UNIVERZITA KARLOVA

Právnická fakulta

Tomáš Jansa

Ochrana osobních údajů v EU

Biometrické údaje

Diplomová práce

Vedoucí diplomové práce: JUDr. Tereza Kunertová, LL.M., Ph.D.

Katedra: Evropského práva

Datum vypracování práce (uzavření rukopisu): 16. 04. 2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval/a samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 139 216 znaků včetně mezer.

……..

Tomáš Jansa

V Praze dne

Poděkování

Děkuji své vedoucí diplomové práce, JUDr. Tereze Kunertové LL.M., Ph.D., za ochotu vést mou diplomovou práci, trpělivý přístup, a především cenné rady, které mi během psaní práce poskytovala. Zvláštní poděkování patří také Ing. Šárce Tětěrukové a mé rodině za podporu, které se mi během studií dostávalo.

Obsah

Úvod 1
1 Systém práva na soukromí a ochrana osobních údajů 3
1.1 Vývoj práva na soukromí a ochrany osobních údajů na území Evropy 3
1.2 Vývoj práva na ochranu osobních údajů v EU 8
1.3 Právní úprava ochrany osobních údajů v USA 15
2 Základní principy 19
2.1 Právní principy ochrany osobních údajů 19
2.1.1 Zásada zákonnosti, korektnosti a transparentnosti 20
2.1.2 Zásada účelového omezení 21
2.1.3 Zásada minimalizace údajů 22
2.1.4 Zásada přesnosti 22
2.1.5 Zásada omezení uložení 24
2.1.6 Zásada integrity a důvěrnosti 25
3 Komplexnost pojmu osobních údajů a jejich zpracování 27
3.1 Osobní údaj 27
3.2 Anonymní údaj 30
3.3 Zvláštní kategorie osobních údajů 31
3.4 Zpracování osobních údajů 32
4 Biometrické údaje 33
4.1 Biometrický údaj jako technický pojem 35
4.2 Biometrický údaj jako právní pojem 36
4.3 Rizika automatizovaného zpracování biometrických údajů 38
5 Biometrické údaje v aplikační praxi 41
5.1 Biometrické údaje a bankovnictví 41
5.2 Biometrické údaje a podpisy 45
5.3 Biometrické údaje a cestovní doklady 47
5.4 Biometrické údaje a Schengenský informační systém 52
5.5 Biometrické údaje a národní identifikační karty 53
5.6 Biometrické údaje a pracovněprávní praxe 54
Závěr 56
Seznam zkratek 58
Seznam použitých zdrojů 59
Abstrakt 71

Úvod

Ochrana osobních údajů se stává čím dál tím více diskutovaným tématem. Její relevance stoupá spolu s rychlostí vývoje výpočetní techniky, její využitelností a dostupností, a právě proto si autor práce vybral toto téma. Téma ochrany osobních údajů zaměřené na biometrické údaje představuje skloubení práva a technologií, kdy obě sféry spadají do oblasti zájmu autora.

V 21. století svět zažil doslova revoluci na poli elektronických zařízení a internetu. Svět se nachází v době, kdy je zcela nemyslitelné, či obtížně představitelné, počínat si v každodenním životě bez využití jakéhokoliv druhu technologie. Lidská závislost na internetu, mobilních telefonech, cloudech mají však neblahý důsledek svěření svých údajů dalším stranám. Jedná se o daň, kterou osoba zaplatí dobrovolně, v zájmu zachování svého pohodlí. Kdy jindy, než dnes bylo možno pouhým dotykem prstu na obrazovce odeslat zprávu, vyfotit fotografii či odeslat jinou osobní informaci. Nakupování se stává hračkou, vše z pohodlí domova.

Osobní údaje jsou pojmem, který bude člověka provázet po celý život. Jedná se o identifikační znaky, které náleží osobám, jako jednotlivcům. Dají se také považovat za jednu z nejvýznamnějších hodnot 21. století, cennější než diamanty a drahé kovy. V březnu roku 2018 prolétla médii zpráva o bezostyšném nakládání s osobními údaji ze strany společnosti Facebook, která vzbudila vlnu nevole a volající po účinné právní úpravě, především v USA. Veřejnosti známá Zuckerbergova společnost prodala osobní údaje 87 milionů lidí firmě Cambridge Analytica, bez jejich vědomí, jejichž data se stala ornou půdou pro vytvoření algorytmu na podporu prezidentské kampaně Donalda Trumpa v USA. Taková je síla shromážděných a chytře uplatněných osobních údajů.

Dnešní doba umožňuje zpracování široké škály osobních údajů. Lze se s ním setkat nejen ze strany veřejnoprávních subjektů, shromažďování k účelům pro vytvoření dokumentů ve formě občanských, řidičských průkazů, či cestovních pasů, ale také ze strany soukromoprávních subjektů. Těmi jsou i výrobci spotřební elektroniky. Celá řada mobilních telefonů, či notebooků obsahuje čtečku některého z biometrických údajů, ať už se jedná o otisk prstů, sken celého obličeje nebo duhovky.

Cílem této práce je proto představit právní úpravu ochrany osobních údajů především ve vztahu k biometrickým údajům. Biometrické údaje představují jakýsi současný magnum opus konjunkce práva a technologií.

V první fázi se jeví jako nezbytně nutné vymezit historický kontext původu ochrany osobních údajů, a to hlavně ve vztahu k právu na soukromí, jež představuje esenciální základ ochrany osobních údajů. Pochopení historického kontextu a uchopení teoretického základu představuje fundamentální aspekt správného ukotvení problematiky. Je to ten hlavní důvod proč autor volí právě tuto cestu. Tato metoda současně zprostředkovává pochopení právního rámce, jež se dotýká problematiky osobních údajů a současně umožňuje provést jistou komparaci mezi právem na ochranu osobních údajů v USA a v Evropské unii.

Teoretický kontext autor vymezí za pomoci objasnění právních principů pojících se k celému právnímu řádu a také těch, jež jsou zakotveny a uplatňovány pouze ve vztahu k ochraně osobních údajů. Současně je nezbytné vymezit obecnou terminologii problematiky, bez které je jen velmi obtížné se seznámit s danou oblastí.

Následně se autor blíže zaměří na pojem samotného biometrického údaje a rozebere jej jak z právního, tak technologického hlediska. Protože, jak již bylo avizováno výše, pochopení obou dvou rovin je nezbytné.

Po překonání historického a teoretického kontextu se autor práce zaměří na nejčastější odvětví výskytu užívání biometrických údajů, pokusí se je analyzovat a nastíní nejčastější způsoby aplikace biometrických údajů. Současně se autor zaměří na nejčastější problémy dotýkající se jednotlivých oblastí a pokusí se o jejich rozbor.

V závěru práce autor zhodnotí celkový výstup, ke kterému došel, a zda-li se mu podařilo naplnit tyto cíle vytyčené v úvodu práce.

1 Systém práva na soukromí a ochrana osobních údajů

Tato kapitola se zaměřuje na historický vývoj ochrany osobních údajů v nutném spojení s vývojem práva na soukromí. Ochrana osobních údajů je pouze jedním z prvků práva na soukromí a je nezbytné ji chápat v jisté provázanosti. Rozboru podléhá právní úprava území Evropy, dále současné Evropské unie, ale také území USA. Důvodem pro zahrnutí otázky ochrany dat v USA je její následné porovnání se současnou úpravou v Evropské unii ve vztahu k biometrickým údajům.

1.1 Vývoj práva na soukromí a ochrany osobních údajů na území Evropy

Ochrana osobních údajů se utvářela ruku v ruce spolu s vývojem a dostupností výpočetní techniky, a to hlavně v 70. letech 20. století, kdy technologie nebyly ani zdaleka na takové úrovni jako dnes. Počítače zaplňovaly celé místnosti a chytrá mobilní zařízení byla něco zcela nepředstavitelného. Při vrácení se zpět v čase a při současném zaměření se na přistání Apolla 11 na Měsíci, samotný naváděcí počítač měl procesor o výkonu 1 MHz a 1 kb RAM. Což je při současných hodnotách více než úsměvné. Vícejaderné procesory, pracující ve vysokých frekvencích se nachází nejenom ve stolních počítačích, ale i noteboocích a hlavně mobilních telefonech a i dostupnost pamětí RAM je vyšší, než kdykoliv předtím. Při srovnání průměrného počítače v roce 2018 se frekvence procesoru pohybuje ve 3,3-3,7 GHz a paměť RAM 8 GB.[1]

Ochrana osobních údajů však náleží do širší kategorie lidských práv, nazývanou právo na soukromí. Pokud lze někomu přisuzovat jednu z prvních definic práva na soukromí, byli to právě Američané Louis Brandeis a Samuel Warren, kteří jej označili jako *"právo na to být ponechán o samotě"* a to již v roce 1890 dlouho před jakoukoliv ucelenou právní úpravou práva na soukromí.[2]

[1]MCKANE, JAMIE. *The average gaming PC – 5 years ago vs today.* [online]. [2018-12-31]. Dostupné z: https://mybroadband.co.za/news/gaming/262481-the-average-gaming-pc-5-years-ago-vs-today.html

[2]WARREN, SAMUEL, BRANDEIS, LOUIS. *The Right to Privacy.* Harvard Law Review, Vol. 4, No. 5, 1890. [online]. [2018-03-12]. Dostupné z: https://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

Čím vůbec lze rozumět právo na soukromí? I v 21. století se jedná o pojem obecný a stále dynamicky se vyvíjející. Byť L. Brandeis a S. Warren částečně uhodili hřebík na hlavičku, nelze předpokládat, že se dotkli pojmu soukromí v celé své komplexnosti, protože pojem soukromí dnes a v roce 1890 nelze zcela ztotožňovat. Soukromí nemůžeme chápat jen jako právo jednotlivce být ponechán v poklidu, ale vyplývá z něj také zřejmě povinnost počínat si tak, aby nedocházelo k zásahům do soukromí druhých. Vyvíjelo se pozvolna. Protože právo v prvopočátcích pokrývalo pouze zásahy do lidského života a majetku, tedy právo na život, či právo vlastnit majetek. Jedná se o práva přirozená, vycházející ze samotné podstaty člověka a jeho intelektu. A až následně se začíná objevovat ochrana této velmi osobní sféry každé lidské bytosti. Historický vývoj ochrany soukromí na území Evropy lze spatřovat již od období 2. světové války, konkrétně 16. prosince 1948 spolu s přijetím Všeobecné deklarace lidských práv (dále jen VDLP) na půdě Organizace spojených národů (dále jen OSN). Byť nezávazná deklarace položila základy veškerému budoucímu rozvoji ochrany soukromí.[3] Fundamentem této deklarace pro účely ochrany soukromí se stal její čl. 12, který stanoví: *"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."*[4] Lze vyčíst, že zcela poprvé nelze chápat ochranu soukromí pouze jako abstraktní hodnotu, ale jako statek, kterému náleží adekvátní ochrana. A jak zmiňuje profesor sociologie Hans Joas z Chicagské univerzity, právě tato deklarace byla těmi nejlépe explicitně vyjádřenými hodnotami, kterými se lidstvo mohlo pochlubit v době, kdy se svět nacházel v poválečné éře. [5]

Aktivní činnost OSN v problematice lidských práv však zde nekončila. O několik let později došlo k přijetí dvou, tentokrát závazných, mezinárodních úmluv. Staly se jimi Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, přičemž pro účely této práce za zmínku stojí čl. 17 první, z výše zmíněných úmluv, jež apeluje na prevenci před svévolným zasahováním do soukromého života, rodiny, domova nebo korespondence, a že každý má právo na zákonnou ochranu před těmito zásahy, či útoky.[6] Byť

[3]USTARAN, EDUARDO. *European privacy: law and practice for data protection professionals.* Portsmouth, NH: International Association of Privacy Professionals, c2012. Str. 3-15

