukromí posuzováno odlišně. Do práv na ochranu osobních údajů pak u takto veřejně známého subjektu ovšem neproporcionálně zasahuje např. zveřejnění informací o zdravotních stavu, či publikace jiných intimních informací, a to i přes to, že na takových údajích může mít společnost zájem.[167]

7.3 Právo na informace vs. ochrana dat v GDPR

V rámci střetu práva na ochranu osobních údajů a práva na informace, které je také garantováno článek 17 Listiny, a detailně popsáno v zákoně č. 106/1999 Sb. o svobodném přístupu k informacím, který definuje, jak je možné vyžadovat, získávat a zpracovávat informace o činnosti veřejných orgánů. Ke kolizi těchto dvou práv dochází poměrně často. Obyčejně ovšem převažuje právo na svobodný přístup k informacím, které jsou v rámci transparentnosti veřejné správy upřednostňovány. Ovšem ani také právo na informace není absolutní. Opět je zde pro správné vyvažování nutné provádět test proporcionality.[168]

[166] Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J., Kovaříková, K. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 529-532.
[167] Ibidem, str. 531.
[168] Ibidem, str. 533.

Závěr

Osobní data se v souvislosti v neuvěřitelně pokročilou technologií stávají cenným zbožím, které každý den v obrovské míře dáváme skrze naše telefony, počítače a jiná zařízení světu najevo. Pro to, abychom udrželi pod kontrolou, jakým způsobem, a v jakém množství jsou tato našimi zařízeními využívána. Měli bychom mít vědomou kontrolu nad našimi daty prostřednictvím účinných a efektivních mechanismů, nikoliv prostřednictvím zřeknutí se jakékoliv odpovědnosti.

Změnu ve využívání a ochraně osobních údajů si můžeme jakožto dotčené subjekty vymoci za pomoci zákonů. Neměli bychom zapomínat, že volná výměna údajů a osobních informací je pro jejich poskytovatele, a v tomto případě jsou poskytovateli myšleni především poskytovatelé sociálních sítí a dalších internetových aplikací, velmi cenným zbožím. Naše osobní údaje jsou zcela bezplatně poskytovány pro zvýšení firemního zisku. A ačkoliv nám v mnohém usnadňují dané aplikace a sítě život, jsou velkým ohrožením pro naše soukromí.

Budoucnost ochrany dat spočívá především v tom, jakým způsobem si je sami budeme chránit. Nemělo by nás činit bezstarostnými to, jakým způsobem a kým jsou naše data sdílena. Je nevyhnutelné začít budovat osobní a komunitní povědomí o praktikách týkající se zneužívání dat a jejich celkovém fungování. Vzdělání v této oblasti je možná ještě tím důležité pro mladou generaci dětí a mládeže, která moderní technologie využívá téměř od narození, a od útlého věku tak odhaluje velké množství svých osobních dat, jejichž zneužití může vést až k nebezpečí na životě.

Náš přístup, a tedy také přístup samotného práva a jeho neustále nutných modifikací, byl měl být v budoucnosti více preventivní, nežli reaktivní a měl by se tak snažit předcházet možnému zneužívání. Je důležité tedy primárně změnit osobní přístup v ochraně dat, a začít tedy dbát na to, jaké si např. vybíráme poskytovatele služeb, jež chrání naše soukromí a integritu našich dat, zároveň dbát na nejvyšší možné nastavení ochrany osobních údajů na sociálních sítích, anebo více investovat do služeb, která chrání naše hesla. Budoucnost ochrany osobních dat tedy bude záležet především na našem osobním přístupu, a na tom, jakou důležitost ochraně citlivých informací o naší osobě dáme. Nelze očekávat, že právo takové podmínky splní před námi.

Seznam použité literatury a dalších zdrojů

Knižní publikace, odborné časopisy

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

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

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. GDPR: hmotné a procesní aspekty prakticky. V Praze: C.H. Beck, 2019. Právní praxe. ISBN 978-80-7400-762-0.

MYŠKA, Matěj. Právní aspekty uchovávání provozních a lokalizačních údajů. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6462-1.

TÝČ, Vladimír. Česká republika a současný svět: (sborník dokumentů). Praha: Linde, 1998. ISBN 80-7201-121-9.

NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

MAISNER, Martin. Základy softwarového práva. Praha: Wolters Kluwer Česká republika, 2011. Právní monografie (Wolters Kluwer ČR). ISBN 9788073576387.

JANEČKOVÁ, Eva a Václav BARTÍK. Ochrana osobních údajů v pracovním právu: (otázky a odpovědi). Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 80-7357-322-9.

Zákon o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 9788025146644.

BARTOŇ, Michal. Svoboda projevu: principy, garance, meze. Praha: Leges, 2010. Teoretik. ISBN 978-80-87212-42-4.