[4]Všeobecná deklarace lidských práv ze dne 10. 12. 1948. čl. 12

[5]JOAS, HANS. *Max Weber and the Origin of Human Rights: A Study on Cultural Innovation*. [online]. [2018-03-14]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=923846

[6]Mezinárodní pakt o občanských a politických právech ze dne 19. 12. 1966.

přijetí těchto smluv bylo stiženo negociačními problémy v důsledku dvou odlišných názorových bloků, svět se přece jenom náchazel v poválečném období a ze spojeneckých velmocí si každá ráčila uzmout svého místa na slunci, jsou kompromisem, jež lze považovat za jistý minimální garantovaný standard lidských práv.[7]

Na poli evropského území nepůsobila jen jedna mezinárodní organizace. Státy pod vlajkou Rady Evropy v Římě v roce 1950 udaly další směr trendu ochrany soukromí přijetím Úmluvy o ochraně lidských práv a základních svobod. Důležitost této úmluvy lze dovodit z její závaznosti pro členské státy Rady Evropy, stejně tak jako povinnosti nových členských států Rady Evropy ratifikovat tuto úmluvu. Dalším přínosem úmluvy bylo zřízení Evropského soudu pro lidská práva ve Štrasburgu (dále jen ESLP), který zajišťuje nejen dodržování této úmluvy, ale působí také jako poslední odvolací instance po vyčerpání všech vnitrostátních opravných prostředků. Nicméně rozhodování ESLP se stalo stěžejním pro určitou oblast práva na soukromí. Právě ESLP přispěl svým rozhodnutím ve věci Niemietz v. Germany[8] k deskripci statku soukromí, kde se ve svém judikátu vyslovil, že soukromím je nutno chápat také právo člověka na utváření a rozvíjení vztahů s dalšími lidskými bytostmi. Byť čl. 8 výše zmíněné úmluvy garantuje jistou míru ochrany soukromí a do jisté míry kopíruje standard poskytnutý VDLP, poprvé v této úmluvě se setkáváme s možností zásahu veřejné moci do práva na soukromí *„státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti.“*[9]. Z definice článku vyplývá primárně povinnost státních orgánů nezasahovat do těchto práv vyjma případů taxativně vyjmenovaných. Úmluva nepostrádá smysl ani dnes. Evropská unie se ve Smlouvě o EU (dále jen SEU) zavazuje nejen k přistoupení k úmluvě, ale zároveň konstatuje, že práva obsažená tvoří obecné zásady práva Unie *„Základní práva, která jsou zaručena Evropskou úmluvou o ochraně lidských práv a základních svobod a která vyplývají z ústavních tradic společných členským státům, tvoří obecné zásady práva Unie“*.[10]

[7]POTOČNÝ, MIROSLAV; ONDŘEJ, JAN. *Mezinárodní právo veřejné: zvláštní část*. 6. dopl. a rozš. vyd. V Praze: C.H. Beck, 2011. Beckovy právnické učebnice. Str. 100

[8]ESLP ve věci 13710/88 ze dne 16. prosince 1992 Niemietz v. Germany

[9]Úmluva o ochraně lidských práv a základních svobod ve znění protokolů 3, 5 a 8 ze dne 4. 11. 1950. V ČR publikováno jako Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb.

[10] Smlouva o Evropské unii, Úřední věstník Evropské unie, C 202, 7. června 2016. Čl. 6 odst. 1 a 2

Vedoucí roli v letech 1960-1980 v oblasti ochrany soukromí tvořily Německo, Francie, Švédsko, Norsko, Rakousko, Španělsko a Portugalsko, přičemž poslední tři výše zmíněné státy nabyly největšího významu. Tyto zcela prvně zakomponovaly ochranu osobních údajů jako základní lidské právo ve svých ústavách.[11] Toto období bylo stiženo také velkým rozkvětem technologií, jež dopadly především na problematiku automatizovaného zpracování informací. Z tohoto důvodu se usnesl Výbor ministrů Rady Evropy na Úmluvě 108 (Úmluva na ochranu jednotlivců ve vztahu k automatickému zpracování osobních údajů).[12]

Za zmínku stojí také přínos Organizace pro hospodářskou spolupráci a rozvoj (dále jen OECD). Ve spolupráci s Radou Evropy byl vydán specifický dokument Pokyny pro ochranu soukromí a přeshraniční přechod osobních údajů.[13] Tento dokument se sestával z osmi fundamentálních principů:

1. Omezení sběru osobních údajů – nastavení limitů pro sběr osobních dat spolu se zákonnými důvodu a jen tam, kde je to vhodné, spolu s vědomím či souhlasem subjektu
2. Kvalita osobních údajů – údaje by měly být užívány jen v souladu se stanoveným účelem, měla by být přesná a úplná
3. Specifikace účelu – údaje sesbírané ke specifickému účelu jsou omezeny na tento účel
4. Omezení užití – osobní údaje nesmí být zveřejněny, učiněny dostupnými nebo jinak použité pro jiné než stanovené účely
5. Bezpečnostní záruky – osobní údaje by měly být dostatečně zabezpečeny před ztrátou, zničením, použitím, úpravou nebo nedovoleným přístupem
6. Princip otevřenosti – měla by být nastavená politika otevřenosti ohledně osobních údajů, což znamená, že subjekty zpracovávající osobní údaje by měly být v každém případě schopny určit účel zpracování apod.

---

[11]USTARAN, EDUARDO. *European privacy: law and practice for data protection professionals*. Portsmouth, NH: International Association of Privacy Professionals, c2012. Str. 3-15

[12]Agentura Evropské unie pro základní práva. *Handbook on European data protection law*. Belgie, 2014. [online]. [2018-03-12]. Dostupné z: http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law str. 15-17

[13]Berkeley Lawschool. *Research Guide to European Data Protection Law*. [online]. [2018-03-12]. Dostupné z: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1001&context=leg_res

7. Individuální participace – subjekty údajů by měly mít jistá práva ve vztahu k správci osobních údajů
8. Odpovědnost – správce by měl být odpovědný za dodržování opatření, jež jsou uvedeny ve výše uvedených principech[14]

Úprava vytyčená těmito pokyny byla i nadále nezávazná a právní ochrana osobních údajů napříč Evropou proto ve vzájemném nesouladu, kdy každý stát aplikoval svůj právní řád. Po přijetí pokynů lze spatřovat snahy OECD o uznání pokynů ze strany USA, nicméně USA nepodstoupily jediný krok k jejich implementaci. Ačkoliv se jednalo o formu doporučujících principů, jejich význam je zcela nesporný. Při přijímání směrnice 95/46/EC je EU vtělila právě do této sekundární legislativy, která se prostřednictvím požadavku transpozice dočkala aplikace v právních řádech států EU.[15]

Zde práce OECD nekončí. V roce 2005 uvedlo velmi pokrokový dokument dotýkající se biometrických údajů. Konkrétně se jedná o Zprávu o pokroku v souvislosti s aplikací principů Úmluvy 108, vzhledem ke shromažďování a zpracování biometrických údajů.[16] Nutnost odůvodňovalo OECD hlavně rychlým vývojem technologií. Dochází k častějšímu výskytu využití otisků prstů, jakož i dalších biometrických údajů a je zapotřebí adekvátní reakce. Nejedná se jen o účely čistě soukromoprávní nebo veřejnoprávní, ale také bezpečnostní. Svět se nachází v období po tragickém 11. září 2001, kdy došlo k sérii plánovaných teroristických útoků na tzv. „dvojčata“. Teroristé užívají mnoha identit, a právě biometrické údaje by mohly být tím, co umožní jejich efektivní identifikaci.[17] Problematice biometrických údajů však budou věnovány samostatné kapitoly, které pokryjí nejenom jejich právní, ale také technologický význam.

[14]OECD. *„Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [online]. [2019-04-10]. Dostupné z: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[15]*tamtéž*

[16]Council of Europe. *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*. 2005. [online]. [2018-03-12]. Dostupné z: https://rm.coe.int/16806840ba

[17]*tamtéž*

1.2 Vývoj práva na ochranu osobních údajů v EU

Evropská unie vznikla v roce 1993 na základě Smlouvy o Evropské unii, tzv. Maastrichtské smlouvy. Následně od účinnosti Lisabonské smlouvy nahrazuje Evropské společenství a je jeho nástupkyní. Založena je na dvou smlouvách, Smlouvě o Evropské unii (dále jen SEU) a Smlouvě o fungování Evropské unie (dále jen SFEU), zapomínat se nesmí na Listinu základních práv EU, jíž je propůjčena závaznost primárních smluv prostřednictvím čl. 6 odst. 1 SEU. V unijní úpravě můžeme i nadále za jakýsi základní stavební kámen právní úpravy ochrany soukromí považovat výše zmíněnou Evropskou úmluvu o ochraně lidských práv a základních svobod, jež byla inspirací pro vytvoření právní úpravy práva na ochranu soukromí v Evropské unii. Požadavek na revizi práva na ochranu osobních údajů se však začíná objevovat až po roce 2009, spolu s přijetím Lisabonské smlouvy.[18]

Do této doby byla v platnosti směrnice 95/46/EC.[19] Tato směrnice se sestávala z 34 článků zabývajících se právě úpravou ochrany osobních údajů a soukromí. Jelikož se jedná o specifický druh sekundární legislativy, státy byly povinny ji transponovat, a to ve lhůtě 3 let. Svého času se jednalo o jediný právní akt EU, který se přímo dotýkal otázek sběru, zpracovávání a uchovávání osobních údajů.[20]

Směrnice 95/46/EC s sebou přinesla určitá nova. Článek 29 zakotvil vytvoření Pracovní skupiny pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (dále jen WP29). Jednalo se o nezávislou, poradní skupinu, která posuzovala otázky dotýkající se aplikace vnitrostátních předpisů k provedení této směrnice, jakož i zaujímala stanoviska o úrovni ochrany v Evropském společenství a třetích zemích. A dále také poskytovala poradenství v oblasti návrzích změn této směrnice.[21]

---

[18]KUNER, CHRISTOPHER. *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law.* 2012. [online]. [2018-03-12]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781

[19]Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů

[20]YU, P. K. *An Introduction to the EU Directive on the Protection of Personal Data*. 2001. [online]. [2018-03-13]. Dostupné z: http://www.peteryu.com/gigalaw0701a.pdf

[21]Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů. Čl. 29

Neméně důležitou směrnicí se stala také směrnice 2002/58/ES, tzv. ePrivacy směrnice, jež platí dodnes. Tato směrnice především harmonizuje předpisy členských států, jelikož stejně jako u směrnice 95/46/ES se dotýká záležitostí, které se neřídí právem Evropského společenství. Cílem směrnice je především poskytnutí ochrany práva na soukromí ve vztahu ke zpracování osobních údajů v odvětví elektronických komunikací.[22] V souvislosti s touto směrnicí se hovoří o jejím nahrazení nařízením, více níže.

V srpnu roku 2003 WP29 zveřejnila práci nazvanou „Pracovní dokument o biometrických údajích z roku 2003". Tento dokument reagoval na předpokládaný vzestup aplikace biometrických údajů, a to nejen ve vztahu k Evropské unii, ale také k USA, kde biometrické údaje hrály významnou roli v cestovních pasech pro tzv. „entry-exit" systém pro cizince.[23] V rámci práce došlo k vytyčení tří základních principů biometrických údajů bez ohledu na to, zda-li byly užity k autentifikaci/verifikaci, či identifikaci osoby, jsou jimi:

1. Universalita – náleží každému člověku, typicky DNA, otisk prstu, či sken duhovky
2. Jedinečnost – vztahující se pouze ke konkrétnímu jedinci
3. Trvalost – neměnné v čase[24]

Evropská komise 19. května 2009 hostila konferenci vztahující se k problematice ochrany osobních údajů, při zohlednění technologického pokroku a nově i cloudových uložišť.[25] Součástí

[22]Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Recitál a Čl 1

[23]KINDT, ELS J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis.* Springer. [online]. [2018-03-12]. Dostupné z: https://books.google.cz/books?id=EvbHBAAAQBAJ&pg=PR4&lpg=PR4&dq=978-94-007-7522-0&source=bl&ots=YGw33z9TPN&sig=nlZZer5evGoAQ-hkOBpGxeRwwgQ&hl=en&sa=X&ved=0ahUKEwjnvomnv8TaAhWDK5oKHQDFApUQ6AEILzAB#v=onepage&q=978-94-007-7522-0&f=false Str. 76-78

[24]Article 29 Working Party. *Working document on biometrics.* Adopted on 1 August 2003; 12168/02/EN, WP 80 [online]. [2018-03-12]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

[25]WILHELM, ERNST-OLIVER. *A brief history of the General Data Protection Regulation.* [online]. [2018-03-12]. Dostupné z: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

byl pak i panel dotýkající se ochrany osobních údajů v globalizovaném světě se zvýšenou mobilitou.[26]

1. prosince 2009 WP29 publikovala dokument nazvaný „The Future of Privacy". Ten na jednu stranu podporuje a uznává doposud uznávané principy v oblasti ochrany osobních údajů, ale zároveň apeluje na modernizaci právní úpravy. Stává se totiž nezbytným dostatečně reflektovat současný vztah společnosti a jejího práva na soukromí.[27]

V roce 2011 se udály dvě důležité události pro ochranu osobních údajů. První z nich bylo přijetí stanoviska evropského inspektora ochrany údajů ke sdělení Komise - „Komplexní přístup k ochraně osobních údajů v EU". Jak vyplývá ze samotného znění dokumentu, inspektor sdělení podporuje a současně vyžaduje po Komisi vyšší ambice, které by mohly vést ještě k účinnější právní úpravě. Vytyčuje problematické rysy, na které dosavadně platná směrnice 95/46/EC není schopna reagovat, typicky, cloud computing, behaviorálně cílená reklama, či sociální sítě. Tento okruh je označován jako technologický vývoj. Druhým je vnímána globalizace, a to především ve spojení s růstem přeshraničního zpracovávání a mezinárodního předávání údajů. Třetím je Lisabonská smlouva a čtvrtým je souběžný vývoj probíhající v souvislosti s mezinárodními organizacemi.[28] Druhou událostí se stalo oznámení Paula Nemitze, ředitele pro základní práva z Generálního ředitelství Evropské komise, o připravované harmonizační úpravě pro ochranu osobních údajů.[29]

Pokud lze nějaký rok považovat za ten, kdy bylo skutečně započato s prací na GDPR, je jím rok 2012. V tomto období Evropská komise navrhla reformu ve formě Návrhu nařízení

[26] NEZMAR, LUDĚK. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. str. 14

[27]TÜRK, ALEX. *The Future of Privacy*. 2009. [online]. [2018-03-14]. Dostupné z: http://194.242.234.211/documents/10160/10704/WP168++The+Future+of+PrivacY

[28]Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - *„Komplexní přístup k ochraně osobních údajů v Evropské unii"* (2011/C 181/01) [online]. [2018-03-14]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:181:FULL:CS:PDF

[29]Gesellschaft für Datenschutz und Datensicherheit. *Einheitliches Datenschutzrecht in Europa durch Verordnung*. Kolín, 2011. [online]. [2018-03-14]. Dostupné z: https://www.gdd.de/aktuelles/startseite/news/einheitliches-datenschutzrecht-in-europa-durch-verordnung

Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a volném pohybu těchto údajů 5853/12.[30] Zpravodajem v Evropském Parlamentu byl ustaven Jan Philipp Albrecht, který je i v současné době specialistou na ochranu osobních údajů. V dnešní době například rozporuje důvody návrhu Evropské Komise na zavedení povinných biometrických občanských průkazů, více v kapitole 5.5.[31] Na návrhu nařízení se podílela od jeho zárodků řada výborů, například výbor pro Průmysl, výzkum a energetiku, pro Hospodářství a měnu, pro Právní záležitosti, ale stěžejní roli hrál výbor pro Občanské svobody, spravedlnost a vnitřní věci. [32]

Stejného roku vypracovala polská advokátní kancelář spolu s německými akademiky z Institutu evropských právních studií publikaci v původním znění. „Reforming the Data Protection Package“, jež byla publikována i Evropským parlamentem. Tento dokument vyzdvihoval technologie, na něž by měla být poutána největší pozornost s ohledem na zpracování dat. Zahrnoval geolokační služby, cloud computing, online gaming, ale také biometrické technologie (rozpoznávání obličejů). Více k tomuto dokumentu, z hlediska přístupu k biometrickým údajům bude pojednáno v kapitole 3.

Výše zmíněný Reforming the Data Protection Package se v jedné ze svých kapitol zaobírá především právní úpravou rozpoznávání obličejů. Konstatuje jejich častější výskyt jak v soukromém, tak veřejném sektoru, ale zároveň jej poprvé explicitně zmiňuje ve vztahu k fotografiím umístěným na sociálních sítí. Důvod k apelu je dán tím, že takovýto technologický pokrok umožňuje nejen zachycení fyzické schránky člověka, ale také jeho emoce, či nálady, tedy jeho psychologickou stránku. Což je velmi důležité z hlediska uplatňování v rámci smart-monitoring systémů. Jeden z velmi pokročilých užívá v současné době Čína.[33] Na základě tohoto

[30]Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) /kód dokumentu 5853/12, KOM (2012) 11 v konečném znění, 2012/0011 (COD)/

[31]BLENKINSOP, Philip. KOESTER, Samantha. EU Commission proposes making fingerprints mandatory in ID cards. Reuters [online]. [2019-01-19]. Dostupné z: https://www.reuters.com/article/us-eu-security/eu-commission-proposes-making-fingerprints-mandatory-in-id-cards-idUSKBN1HO23A

[32]European Parliament. 2012. Dostupné z: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en

[33]RUSSEL, JOHN. *China's CCTV surveillance network took just 7 minutes to capture BBC reporter.* 2017. [online]. [2018-04-10]. Dostupné z: https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/

pozorování je totiž možno dospět nejen k prevenci, ale také k predikci vzorce určitého chování sledovaných subjektů. Dokument přímo zmiňuje ty nejjemnější pohyby lidského těla, jako je pohyb očí, mrkání, ale také rychlost dechu, chvění hlasu, či tlukot srdce. Takovéto možnosti s sebou samozřejmě přináší velmi účinný prostředek v boji s kriminalitou. Nicméně s mocí přichází zodpovědnost. Data takového kalibru je zapotřebí někde uchovávat a zpracovávat. Jejich zneužití by mohlo vést k závažným problémům. Jedná se o citlivé údaje, které obsahují informace o rase, etniku apod. a je zapotřebí je zpracovávat v souladu s principem proporcionality.[34]

Problémem ustavení nové regulace byla její forma. Ve sledu debat se orgány a státy vyjádřily ve prospěch jak nařízení, tak směrnice. Komise samotná byla pro přijetí nařízení, nicméně ostatní aktéři spíše pro přijetí směrnice.[35] Nařízení lze vnímat jako legislativu, kterou lze považovat za jistý zákon celounijní působnosti. Tedy, tam, kde vyžadujeme úpravu zahrnující všechny členské státy, bez diskuze. Charakteristickými prvky je jeho přímý účinek a přímá použitelnost za naplnění příslušných podmínek (viz test Van Gend en Loos).[36] Což byl jeden z hlavních argumentů Komise – neponechat státům žádnou míru flexibility při úpravě ochrany osobních údajů a stanovit tak dostatečně pevný unijní rámec na regionální úrovni. Směrnice by naopak vyžadovala transpozici a implementaci směrnice do vnitrostátních právních řádů, což by se mohlo jevit jako problematické a nedošlo by k vytvoření vhodné právní úpravy.[37] Nicméně i přesto GDPR působí v současné době poměrně flexibilně, kdy umožňuje celou řadu odchylek. Je na členských státech, aby si ve vymezených oblastech formou adaptačního zákona stanovily svoje vlastní pravidla nebo výjimky.[38]

Nepřipravenost jednotlivých států, ale především organizací působících v Evropské unii na připravované nařízení se projevila už v roce 2013. Nezávislá studie vypracovaná London

[34]European Parliament. 2012. Directorate-General for Internal Policies. *Reforming the Data Protection Package.* Dostupné z: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET(2012)492431_EN.pdf

[35]Debate in Council 2012/0011 (COD) – 25/10/2012 [online]. [2019-01-19]. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1232253&l=en&t=E

[36]Jasnost, platnost, nepodmíněnost a není nutnost, aby bylo konkretizováno národním právním řádem

[37]TOMÁŠEK, MICHAL, TÝČ, VLADIMÍR a MALENOVSKÝ JIŘÍ. *Právo Evropské unie*. Praha: Leges, 2013. Student (Leges). str. 107-110

[38]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. 6 (2, 3), 8 (1), 9 (2a, 4), 10, 23 apod.

Economic‘s v detailu popisuje problematiku jak finanční stránky věci, tedy nákladů, které bude nutno vynaložit na uspokojivý přechod v souladu s novým nařízením, tak na komplikace čekající na podniky v souvislosti s dodržováním nového nařízení. Zmiňovány byly především právo být zapomenut, minimalizace údajů, či právo na omezení zpracování.[39]

Návrh se v průběhu let dočkal řady změn. Jeden z výborů Evropského parlamentu, výbor pro Občanské svobody, spravedlnost a vnitřní věci apeloval na modifikaci tehdejšího návrhu. Předmětem byly hlavně přísnější sankce, či upřesnění „one-stop“ mechanismu. Modifikace se dočkaly velké podpory a umožnily jejich projednání před Radou EU.[40]

Byť GDPR začínalo být čím dál tím více zvučné. Jeho přijetí se neobešlo bez komplikací a odkladů. Hlasy proti se ozývaly především z půdy Francie, Německa a Velké Británie. Právě výše zmíněný „one-stop“ mechanismus, představoval problematický aspekt. Občanům členských států by se tím dostala do rukou mocná zbraň v možnosti podání stížnosti na jakékoliv porušení ochrany osobních údajů napříč všemi členskými státy EU u jejich místní autority. Tedy, v případě, že by došlo k porušení ze strany Německa, občan České republiky by si mohl stěžovat u svého domovského úřadu a obejít tak institucionální uspořádání v Německu. Což samozřejmě větším státům nebylo po chuti a namítaly, že by tím došlo k narušení jejich suverenity a apelovaly na přijetí směrnice namísto nařízení, která umožňuje větší míru flexibility.[41]

V roce 2015 pověřenec pro ochranu osobních údajů Giovanni Buttarelli řekl: *„Na ochraně soukromí a osobních údajů záleží lidem více než kdykoliv předtím. Poprvé v historii EU máme možnost modernizovat, harmonizovat a zjednodušit pravidla, jak jsou osobní údaje zpracovány. Tato pravidla musí být vytvořena tak, aby byla relevantní pro budoucí generace technologií…“*

---

[39]Implications of the European Commision´s proposal for a general data protection regulation for business, London Economics [online]. [2019-01-19]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf str. 7-9

[40]HOGAN LOVELLS. *EU draft Data Protection Regulation: the LIBE Committee amendments*. [online]. [2019-01-19]. Dostupné z: https://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf str. 1

[41]FLEMING, JEREMY. *EU lawmaker warns of data protection rules delay till 2016.* [online]. [2019-01-19]. Dostupné z: https://www.euractiv.com/section/digital/news/eu-lawmaker-warns-of-data-protection-rules-delay-till-2016/