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

Cizojazyčné

Richards, Neil. Intellectual privacy rethinking civil liberties in the digital age, Oxford: Oxford University Press, 2015. ISBN 978-0199946143

LLOYD, Ian J. Information Technology Law. Vyd. 8. Oxford, UK: Oxford University Press, 2017. ISBN 9780198830559

Bruns, A. Compromised Data: From Social Media to Big Data, 1. vydání. Bloomsbury Academic, 2015. ISBN 9781501306525

Gregory J. Walters, Human Rights in an Information Age: A philosophical Analysis, University of Toronto Press, 2001. ISBN 978-0802085504

Rodrigues, Ruben. Privacy on Social Networks: Norms, Markets, and Natural Monopoly' in Saul Levmore and Martha Nussbaum (eds) The Offensive Internet,

Speech Privacy and Reputation, Harvard University Press, 2010. ISBN 9780674064317

Paul De Hert a Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Gutwirth S., Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (eds) Reinventing data protection? (Springer Science, Dordrecht 2009) ISBN 978-1-4020-9497-2

Stanley Fish, There's no such Thing as Free Speech and it's a Good Thing, Oxford University Press. 1994. ISBN 9780195093834

O'Callaghan, Patrik. Refining Privacy in Tort Law Heidelberg: Springer-Verlag Berlin, 2013. ISBN 978-3-642-31883-2

Solove, D. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126, 1880-1903.

Freelon, D. Online Fragmentation in Wartime: A Longitudinal Analysis of Tweets about Syria, 2011–2013. The ANNALS of the American Academy of Political and Social Science 2015.

Wacks, Raymond. Law, Mortality and the Public Domain, Hong Kong: Hong Kong University Press, 2000.

Julie E. Cohen "What Privacy is for" in "Synopsium: (2013) 126 Harvard Law Review 1879.

Samuel D. Warren a Louis D. Brandeis, "The Right to Privacy" (1890) 5 Harvard Law Review 1879.

Prof. Silvia Parusheva, Identity Theft and Internet Banking Protection, University of Economics - Varna, Economic Alternatives, Issue 1, 2009, strana 44.

Právní předpisy České republiky

Zákon č. 127/2005 Sb., o elektronických komunikacích

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

Právní prameny Evropské unie a mezinárodní dokumenty

Všeobecná deklarace lidských práv

Mezinárodní pakt o občanských a politických právech

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

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

Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislost se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“

Judikatura

Rozsudek Soudního dvora EU ve věci C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González

Internetové zdroje

Anthony Cuthbertson, Stolen UK identities selling for as low £10 on, The Independent. [online]. [cit. 27.3.2022]. https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-id-value-hackers-cyber-crime-a8683821.html

Doug Shadel, Is My Identity on the Dark Web?, AARP. [online]. [cit. 27.3.2022]. https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-we

Jake Stroup, A Brief History of Identity Theft, The Balance. [online]. [cit. 27.3.2022]. Dostupné z: https://www.thebalance.com/a-brief-history-of-identity-theft-1947514

GRIMES, Roger A. Why it's so hard to prosecute cyber criminals. csoonline.com [online]. [cit. 27.3.2022]. Dostupné na https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html

ROUSE, Margaret. Hacker. searchsecurity.techtarget.com [online]. [cit. 27.3.2022]. Dostupné na https://searchsecurity.techtarget.com/definition/hacker

John Stevenson, All you need to know about Darkweb. [online]. [cit. 27.3.2022]. Dostupné z: https://books.google.lv/books?id=OAZuDAAAQBAJ&printsec=frontcover&hl=lv#v=onepage&q&f=false

THEOHARIS, Mark. Laws on Fraud. criminaldefenselawyer.com [online]. [cit. 27.3.2022]. Dostupné z https://www.criminaldefenselawyer.com/crime-penalties/federal/Fraud.htm

FONTINELLE, Amy. Debit Card Fraud: Is Your Money At Risk? investopedia.com [online]. [cit. 27.3.2022]. Dostupné na https://www.investopedia.com/articles/pf/09/debit-card-fraud-at-risk.asp

BUSSELL, Jennifer. Cyberspace. britannica.com [online]. [cit. 27.03.2022]. Dostupné z https://www.britannica.com/topic/cyberspace

DENNIS, Michael Aaron. Cybercrime. britannica.com [online]. [cit. 27.03.2022]. Dostupné z https://www.britannica.com/topic/cybercrime

Sell Your Personal Data for $8 a Month | MIT Technology Review. MIT Technology Review [online]. [cit. 26.03.2022]. Dostupné z: https://www.technologyreview.com/2014/02/12/174259/sell-your-personal-data-for-8-a-month/