Současně došlo ke spuštění mobilní aplikace, která umožňovala evropským zákonodárcům se snázeji orientovat v návrzích ze strany Komise, Evropského parlamentu a Rady EU.[42] Nicméně i přesto, že docházelo k finalizaci nařízení, se na něj snesla vlna kritiky, a to hlavně z úst Loretty Lynch, generálního prokurátora Spojených států, a to hlavně v souvislosti s teroristickými útoky, jež se udály v Paříži a Kalifornii. Jejími argumenty byly především, že žádný z národů nemůže oponovat terorismu sám. GDPR podle ní vytváří neúnosný systém restrikcí na možnou přeshraniční spolupráci orgánů potírajících kriminalitu. A v samotném důsledku dojde k usnadnění vykonání teroristických útoků, kdy sami teroristé se budou moci spolehnout na nedostatky tohoto systému.[43] Avšak ani tyto argumenty nezabránily krokům kupředu. 17. prosince 2015 se výbor pro Občanské svobody, spravedlnost a vnitřní věci usnesl na formálním textu GDPR, včetně těch nejdůležitějších ustanovení týkajících se práva být zapomenut nebo dětí užívajících sociální sítě, kdy dítě, které nedosahuje stanoveného věku, si může založit účet na sociální síti pouze se souhlasem svých rodičů.[44] Následujícího dne se Výbor stálých zástupců (dále jen „COREPER“) usnesl na textu, jež byl výsledkem kompromisu mezi Evropským parlamentem a Komisí. COREPER představuje nejspíše nejdůležitější článek, jež zprostředkovává kontakt mezi Evropskou komisí a členskými státy, je tvořen stálými zástupci členských států a je půdou pro přípravu a projednávání legislativních návrhů, o nichž následně rozhoduje Rada.[45] Tímto se kola daly do pohybu a samotnému přijetí Radou a Evropským parlamentem už nic nebránilo. Akt samotný byl podepsán 27. dubna 2016, vstoupil v platnost 24. května 2016 a od 25. května 2018 dochází k jeho uplatňování.[46]

---

[42]Volný překlad autora: *„Privacy and data protection matter more than ever to people. For the first time in a generation the EU has an opportunity to modernise, harmonise and simplify the rules on how personal information is handled. These rules must be relevant for the next generation of technologies…“*

EDPS. *Opening a new Chapter for Data Protection.* [online]. [2019-01-19]. Dostupné z: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2015-06-edps_gdpr_en.pdf

[43]HOLDEN, MICHAEL. *Attorney General Lynch Chides EU decisions to restrict data sharing.* Reuters. [online]. [2019-01-19]. Dostupné z: https://www.reuters.com/article/us-usa-security-europe/attorney-general-lynch-chides-european-decisions-to-restrict-data-sharing-idUSKBN0TS0UV20151209

[44]Evropský parlament. *New EU rules on data protection put the citizen back in the driving seat.* Press release. [online]. [2019-01-19]. Dostupné z: http://www.europarl.europa.eu/news/en/press-room/20151217IPR08112/new-eu-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat

[45]O/DOK. *COREPER I/II.* [online]. [2019-04-10]. Dostupné z: https://help.odok.cz/vykladovy-slovnik/-/wiki/Výkladový%20slovn%C3%ADk/COREPER+I%3CSLASH%3EII

[46]KOMÍNKOVÁ, MAGDA. *Jak vznikalo GDPR*. [online]. [2019-01-19]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

V souvislosti s GDPR je také hojně diskutovaným tématem přijetí tzv. ePrivacy nařízení, jež by mělo zrušit dosavadní ePrivacy směrnici. Byť tato směrnice byla novelizována v roce 2009, tato novelizace je často označována jako „cookie zákon“, ozývá se čím dál tím více hlasů volajících po modernější právní úpravě v Evropské unii.[47] Z důvodové zprávy návrhu plyne, že došlo k podstatnému technologickému a ekonomickému vývoji. Podniky i spotřebitelé jsou čím dál tím více úžeji vázáni na využití služeb elektronických komunikací a velice často se stává, že tento typ služeb není pokryt stávající směrnicí. Dalším podstatným bodem je také vazba na GDPR. Původní plán byl, že obě dvě nařízení začnou platit současně, nicméně ePrivacy nařízení i dnes stále v platnosti není. ePrivacy nařízení bude představovat, v případě přijetí, právní úpravu lex specialis vůči GDPR, které bude působit jako lex generalis.[48]

Závěrem lze jen dodat, že Working Party 29 se přijetím GDPR stala European Data Protection Board, která podporuje a uznává vybrané dokumenty vydané Working Party 29. European Data Protection Board je vytvořena jako nezávislý orgán, odpovědný za správnou a konzistentní aplikaci GDPR.[49]

1.3 Právní úprava ochrany osobních údajů v USA

Přístup USA k ochraně osobních údajů je velmi problematický. Jakožto demokratická federativní prezidentská republika nemají ucelenou federální právní úpravu, která by se dotýkala výhradně ochrany osobních údajů. Namísto toho existuje široká škála aktů, které fragmentárně upravují osobní údaje ve vztahu k určitému odvětví. Typicky se jedná o oblast finanční, zdravotnictví, popř. elektronické komunikace. Americký Kongres si je velmi vědom tohoto nedostatku, i ve světle nových událostí, kauza Cambridge Analytica a Facebook, a s každým

[47]ARROWS advokátní kancelář, s. r. o. *ePrivacy a nařízení a GDPR.* [online]. [2019-01-19]. Dostupné z: https://www.epravo.cz/top/clanky/eprivacy-narizeni-a-gdpr-107391.html

[48]Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) Důvodová zpráva

[49]The European Data Protection Board. *Endorsement 1/2018.* [online]. [2019-04-08]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

volebním obdobím se objevují nové propozice pro jednotnou právní úpravu, byť neúspěšně.[50] Cílem této podkapitoly však není všeobsáhle pokrýt celou právní úpravu ochrany osobních údajů v USA, ale spíše jen vytyčit ty nejdůležitější z aktů, dotýkající se této oblasti práva.

Nejznámějším z těchto na určité odvětví zaměřených aktů je The Federal Trade Commission Act (dále jen FTC Act). FTC Act byl přijat Kongresem v roce 1914, jehož hlavním cílem je ochrana spotřebitele a zamezení protisoutěžního jednání.[51] Na základě Sekce 5 FTC Actu došlo k vytvoření Federální Obchodní Komise. Jedním z prvních federálních zákonů, přijatých komisí v oblasti ochrany osobních údajů byl tzv. Fair Credit Reporting Act. Tento akt byl v roce 2003 novelizován jako Fair and Accurate Credit Transactions Act. Tento akt byl původně přijat z důvodu ochrany osob před negativním hodnocení jejich úvěroschopnosti. V 60. letech bylo zcela běžné, aby docházelo k užívání uměle vytvořených negativních informací, či neúplných informací o úvěruschopnosti subjektu. Mimo jiné ale osoby, jež sdružovali tyto informace, obstarávaly i takové informace, jež zcela nesouvisely s poskytováním úvěru, např. jak udržují doma čistotu, jejich koníčky apod.[52]

Dalším z právních předpisů je Gramm Leach Billey Act. Tento právní předpis upravuje ochranu osobních údajů ve vztahu k finančním institucím. Ve své hlavě V., nazvané „Soukromí“ obsahuje ustanovení týkající se neveřejných informací daného subjektu. Tedy, že veškeré finanční instituce musí respektovat soukromí svých klientů, jakož i chránit jejich bezpečnost a důvěrnost. Finanční instituce musí také užívat příslušné technické, organizační a jiné standardy, aby zabezpečily výše zmíněné hodnoty a předcházely tak hrozbám, či útokům směřujícím proti údajům daných subjektů.[53]

---

[50]JOLLY, IEUAN. *Data protection in the United States: overview.* 2017. [online]. [2018-04-12]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[51]LANG, JAMES C. *The Legislative History of the Federal Trade Commission Act*. 1974. [online]. [2018-04-13]. Dostupné z: http://heinonline.org/HOL/LandingPage?handle=hein.journals/wasbur13&div=14&id=&page=

[52]ICLG. *The International Comparative Legal Guide to: Data Protection 2018*. 5th Edition [online]. [2019-03-18]. Dostupné z: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

[53]113 STAT. 1338 Public Law 106-102, 106th Congress, *The Gramm Leach Billey Act,* [online]. [2019-03-18]. Dostupné z: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf Hlava V, čl. 501 a násl.

Dalším z aktů je Health Information Portability and Accountability Act, který upravuje ochranu osobních údajů hlavně ve vztahu ke zdravotním službám. Jedná se o informace o zdravotním stavu pacienta. Touto problematikou se zabývá článek 221, který obsahuje právní normu vyžadující vytvoření programu, jež je cílen proti podvodům v oblasti zdravotní péče a zneužívání sběru dat od subjektů. Dochází tím k vytvoření informační povinnosti zdravotnických institucí a apelu, aby zajistily, co největší míru důvěrnosti osobních údajů svých pacientů.[54]

Ochrana před spamem je v USA chráněna za pomoci CAN-SPAM Act. Tento právní předpis se z hlediska ochrany osobních údajů dotýká především „opt-out" mechanismu při zasílání reklamy prostřednictvím e-mailu. Stanovuje tudíž technické požadavky na zasilatele těchto e-mailů s cílem předejít nevyžádané korespondenci. Zároveň vymezuje, aby došlo ke zřetelnému označení e-mailu, zda-li se jedná o reklamní či jinak nabídkový e-mail, adresu odesílatele, za současného umožnění zrušení odběru těchto e-mailů.[55]

Zvláštní ochrany se dočkávají děti. Tato oblast je upravena Children's Online Privacy Protection Act. Tento právní předpis především zakazuje podvodné jednání ve vztahu k nakládání s osobními informacemi dětí, tedy, dle tohoto předpisu, osobami mladšími 13 let. Musí být zajištěna bezpečnost, důvěrnost a integrita informací shromážděných od dětí. Stejně tak při shromáždění informací za současného respektování hodnot uvedených výše je možno takovéto informace poskytnout dále pouze za současného ujištění, že entita, jíž budou poskytnuty, bude výše uvedené hodnoty taktéž respektovat.[56]

Dalšími akty jsou například The Video Privacy Protection Act nebo The Telephone Consumer protection Act, které se dotýkají opět dalších oblastí v rámci právní úpravy ochrany osobních údajů. Je nutno si uvědomit, že se jedná, jak již byl nastíněno výše, o právní úpravu, jež je velmi

[54]110 STAT. 1936 PUBLIC LAW 104-191, 104th Congress, *The Health Information Portability and Accountability Act,* [online]. [2019-03-18]. Dostupné z: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf Hlava II, čl. 221

[55]117 STAT. 2708 PUBLIC LAW 108-187, *CAN-SPAM Act,* [online]. [2019-03-18]. Dostupné z: https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf čl. 5

[56]15 U.S.C. 6501-6506, *The Children's Online Privacy Protection Act* [online]. [2019-03-18]. Dostupné z: https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5

rozkouskována a je nezbytné mít na paměti, že státy samotné, v rámci federace, mohou přijímat právní předpisy stejné či přísnější než ty, jež jsou federální povahy.[57]

[57]ICLG. *The International Comparative Legal Guide to: Data Protection 2018*, 5th Edition [online]. [2019-03-18]. Dostupné z: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

2 Základní principy

Autor se domnívá, že pro správné pochopení právní úpravy ochrany osobních údajů je zapotřebí nejen vysvětlit obecně institut právního principu napříč právními řády, ale také objasnit principy speciální ve vztahu k ochraně osobních údajů. Evropské právo stejně jako národní právní systémy jsou tzv. objektivním právem. Objektivní právo představuje souhrn právních norem jako obecně závazných pravidel uznaných, či stanovených státem, popř. mezinárodním společenstvím států. Stěžejním prvkem je právní norma. Nicméně existují i další prvky, jež je nutno zmínit. Jedním z takových je právní princip. Právní principy jsou obecné regulativní ideje, na kterých stojí právní řád. Od právních norem se odlišují především jejich mírou abstraktnosti a mohou mít také kontradiktorní charakter. Mezi nejznámější principy patří např. *zásada pacta sunt servanda* nebo *ignoratia legis non excusat*. Právní principy tvoří nedílnou součást právního řádu a v rámci mezinárodního a v tomto případě především evropského práva dochází k jejich formulaci prostřednictvím rozhodovací činnosti Soudního dvora Evropské unie. Právní principy jsou důležité jak z hlediska normotvorby, tak z hlediska aplikace práva. Zákonodárce je dodržuje, aby zachoval konzistenci právního řádu a orgány aplikující právo je uplatňují k řešení složitých případů.[58]

2.1 Právní principy ochrany osobních údajů

Tato podkapitola pojednává o právních principech zpracování dle nařízení. K jejich nalezení postačí nahlédnout do článku 5 GDPR jež zprostředkovává jejich znění. Nařízení je velmi komplexním právním aktem, a proto pro správnou interpretaci jednotlivých článků je zapotřebí je chápat vždy ve vztahu k odpovídajícím částem recitálu. Porušením principů se subjekt vystavuje hrozbě pokuty až do výše 20 000 000 EUR či 4 % ročního obratu. Odpovědnost dodržovat principy je břemenem správce, který musí být schopen doložit soulad mezi zpracováním osobních údajů a zněním článku 5 GDPR.[59]

[58]GERLOCH, Aleš. *Teorie práva*. 5., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). str. 19-34

[59]VOIGT, PAUL. von dem BUSSCHE, AXEL. *The EU General Data Protection Regulation (GDPR).* Spring International Publishing 2017. str. 87

2.1.1 Zásada zákonnosti, korektnosti a transparentnosti

Úvodní princip článku 5 GDPR se sestává ze 3 ústředních pojmů. Při zpracování osobních údajů je zapotřebí dodržet zákonnost, korektnost a transparentnost. Aby bylo zpracování zákonné je zapotřebí zpracovávat osobní údaje tím způsobem, aby došlo k naplnění alespoň jednoho z právních titulů vyjmenovaných v čl. 6 odst. 1 GDPR.[60] Jedním z takovýchto titulů je udělení souhlasu ze strany subjektu údajů. Souhlas má svá specifika. Pokud dochází ke zpracování osobních údajů, daný souhlas musí být prokazatelný. Správce musí být v každé situaci schopen doložit, že souhlas byl ze strany subjektu osobních údajů dán. Navazujícími atributy souhlasu je jeho informovanost a svoboda vyjádření. V prvém případě je nezbytně nutné, aby subjekt údajů znal totožnost správce a účely zpracování a zároveň, že subjekt má zajištěnou skutečně svobodnou volbu. V situacích, kdy subjektu hrozí újma z důvodu nemožnosti souhlas odvolat, nejedná se o souhlas svobodně daný. Nedílnou součástí zásady legitimity zpracování je transparentnost. Tedy, že *„všechna sdělení týkající se zpracování těchto osobních údajů budou snadno přístupné a srozumitelné…“* S principem transparentnosti se lze setkat téměř na denní bázi, byť může být do značné míry přehlížen. Typickým porušením principu transparentnosti je například jeden z posledních případů, kdy společnosti Google byla uložena pokuta ze strany francouzského regulátora Commission Nationale de l`Informatique et des Libertés. V této kauze Google při zakládání nových účtů u telefonů s operačním systémem Android porušoval GDPR. Nejdůležitější informace, jakými jsou účel zpracování osobních údajů, doba uchování údajů, nebo kategorie údajů dále zpracovávané pro individualizaci reklam byly velmi často rozkouskovány po celé řadě dokumentů. Tím znemožňovaly novým uživatelům telefonů se řádně s těmito podmínkami seznámit. Regulátor argumentoval i přímým počtem prokliknutí, které byly nezbytné k tomu, aby se uživatel složitým způsobem propracoval k potřebným informacím. Zpravidla i po nalezení těchto informací, se jednalo o informace kusé s obecnými či vágními termíny.[61] Transparentnost je velice úzce spjata s korektností.[62] Obě tyto zásady lze spatřovat v praxi nejčastěji v povinnosti informovat subjekt údajů o zpracování v v rozsahu, který je uložen článkem 13 a 14 GDPR.

[60]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. Str. 106

[61]CNIL. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC.* [online]. [2018-04-12]. Dostupné z: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[62]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.. Recitál 39, 41, 42, 43

Závěrem lze podotknout, že původní směrnice 95/46/ES neobsahovala pojem transparentnosti a uváděla pouze korektnost a hranice mezi těmito dvěma zásadami se velmi často stírají.[63]

2.1.2 Zásada účelového omezení

Účelové omezení zpracování dat je rigidní restrikcí. Článek 5 odst. 1 písm. b) GDPR stanoví: *„Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.“* Zde by si autor dovolil uvést příklad zpracování osobních údajů ze strany školy. Obecně, ve vztahu ke zpracování fotografií ve školách mohou nastat 2 situace, vztáhneme-li tuto problematiku k českému právnímu řádu a evropské legislativě. Prvou situací je pořizování a zveřejňování fotografií z činností školy. Příkladmo, jedná se o ilustrativní fotografie, kde není zjevná podoba žáků. Fotografie jsou vystaveny na webu školy, popř. v tištěné podobě. Velmi často se jedná o fotografování školních akcí, výstavek a činností studentů. V tomto případě se však nejedná o případ spadající pod GDPR a uplatní se právní úprava ochrany osobnosti, resp. právo na ochranu soukromí dle § 84 zákona č. 89/2012 Sb., občanský zákoník. Důvodem pro tento postup lze spatřovat v samotné definici osobního údaje dle GDPR *„osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě.“*[64] Právě ona identifikovatelnost[65] zde představuje bariéru pro uplatnění postupu dle GDPR. Nedochází zde k možnosti určení osoby. Pokud by ale k takovýmto fotografiím došlo k návaznosti a byly by opatřeny údaji, např. ze školní matriky, zde už se dostáváme do kolize s GDPR.[66] Typickou situací by mohla být propagace školy pro reklamní letáky. K tomuto se vyjadřuje metodická pomůcka ministerstva školství mládeže a tělovýchovy. V takovémto případě je již zapotřebí vyžadovat souhlas se zpracováním osobních údajů a užívat následně poskytnuté údaje pouze v souladu s účelem, ke kterému byly poskytnuty.[67]

---

[63] NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. Str. 106-107

[64] 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. 1

[65] Více k identifikovatelnosti v podkapitole 3.1.

[66] UOOU, Q&A *Ze školství* [online]. [2019-02-01]. Dostupné z: https://www.uoou.cz/ze-skolstvi/ds-5088/p1=5088

[67] MŠMT. *Metodická pomůcka k aplikace obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství.* [online]. [2019-02-01]. Dostupné z: http://www.msmt.cz/file/44592/ str. 28

2.1.3 Zásada minimalizace údajů

Zásada minimalizace údajů představuje určitou brzdu v rozsahu zpracování osobních údajů. Fundamentálním prvkem je zpracování přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu.[68] Vazba k předchozí zásadě je zcela nesporná. Příkladem by mohl být podnik, jehož sféra poskytovaných služeb se omezuje na online prostředí a prostřednictvím e-mailu zasílá reklamní nabídky svým recipientům. V tomto případě je namístě posoudit, přiměřenost a relevantnost takového zpracování. Pro tyto účely lze říci, že nezbytnost opatření osobních údajů lze limitovat na e-mailovou adresu, popř. jméno recipienta. Adekvátní, a tedy pro tyto účely vyhovující již ale není zpracování, které by šlo nad rámec účelu, např. společnost nepotřebuje získat informace o datu narození, bydlišti nebo náboženské afiliaci adresáta. Další příklad by mohl představovat kupon na městskou hromadnou dopravu, obsahující čip a jméno adresáta jak napsané na vrubu kuponu, tak uchované v elektronické podobě na čipu. Zde vyvstává otázka, jakým způsobem by mělo dojít k ověřování platného jízdného. Jakmile jsou data uchována v elektronické podobě na čipu, pak je zcela očividné, že musí existovat centrální uložiště takovýchto dat. V této situaci je pak jako nejvhodnější řešení, a tedy v souladu se zásadou minimalizace údajů, uplatnit kontrolu jízdného nikoliv cestou porovnávání údajů obsažených v čipu s centrální databází, ale spíše vytvořit např. čárový kód, unikátní pro daný kupon, který poslouží jako prostředek verifikace platného jízdného.[69]

2.1.4 Zásada přesnosti

Zásada přesnosti představuje především požadavek, aby nebyly zpracovávány údaje, jež jsou neaktuální. Taková data pak musí být vymazána nebo opravena.[70] Již za účinnosti směrnice 95/46/EC byla považována za důležitý princip. V roce 2009 Evropský soudní dvůr judikoval

[68]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. 5 odst. 1 písm. c)

[69]Council of Europe. *Handbook on European data protection Law.* 2018, [online]. [2019-02-01]. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf

str. 126

[70]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. 5 odst. 1 písm. d)

v případě M.E.E. Rijkeboer, že směrnice požaduje po členských státech nejenom umožnit přístup k informacím ohledně recipientových zpracovaných osobních údajů, ale také zajistit, aby zpracované osobní údaje byly aktuální vzhledem k přítomnosti, ale i minulosti. V případu šlo o spor mezi nizozemským občanem a městem Amsterodam. Rijkeboer požadoval, aby byl upozorněn na všechny případy zpracování osobních údajů ze strany lokální autority a jejich sdělení třetím stranám. Jeho požadavek byl především zjistit, komu byla poskytnuta jeho předchozí adresa v době 2 let od učinění jeho podání. Amsterodam mu vyhověl pouze částečně *„…mu sdělil pouze informace týkající se období jednoho roku před jejím podáním“*, proti čemuž podal opravný prostředek. Spor se vlekl, až se dostal před Evropský soudní dvůr ve formě řízení o předběžné otázce. Evropský soudní dvůr konstatoval, že *„subjekt se může ujistit, zda jsou jeho osobní údaje zpracovávány bezchybně a přípustným způsobem, což zejména znamená, že jsou základní údaje, jež se jej týkají, správné a že jsou určeny oprávněným příjemcům.“*[71] Směrnice 95/46/ES ve svém čl. 12 stanovovala právo na přístup, a tedy právo subjektu získat od správce potvrzení ohledně účelů zpracování, kategorií údajů, ale i příjemců, kategorií příjemců, kterým jsou údaje sdělovány. GDPR toto právo přejímá a rozšiřuje ve svém článku 15 a zároveň zakotvuje nárok na první bezplatnou kopii této informace *„Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie… může účtovat přiměřený poplatek.“*[72]

V souvislosti se zásadou přesnosti je také závěrem nutno zmínit právo na opravu zakotvené v GDPR *„Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají.“*[73] Z ustanovení však nevyplývá přímo povinnost správce aktivně nacházet nepřesné osobní údaje, nýbrž povinnost na základě žádosti subjektu údajů opravit nepřesné údaje.[74]

[71]Rozsudek ESD ve věci C-553/07 ze dne 7. května 2009 ve věci College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer

[72]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. 15 odst. 3

[73] *tamtéž* čl. 16

[74]Úřad ochrany osobních údajů. *Základní příručka k GDPR.* [online]. [2019-02-01]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=4728