Facebook users by country 2021, Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. [cit. 26.03.2022]. Dostupné z: https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/#:~:text=With%20around%202.9%20billion%20monthly,most%20popular%20social%20media%20worldwide

Boyd, D., Crawford, K. Six Provocations for Big Data, 2011. [online]. [cit. 26.03.2022] Dostupné z: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1926431_code1210838.pdf?abstractid=1926431&mirid=1

[online]. [cit. 26.03.2022] Dostupné z: https://www.facebook.com/about/privacy/

GDPR | Obecné nařízení o ochraně osobních údajů —prakticky. [online]. [cit. 23.03.2022] Dostupné z: https://www.gdpr.cz/blog/osobni-data-jako-vzacny-artikl/

Agentura Evropské unie pro kybernetickou bezpečnost, Hodnota osobních údajů. [online]. [cit. 23.03.2022]. https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data

Sirota, D. (2018, April 23). GDPR: Analýza nákladů a přínosů. [online]. [cit. 23.03.2022]. Dostupné z: https://www.informationweek.com/strategic-cio/security-and-risk-strategy/gdpr-a-cost-vs-benefit-analysis/a/d-id/1331616

Ambler, T., Chittenden, F. & Bashir, A. (2019). Counting the Cost of EU Regulation to Business (Počítání nákladů na regulaci EU pro podniky). Evropský hospodářský a sociální výbor. [online]. [cit. 23.03.2022]. Dostupné z https://www.eesc.europa.eu/en/documents/counting-cost-eu-regulation-business

Philip Heijmans, „Getting the Business Over Data Privacy“ (US News, 1. srpna 2018) [online]. [cit. 23.03.2022]. Dostupné z: https://www.usnews.com/news/best-countries/articles/2018-08-01/across-europe-new-data-privacy-law-still-leaves-confusion

EMOTA, „Lessons from Europe and Data Protection“ (Konference OSN o obchodu a rozvoji 2017) [online]. [cit. 23.03.2022]. Dostupné z: https://unctad.org/system/files/non-official-document/dtl_eWeek2017p13_OliverHateley_en.pdf

The History of the General Data Protection Regulation| European Data Protection Supervisor. Redirecting to https://edps.europa.eu/_en [online]. [cit. 20.03.2022] Dostupné z: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Úřad k návrhu nařízení o soukromí a elektronických komunikacích: Úřad pro ochranu osobních údajů: Titulní stránka [online]. [cit. 15.03.2022] Dostupné z: https://www.uoou.cz/urad-k-navrhu-narizeni-o-soukromi-a-elektronickych-komunikacich/d-49300

STIGLER, STEPHEN, M. Perspectives; Galton and Identification by Fingerprintes. Statistics Department, Chicago. [online]. [cit.15.03.2022]. Dostupné z: http://www.genetics.org/content/140/3/857

Biometrics News, Companies and Explainers | Biometric Update [online]. [cit. 15.03.2022]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

Biometrické údaje | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. [cit. 15.03.2022]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/biometricke-udaje/

Mireille Hildebrandt. "Privacy and Identity" Oxford - Antwerp*Privacy and the Criminal Law* (2006) [online]. [cit. 15.03.2022]. Dostupné z: http://works.bepress.com/mireille_hildebrandt/6/

Summary

With incredible advances in technology, personal data is becoming a precious commodity that we make known to the world every day on a massive scale through our phones, computers and other devices. We need to keep control of how, and how much, it is used by our devices. We should have conscious control over our data through effective and efficient mechanisms, not through abdication of any responsibility.

As affected entities, we can enforce changes in the use and protection of personal data by using the law. We should not forget that the free exchange of data and personal information is a very valuable commodity for its providers, and in this case the providers are primarily providers of social networks and other Internet applications. Our personal data is provided completely free of charge to increase corporate profits. And although these applications and networks make our lives much easier, they are a major threat to our privacy.

The future of data protection is all about how we protect it ourselves. We should not be complacent about how and by whom our data is shared. It is imperative that we start building personal and community awareness of data misuse practices and their overall operation. Education in this area is perhaps even more important for the younger generation of children and young people, who have been using modern technology almost from birth, exposing large amounts of their personal data from an early age, the misuse of which can lead to life-threatening harm.

Our approach, and therefore that of the law itself and its constantly necessary modifications, should in future be more preventive than reactive, and should thus seek to prevent possible abuse. It is important, therefore, to change our personal approach to data protection first and foremost, and to start paying attention, for example, to the service providers we choose that protect our privacy and the integrity of our data, while at the same time ensuring that we set the highest possible privacy settings on social networks, or invest more in services that protect our passwords. The future of data protection will therefore depend primarily on our personal approach, and the importance we give to protecting sensitive personal information. We cannot expect the law to meet such conditions before us.