2.1.5 Zásada omezení uložení

Zásada omezení uložení osobních údajů vypovídá o povinnosti smazání a anonymizování osobních údajů od okamžiku, kdy není zapotřebí je uchovávat pro účely, pro které byly zpracovávány. Z tohoto principu však existuje výjimka pro vědecké, historicky výzkumné nebo statistické účely, kde z povahy logiky věci je samotným smyslem výše uvedených činností uložení údajů po zpravidla dlouhé časové úseky. Nicméně i přesto musí být dosažen určitý standard technických a organizačních opatření z důvodu ochrany osobních údajů subjektu.[75] Princip omezení uložení je úzce vázán na dobu, po kterou jsou osobní údaje zpracovávány. Doba může být stanovena buďto určitě, tedy, kdy uložení osobních údajů bude pevně časově ohraničeno nebo relativně, kdy bude vázána na příslušnou událost, kupříkladu poskytování určité služby. Je tudíž nezbytné, aby doba nepřekročila dobu nezbytnou pro naplnění účelu zpracování.[76] Objasnění tohoto principu se věnuje judikát Evropského soudu pro lidská práva ve věci S. & Marper v. UK. Stěžovatelům, jež byli zadrženi a obviněni z loupeže, byly odebrány otisky prstů a vzorky DNA před samotným uskutečněním soudního řízení, které se však následně ani nekonalo. Stěžovatelé se tedy domáhali zničení vzorků DNA a otisků prstů. Odvolací soud v UK byl však proti. Stěžejním bodem argumentace soudu se stala skutečnost, že otisky prstů i DNA vzorky obsahují pouze omezené množství informací o jejich nositeli. Sněmovna lordů taktéž smetla stížnost ze stolu s argumentací, že shromáždění těchto údajů není diskriminační a nezakládá stigmatizaci stěžovatelů. Po vyčerpání všech opravných prostředků se tedy stěžovatelé obrátili na Evropský soud pro lidská práva, který v jejich věci rozhodl, že nekonečně dlouho trvající shromáždění otisků prstů, jakož i DNA vzorků a profilů stěžovatelů bylo neproporcionální, a nikoliv nutné v demokratické společnosti a tím spíše v situaci, kdy k samotnému řízení před soudem vůbec nedošlo.[77]

[75]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. 5 odst. 1 písm. e)

[76]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. Str. 114

[77]ESLP ve věci 30562/04 a 30566/04 ze dne 4. prosince 2008 S. and Marper v. the UK

2.1.6 Zásada integrity a důvěrnosti

Posledním z principů je zásada integrity a důvěrnosti. Je nutno si v každém případě uvědomit, že osobní údaje představují natolik citlivé informace o subjektech, že jejich zneužití může mít katastrofální následky. GDPR stanovuje povinnost pro náležité zabezpečení osobních údajů a jejich ochranu prostřednictvím vhodných opatření. Ta mohou být jak organizačního nebo technického rázu, jak stanoví čl. 32 GDPR. Jedním z prostředků zabezpečení se stává pseudonymizace. Nesmí být však zaměňována s anonymizací. Anonymizace je de facto nevratný proces. Po jejím uplatnění již nebude nikdy možné zpětně dohledat nositele osobního údaje.[78] Pseudonymizace na druhé straně umožňuje jisté „zašifrování" osobního údaje jeho nositele za současného umožnění jeho zpětné identifikace. Příkladmo: Jan Novák, narozen 1. 6. 1992, bydlištěm Praha, rodné číslo 4783/0672; J.N. 92 Pha. 4/2[79]. Na pseudonymizaci odkazuje čl. 25 GDPR, jež ji označuje jako *vhodné technické a organizační opatření*.[80] Proces pseudonymizace umožňuje takové zpracování osobních údajů, že nelze rozpoznat jejich nositele bez toho, aniž by byly předem získány dodatečné informace. Na výše uvedeném příkladu došlo k pseudonymizaci všech údajů. Nicméně rovina volby údajů, jež mají být pseudonymizovány, je čistě subjektivní. Z hlediska důležitosti by nejspíše autor zařadil právě rodné číslo zcela nejvýše, protože automaticky vypovídá o dvou údajích, a to o pohlaví a věku osoby, nicméně i přesto samo o sobě bez znalosti dalších údajů zneužitelné není.[81] Na což reaguje například i česká legislativa, že rodné číslo není řazeno do zvláštní kategorie osobních údajů.[82] Dalšími prostředky zabezpečení jsou schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, dále schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických problémů a v poslední řadě proces pravidelného testování, posuzování a

[78]K anonymizaci více v podkapitole 3.2.

[79]ŠKORNIČKOVÁ E. *Anonymizace a pseudonymizace.* [online]. [2019-02-01]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/

[80]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. 25

[81]NEZMAR, LUDĚK. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. str. 115-118

[82]Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, § 4 písm. b), současně by však autor chtěl upozornit na probíhající legislativní proces zákona o zpracování osobních údajů, jež v době psaní této práce prošel Senátem a byl k 2. 4. 2019 doručen prezidentu republiky k podepsání

hodnocení účinnost zavedených technických a organizačních opatření k zajištění bezpečnosti zpracování.[83]

V případě porušení zabezpečení osobních údajů ukládá GDPR povinnost správci, bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu. Pokud není ohlášení učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.[84] Za porušení zabezpečení lze označit náhodné či protiprávní zničení, změna, ztráta nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Ne vždy je však nutno porušení zabezpečení hlásit, pokud nenastane riziko pro práva a svobody fyzických osob, pak není stanovena povinnost porušení zabezpečení hlásit, i přesto je však nutnost jej alespoň zadokumentovat.[85]

[83]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. 32

[84]*Tamtéž* čl. 33

[85]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. Str. 296-297

3 Komplexnost pojmu osobních údajů a jejich zpracování

Cílem této kapitoly je uvedení některých základních pojmů v oblasti ochrany osobních údajů. Znalost pojmosloví se jeví nezbytnou pro pochopení různorodé problematiky ochrany osobních údajů. Předmětem bude nejenom vymezení samotného pojmu osobního údaje, ale také jeho možné kategorizace v souladu s platnou právní úpravou.

3.1 Osobní údaj

Osobní údaj představuje fundamentální pojem v oblasti ochrany osobních údajů. V českém právním řádu vymezen: *„osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. 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“*[86] Jedná se tedy o takový údaj, jaký se dotýká fyzické osoby, jež je nebo může být určena. Taková osoba je pak určena či určitelná, pokud pomocí jednoho, či více osobních údajů lze určit její identitu. Nezáleží na tom, o jaký osobní údaj jde a na jeho počtu, může se jednat o jeden konkrétní údaj, jakým je např. fotografie, ale spíše se lze častěji setkat s většími počty údajů. Je nutno si uvědomit, že zákon o ochraně osobních údajů však pokrývá jen případy, které odpovídají definici osobního údaje, v případě, že definice není naplněna, užívají se příslušná ustanovení občanského zákoníku.

V evropském měřítku jej definuje čl. 4 GDPR jako *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“), identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat…“*[87] V minulosti byla právní úprava osobních údajů obsažena ve směrnici 95/46 ES v čl. 2 písm. a) *„osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné osobě (dále jen „subjekt údajů“), identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat…“*[88] Tato

[86]Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, § 4 písm. a)

[87]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 73

[88]KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony.

definice měla původ v Úmluvě Rady Evropy č. 108, ale směrnice tuto definici rozšířila. Dle úmluvy se osobním údajem rozuměly pouze *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“).“*[89] Byť definice je poměrně široká, což nesporně představuje úmysl zákonodárců, je současně nezbytné mít na paměti, že k jejímu formování docházelo i prostřednictvím činnosti moci soudní. Konkrétně se jedná o činnost Evropského soudního dvora, kdy v případě Breyer v. Deutschland, soud konstatoval, že za osobní údaj je nutno považovat i dynamickou IP adresu.[90]

Z definice osobního údaje je nutno vyložit stěžejní pojmy.

Identifikovatelnost neboli určitelnost subjektu nastává v situaci, kdy je správce, či zpracovatel nebo kterákoliv jiná osoba schopna subjekt identifikovat bez ohledu na původ osobních údajů. Subjekt lze označit za identifikovaný nebo identifikovatelný, pokud jej správce nebo zpracovatel dokáže rozlišit od ostatních osob. Rozsah údajů potřebných k identifikaci je ale již přímo závislý na daném případě.[91] GDPR se stejně jako směrnice 95/46 EC vyjadřuje k pojmu identifikovatelnosti. Při stanovení, zda je subjekt určitelný by se mělo přihlédnout ke všem prostředkům, které lze použít pro přímou nebo nepřímou identifikaci. Preambule doporučuje např. výběr vyčleněním.[92] Tyto prostředky mají také svá rozhodná kritéria, která je zapotřebí brát v potaz. Jedním z faktorů jsou náklady na provedení identifikace, dalším zamýšlený účel zpracování, či zájmy jednotlivců nebo organizační selhání. V každém případě je však nutno chápat identifikaci jako dynamický prvek. Je důležité zajistit dostatečný nadhled nad dostupnými technologiemi v současnosti a jejich možnému vývoji v budoucnosti. Pokud v současné době prostřednictvím daného prostředku nelze provést identifikaci, to ještě neznamená, že identifikace nenastane v budoucnu v důsledku technologického vývoje daného prostředku. Současně je zapotřebí uchovávat v paměti na jakou dobu je plán údaje uchovat. Systém by měl být tudíž

[89]Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28. 1. 1981. Čl. 2 písm. a)

[90]Rozsudek ESD ve věci C-213/15 ze dne 19. října 2016 Patrick Breyer v. Spolková republika Německo

[91]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 78

[92]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. Preambule 26

proveden takovým způsobem, který umožní dynamické a flexibilní reakce na všechny v budoucnu vzniklé možnosti a překážky.[93]

Dále jsou to veškeré informace. Jak již bylo uvedeno výše, zcela očividným záměrem zákonodárce bylo pojmout osobní údaj co nejširším způsobem. To však ponechává prostor k širokému výkladu. V zásadě se lze zaměřit na okruh obsahu, povahy a formátu informací. Co se týče obsahu informací, pak je namístě zmínit, že se jedná o všechny relevantní druhy informací vztahující se k subjektu. Může se jednat jak o zcela soukromou sféru jednotlivce, zahrnující jeho blízké vztahy, ale také informace dotýkající se jeho aktivního se podílení na ekonomické, či pracovněprávní činnosti. Dalším z termínů je povaha informací. Povaha informací má subjektivní a objektivní rovinu. Objektivní rovina je určitým měřítkem, kterou je možno zprostředkovat určité výsledky, např. procento tuku v těle. Subjektivní rovina je již blíže spjata například s ideologií subjektu. V poslední řadě se jedná o formát informací. Formát informací je představován médiem, jež figuruje jako nositel informací. Do jisté míry značně závislý na technologickém vývoji. Jedná se o celou řadu způsobů uchování informací. Typicky se jedná o prostý text, čísla, kódy, šifry, obrazy, fotografie, či zvuky. V této souvislosti je na místě zmínit biometrické údaje (jejichž vysvětlení je k nalezení v kapitole 4). Unikátním aspektem biometrických údajů je, že mohou být obsahem informace o konkrétní fyzické osobě, např. retinální sken, ale současně také obsahují úzkou vazbu na konkrétní fyzickou osobu, protože náleží jenom jí.[94]

Závěrem lze podotknout, že GDPR oproti směrnici přineslo dva nové druhy informací, které lze považovat za určovatele subjektu. Jedná se o síťové identifikátory a lokační údaje. Lokační údaj umožní zjistit údaje o místě pohybu či pobytu subjektu. Dalším je síťový identifikátor *„fyzickým osobám mohou být přiřazeny síťové identifikátory, které využívají jejich zařízení, aplikace, nástroje a protokoly, jako například adresy internetového protokolu či identifikátory cookies, nebo jiné identifikátory, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob*

[93]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko č. 4/2007 k pojmu osobního údaje přijaté dne 20. června 2007.* [online]. [2019-02-01]. Dostupné z: https://www.uoou.cz/files/wp29-stanovisko_4-2007.pdf str. 15

[94]*tamtéž* str. 8

a k jejich identifikaci.“[95] Za síťové identifikátory považujeme takové, které jsou uplatňovány v rámci elektronických sítích např. IP adresa, cookies apod. K tomu, aby síťový identifikátor naplnil svůj účel, je nezbytné, aby zde existovala pevná vazba mezi příslušným zařízením a jeho vlastníkem. Tedy, že je možno dovodit, že z důvodu, že je dané zařízení ve vlastnictví dané osoby, bude používáno touto osobou.[96]

3.2 Anonymní údaj

Jedna z odnoží osobních údajů je tzv. anonymní údaj. Anonymní údaj představuje určitý kontrast oproti osobnímu údaji. Obecně platí, jak již bylo zmíněno výše, že principy ochrany osobních údajů se vztahují jen na informace vztahujících se k identifikovaným nebo identifikovatelným subjektům. Proto by se tyto zásady neměly vztahovat na anonymní informace, protože ty se netýkají určené nebo určitelné fyzické osoby, ani na osobní údaje, jež prošly procesem anonymizace, tedy kdy fyzická osoba přestala být identifikovatelnou.[97] Pokud se výše zmíněné uvede na příkladu, pak první skupina anonymních údajů představuje informace zcela obecné, jako např. počet dešťových srážek, a druhá skupina představuje takové údaje, které byť by bylo za jejich pomoci možno identifikovat daný subjekt, není to možné, protože prošly procesem anonymizace.[98]

Proces anonymizace byl obsažen taktéž v recitálu 26 směrnice 95/46/ES. Mimo jiné je také upraven v recitálu 26 e-Privacy směrnice: *„Provozní údaje používané pro marketing komunikačních služeb nebo pro poskytování služeb s přidanou hodnotou by měly být po poskytnutí služby vymazány nebo anonymizovány“*[99] Směrnice se tedy staví k procesu anonymizace ve

[95]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. Preambule 30

[96]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 79-82

[97]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. Recitál 26

[98]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 83

[99]Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Recitál 26

stejném duchu jako GDPR v současné době. Jak již bylo uvedeno v předchozí kapitole týkající se základních principů, anonymizace je nevratný proces. Napříč právním řádem neexistuje žádný závazný řád, který by stanovoval, jakým způsobem má být anonymizace v dané situaci provedena. Je však zapotřebí mít na paměti také rizika, jež vyplývají z procesů anonymizace, prvním je, když správce nesprávně postaví na roveň pseudonymizaci a anonymizaci. Dalším je, že užití anonymizace zbavuje jednotlivců bezpečnostních záruk anebo jaký dopad může mít užití anonymizovaných údajů na profilování.[100] Anonymizace může být provedena znáhodněním, zobecněním. Znáhodnění je metoda, kterou dochází k úpravě atributů, které zamezí spojení mezi anonymizovanými údaji a původními atributy. Zobecnění je technika, která v zásadě zobecní termíny, které by vypovídaly konkrétně o dané osobě, příkladmo, namísto uvedení města, či ulice, kde daná osoba žije, se uvede stát. I když se proces anonymizace může zdát jako dostatečně efektivní, i přesto může představovat určitá slepá místa. A v samotném důsledku bude vždy na správci dat, aby předem vymyslel systém, který bude dostatečně efektivní, všepokrývající a poskytne tím dostatečné záruky ochrany soukromí.[101]

3.3 Zvláštní kategorie osobních údajů

GDPR stejně jako směrnice 95/46/ES stanovuje existenci zvláštních kategorií osobních údajů. Podle čl. 9 odst. 1 GDPR jsou jimi osobní údaje vypovídající o rasovém, či etnickém původu, o politických názorech, náboženském vyznání, či filozofickém přesvědčení nebo členství v odborech, dále genetické údaje, biometrické údaje, pokud jsou zpracovány za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.[102] Oproti výše zmíněné směrnici přibyly údaje genetické a biometrické, které jsou důležité pro účely této práce. Genetickým údajem se rozumí takový údaj, jež se týká zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace

[100]Poznámka autora: profilováním se rozumí technika, která umožňuje zpracování osobních údajů se záměrem získání předpovídajících informací na základě profilu, který byl vytvořen z atributů, preferencí apod. Umožňuje tedy predikovat chování dané osoby.

[101]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko 5/2014 o Anonymizačních Technikách, přijato 10. dubna 2014.* [online]. [2018-04-11]. Dostupné z: https://www.pdpjournals.com/docs/88197.pdf

[102]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. 13 14 a 9 odst. 1

o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby. Biometrický údaj bude blíže nadefinován v kapitole 4. Nařízení nepracuje ve svých článcích s terminologií „citlivého osobního údaje“, nýbrž s pojmem „zvláštních kategorií osobních údajů“. Pojem citlivého osobního údaje lze však dohledat v recitále nařízení, který stanovuje, že pro tyto typy údajů je poskytnuta členským státům míra autonomie pro stanovení vlastních pravidel pro zpracování těchto údajů *„Toto nařízení rovněž poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů („citlivé osobní údaje“). V tomto rozsahu nařízení nevylučuje, aby právo členského státu stanovilo okolnosti konkrétních situací, při nichž dochází ke zpracování, včetně přesnějšího určení podmínek, za nichž je zpracování osobních údajů zákonné.“*[103] Na tyto typy údajů se také vztahují přísnější povinnosti a jejich zpracování je možno provádět pouze za splnění jedné z taxativně vypočtených podmínek v čl. 9 odst. 2 GDPR za současného naplnění obecného titulu pro zpracování dle čl. 6 odst. 1 GDPR, více v kapitole 4.2.[104]

3.4 Zpracování osobních údajů

Jedním z pojmů a činností, které jsou nedílně spojeny s osobními údaji je zpracování osobních údajů. Zpracování osobních údajů je stejně jako osobní údaj definováno v čl. 4 GDPR jako: *„jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění seřazení či zkombinování, omezení, výmaz nebo zničení.“*[105] Výčet postupů zpracování není uzavřený, jedná se o demonstrativní výčet. Přičemž nezáleží na tom, jakým způsobem je zpracování prováděno tzn. bez ohledu na zpracování v elektronické či jiné formě.

[103]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. Recitál 10

[104]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 162-164

[105]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. 2

4 Biometrické údaje

Pojem biometrický údaj pochází z řeckého „bios“, jež je významem shodné s „život“ a „metron“, tedy „změřit“ (biologické, tedy fyziologické a anatomické vlastnosti, ale také behaviorální charakteristiky). Výskyt prvních biometrických údajů ve formě otisků prstů lze datovat na několik desítek tisíc let nazpět, ačkoliv přesné období nelze přesně určit. Jejich existenci lze dovodit z nástěnných maleb v jeskyních, dříve obývanými prehistorickým člověkem. Kdy každá z těchto maleb byla označena právě otiskem prstu. Ten sloužil jako jistý podpis autora díla. To však není jediný důkaz jejich původu. Kupříkladu ve starověkém Babylonu sloužil otisk prstu jako forma stvrzení obchodní transakce. Tehdejší obchody byly realizovány za pomocí hliněných desek, které nesly právě toto označení.[106] Nejde jen o znaky jedinečnosti, ale také o znaky univerzality.

Jedinečnost biometrických údajů spočívá v možnosti učinit distinkci mezi tím, či oním člověkem. Byť existují ojedinělé případy shody těchto znaků mezi několika jednotlivci, lze hovořit o poměrně přesném atributu. V roce 1892 provedl Francis Galton první kalkulaci pravděpodobnosti dvou shodných otisků prstů ve společnosti. Vycházející z tehdejšího stavu populace na Zemi, tedy zhruba 1,6 mld. obyvatel, došel k závěru, že šance na shodu mezi dvěma jednotlivci se pohybuje okolo 1:64000000.[107]

Univerzalitu dovozujeme z jejich všudypřítomnosti. Každý člověk, pokud například nebyl účasten nehody nebo se nenarodil s fyziologickou vadou, disponuje těmito znaky.

Souvisejícím pojmem s biometrickým údajem je vědní odbor nazývaný biometrie. Cílem biometrie je analýza člověka z hlediska jeho charakteristických rysů. I biometrie má své charakteristické pojmosloví, bez něhož se pro její správné pochopení nelze obejít.

V zásadě lze vymezit tyto čtyři základní pojmy:

1. Rozpoznávání – termín označující rozpoznávání člověka dle tělesných vlastností

[106]MAYHEW, STEPHEN. *History of Biometrics*. 2018. [online]. [2018-04-11]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

[107]STIGLER, STEPHEN, M. *Perspectives; Galton and Identification by Fingerprintes*. Statistics Department, Chicago. [online]. [2018-04-11]. Dostupné z: http://www.genetics.org/content/140/3/857

2. Ověření – rovněž označován jako verifikace, umožňuje potvrdit totožnost jedince při užívání šablony, tedy již v minulosti sejmutým vzorkům, tzv. „one-to-one“ princip
3. Autentifikace – často splývá s pojmem rozpoznávání, nicméně zde na konci procesu získává osoba určitý pozitivní nebo negativní status
4. Identifikace – v zásadě shodná s ověřením, zde se však uplatňuje princip „one-to-many“[108]

Prvky biometrie se uplatňují v rámci automatizovaných systémů. Jako nejzásadnější pojem vymezujeme autentifikaci, někdy také označovanou jako autentizaci. Ta se totiž vyskytuje hned ve třech podobách, a to nejen ve vazbě na biometrii. Autentizace heslem patří mezi nejstarší formy. Vytvoření hesla prostřednictvím řady písmen, čísel, znaků, často požadované délky. Skýtá v sobě ale řadu nevýhod. Nejčastějšími jsou rozšifrování hesel počítačovými aplikacemi, lidská zapomnětlivost anebo social engineering.

Autentizace předmětem patří mezi mladší formy. K přístupu do systémů může posloužit token. Jedná se o zcela jedinečný předmět, jehož velkým kladem a současně záporem se stává jeho portabilita.

Biometrická autentizace tvoří pomyslný vrchol autentifikace. Umožňuje vstoupit do systému bez nutnosti zapamatovat si složité kombinace hesel, či nosit neustále při sobě malý, lehko přehlédnutelný token. Řada výrobců spotřební elektroniky argumentuje právě pro užívání těchto lidských dispozic, namísto běžných hesel.[109] Avšak ti střízlivější z nich i nadále poskytují možnost vytvoření hesel vedle snímání takového údaje, technologie není bezchybná, stejně tak jako člověk se nenachází jen v bezpečném prostředí.

Byť na jednu stranu užití biometrické autentifikace představuje komfortní přístup do různých zařízení a aplikací. Na druhou stranu nelze zapomínat na citlivou povahu biometrického údaje a jeho adekvátní ochranu.

[108]ŠČUREK, RADOMÍR. *Biometrické metody identifikace osob v bezpečnostní praxi*. Ostrava, 2008. [online]. [2018-04-11]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

[109]*tamtéž*

4.1 Biometrický údaj jako technický pojem

Jak již bylo naznačeno výše. Biometrických údajů je celá řada. Rozpoznání tvaru uší, obličeje, otisku prstů, geometrie ruky, retinální skeny, ale také rozpoznání stylu písma, hlasu, či úderů kláves. Technologický pokrok umožnil nové metody jejich aplikace a shromažďování. Vždyť dříve možnost snímání natolik jemných a citlivých znaků jakými je vroubkování kůže na prstu by bylo téměř nemožné. A dnes se s ním lze setkat zcela běžně na našich mobilních telefonech, noteboocích, či tabletech. Lze jej vnímat jako součást každodenní reality, jako prostředek zjednodušení přístupu do oblíbených zařízení za souběžného přesvědčení jeho nenahraditelnosti a unikátnosti, tedy patří jen nám a jen my jej můžeme využít k odemčení zamknutého přístroje.

Nutno podotknout, že využití biometrických údajů nespadá pouze do sféry spotřebitele, jak by se mohlo z prvního pohledu zdát. Jejich význam roste také v souvislosti s pokrokem vědecké činnosti, jako je oblast biologie, medicíny, či v „machine learning“.[110] Každý z jednotlivých typů biometrických údajů disponuje širokým spektrem možné aplikace.

Středobodem zpracování biometrických údajů je využití automatizace. Díky ní, respektive příslušným algoritmům jsou stroje schopny rozeznat i ty nejjemnější rozdíly napříč konkrétními typy těchto dat. V této oblasti figuruje jako alfa a omega pojem tzv. „biomarkeru“. Biomarker lze definovat, jako určitou charakteristiku, která je bez jakéhokoliv subjektivního zabarvení změřena a zhodnocena. Problémem se stává však jeho nadměrná dostupnost. Veškeré zdroje jsou veřejně přístupné, a tudíž každý může zakomponovat do svého biometrického systému některý z druhů této analýzy.[111]

K jednotlivým biometrickým údajům:

Otisky prstů mohou být zkoumány z hlediska rozeznání pohlaví, či původu dané osoby, tedy, kdo byly její předci. Důležitou roli hraje především teplota prstů. Pomocí ní jsme schopni určit, zda se osoba nachází ve stresu nebo klidu, technologie dokonce umožňuje rozbor míry intenzity

[110]Machine learning je považován za jednu z odnoží umělé inteligence. Cílem machine learning je schopnost učit se. Škála využití je velmi široká. Na tomto principu pracují např. autopiloty v automobilech, jako je Tesla

[111]KRAUSOVÁ A., HAZAN H., MATEJKA J., *Biometric Data Vulnerabilities: Privacy Implication*s. [online]. [2019-01-24]. Dostupné z: www.noveaspi.cz

akutního stresu. Z hlediska medicíny umožňuje poskytnutí pomoci se stanovením diagnóz, zjištění genetických abnormalit dokonce i abnormální funkci srdce.[112]

Dalším z nezaměnitelných znaků, lidský obličej, lze říci nejexpresivnější ze všech biometrických údajů. Jehož zkoumáním dosáhneme výstupů v oblastech staří člověka, jeho etnika a pohlaví. Obličej zaujímá v oblasti biometrických údajů zvláštní roli. Ta se jenom prohlubuje díky postupu technologií umělé inteligence, a především machine learningu, kdy stroje jsou mimo jiné schopné určit i míru atraktivity člověka založenou na výsledcích analýzy obličeje.[113]

Retinální skeny slouží především k získávání informací o různých nemocech, ne nutně souvisejícími se samotným okem.[114]

Zvláštností, dle autorova názoru, jsou hlas a dynamika úderů na klávesnici. Hlasová rekognice umožňuje rozpoznání nejenom věku, emočního rozpoložení, či pohlaví, ale také i rozpoznání závažných onemocnění jakými je Parkinsonova nebo Alzheimerova choroba. Současně hlas svědčí o typu osobnosti daného jedince. Údery na klávesnici naproti tomu mohou být analyzovány z hlediska, opět, věku, pohlaví, náladového rozpoložení, poslouží ke zjištění Parkinsonovy choroby, ale zároveň pomáhají objasnit spánkový režim.[115]

4.2 Biometrický údaj jako právní pojem

Právní úprava biometrického údaje, respektive jeho definice je zakotvena v čl. 4 odst. 14 GDPR. Rozumí se jím *„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[116]. “[117]*

[112]*tamtéž*

[113]*tamtéž*

[114]*tamtéž*

[115]*tamtéž*

[116]Pozn. Autora: Daktyloskopií se rozumí věda o kožních papilárních liniích na prstech, dlaních, nohou. Jinými slovy otisky prstů.

[117]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

Biometrický údaj náleží, jak již bylo výše uvedeno do zvláštní kategorie osobních údajů, a proto se na jejich zpracování vztahují jiná pravidla. Obecně platí zákaz zpracování tohoto typu osobního údaje. Avšak GDPR přímo stanovuje výjimky z tohoto omezení. První z těchto výjimek je výslovný souhlas dle čl. 9 odst. 2 písm. a) GDPR, pro který je zapotřebí, aby subjekt explicitně deklaroval, že souhlasí s takovýmto zpracováním osobního údaje. Další je plnění povinností a výkon práv v oblasti sociálního zabezpečení a sociálního práva dle čl. 9 odst. 2 písm. b) GDPR, jedná se o situace, kdy takové zpracování je povoleno právem Evropské unie nebo členského státu nebo kolektivní smlouvou. Další z výjimek je ochrana životně důležitých zájmů dle čl. 9 odst. 2 písm. c) GDPR, s ochranou životně důležitých zájmů úzce souvisí náhlá neštěstí nebo katastrofy, kdy ke zpracování pak může dojít za účelem poskytnutí ochrany těch nejvyšších hodnot daného subjektu. Dále je možné zpracování v případě že se jedná o legitimní činnosti neziskových subjektů, nadací či sdružení, jejichž cíle jsou omezeny na politické, filozofické, náboženské nebo odborové dle čl. 9 odst. 2 písm. d) GDPR. Je nutno ale podotknout, že bez souhlasu subjektů údajů nelze tyto údaje poskytnout mimo sféru dané nadace, sdružení apod. Dalším je údaj zjevně zveřejněný subjektem dle čl. 9 odst. 2 písm. e) GDPR, zpravidla se jedná o situace, kdy osoba v rámci své publikační činnosti projevuje svůj názor ohledně své politické afiliace. Zpracování zvláštní kategorie citlivých údajů je také možné v souvislostí s určením, výkonem nebo obhajobou právních nároků a výkonem soudních pravomocí dle čl. 9 odst. 2 písm. f) GDPR, toto ustanovení především přináší rovnováhu mezi právem na ochranu osobních údajů a právem osob na uplatnění nároků. Stejně tak, jako řada dalších právních odvětví, i zde se lze setkat s výjimkou v podobě konceptu veřejného zájmu, a to na základě unijní nebo vnitrostátní právní úpravy dle čl. 9 odst. 2 písm. g) GDPR, takovéto zpracování však musí být přiměřené, v rámci sledovaného cíle a data by zpravidla měla být uchovávána jen po nezbytně dlouhou dobu. Další výjimku představuje zdravotní a sociální péče dle čl. 9 odst. 2 písm. h) GDPR, a to hlavně pro účely poskytování zdravotních služeb, dále veřejný zájem v oblasti veřejného zdraví dle čl. 9 odst. 2 písm. i) GDPR, archivace vědecký či historický výzkum a statistika dle čl. 9 odst. 2 písm. j) GDPR.[118]

GDPR dále stanovuje v čl. 9 odst. 4 že, *„Členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických či údajů o zdravotním stavu.“* GDPR tedy umožňuje členským státům odchýlit se od právní úpravy uvedené

[118]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 162-169

v nařízení a to tak, že mohou být uloženy další podmínky či omezení. V této situaci bude na národní právní úpravu pohlíženo jako na právní úpravu *lex specialis* působící vůči čl. 9 odst. 2 GDPR.[119]

4.3 Rizika automatizovaného zpracování biometrických údajů

V této podkapitole se bude autor zabývat riziky automatizovaného zpracování biometrických údajů, které spadá do věcné působnosti GDPR dle čl. 2 odst. 1 *„toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů…“*. Důvodem pro zahrnutí pouze automatizovaného zpracování je jeho úzká vazba na biometrické údaje. Automatizované zpracování představuje proces, kdy dochází k zpracování zcela automatizovaně bez nutnosti lidského zásahu. U neautomatizovaného zpracování dochází především k manuálnímu řazení osobních údajů do příslušných evidencí.[120] V rámci této podkapitoly se autor bude zabývat vytyčenými obecně doporučenými technickými postupy zpracování biometrických údajů, a jakým způsobem na ně reaguje GDPR vzhledem k poznatkům získaným v kapitolách zpracovaných výše.

Zpracování biometrických údajů za pomoci výpočetní techniky se neobchází bez rizik. Ta vyvstávají hlavně vůči jednotlivcům, jejichž data jsou shromažďována. Nejdůležitější roli hrají především dva faktory, a to monitorovací sensory a následně algoritmy, jež zpracovávají informace zjištěné těmito sensory. Nutno podotknout, díky výše zmíněným druhům biometrických údajů, neexistuje jednotná metoda jejich získávání, jeden sensor nelze užít univerzálně. Sensory jako takové hrají velmi důležitou roli ve vztahu k množství a přesnosti získaných dat. Čím více údajů je shromažďováno, tím častěji dochází k získávání dalšího množství nechtěných informací o daném subjektu. Pohled a vnímání na opatřování biometrických údajů se u jednotlivců liší. Neexistuje ucelený názor na tuto problematiku. V praxi se setkáváme s mnoha mylnými představami ohledně tohoto specifického shromažďování dat. Častým omylem je předpoklad, že snímání jakéhokoliv z těchto znaků má 100 % úspěšnost. Není tomu tak. Kde však už uživatelé příliš nechybují je jejich obava ze zneužití. Správně dochází k určení, že největší slabinou je potom samotný přenos a následné ukládání informací. Byť by se na první pohled mohlo zdát, že shromážděná data nebudou následně užita k účelům, pro které nebyl dán souhlas, velmi často bývá

[119] *tamtéž* str. 169

[120] European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law 2018 edition.* [online]. [2019-01-24]. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf str. 99

tato mylná domněnka nenaplněna. Stává se totiž velmi obtížným zajistit dostatečnou ochranu před jejich zneužitím, když dochází k online transferům na serverová uložiště, kde mnohdy existuje více subjektů, jež mají k těmto přístup. Zároveň se lze setkat i s názory, které nesouhlasí s užitím biometrických údajů, jako prostředkem verifikace z prostých hygienických důvodů. Pokud existují tací, kteří se netají svou nenávistí k „mastným tyčím" v městské hromadné dopravě, proč by se nevyskytovali i tací, jež by se měli dennodenně dotýkat jednoho konkrétního sdíleného snímače otisku prstu. Jak již bylo výše zmíněno, nechtěné získání dalších informací o daném uživateli je také jedním z důvodů k obavám. V konzumní kapitalistické společnosti, kde jsou potřeby osob uspokojovány koupí materiálních statků, informace o jejich vkusu, životní situaci nebo periodicitě nákupů, se stává nevyčíslitelnou hodnotou. A proto je více než na místě se právoplatně obávat sledování ze strany společností, které by tyto informace využily ke generaci zisku. Tento aspekt bývá velmi často spojován s tzv. syndromem velkého bratra, tedy neustálého sledování každého pohybu.[121]

Samotná rizikovost spočívá v několika aspektech. Do posuzování rizikovosti zpracování je nutno zahrnout z jakého důvodu je zpracování biometrických údajů činěno. Údaje mohou být zpracovávány ze dvou důvodů, buď za účelem identifikace nebo verifikace, ale dokonce i za účelem sledování osob, viz CCTV v Číně. Z čistě etického hlediska je více než zřejmé, že identifikace a verifikace jsou obecně vítanějšími způsoby aplikace biometrických údajů. Na základě podkapitoly o zákonnosti zpracování se čtenář textu mohl seznámit s tím, že GDPR umožňuje shromažďování pouze pro určité, výslovně vyjádřené a legitimní účely, a že nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Dalším faktorem je délka uchování těchto informací. Ideální situace nastává v případě, kdy délka uchování dat je pevně daná a ta jsou následně po její uplynutí automaticky smazána. Což GDPR reflektuje hned v jedné ze základních zásad, omezení uložení, kdy, jak již bylo výše uvedeno v podkapitole 2.1.5., délka uchování informací je pevně daná, byť může být relativní a záviset na určité okolnosti, nesmí být stanovena zcela neurčitě. S délkou úzce souvisí otázka uložiště. Zda jsou data uchovávána v dosahu nebo mimo dosah subjektů, mimo jiné také, zda-li existuje pouze jedno centrální uložiště nebo jsou uloženy decentralizovaně. Decentralizované uložiště znamená, že informace je rozdělena do několika částí, následně zašifrována a rozdělena například v rámci cloudu (dnes viz blockchain). Oproti tomu centrální uložiště obsahuje celou informaci v rámci jedné databáze.

[121]NIKOLAOS V. BOULGOURIS, KONSTANTINOS N. PLATANIOTIS a Evangelia MICHELI-TZANAKOU. *Biometrics Theory, Methods, and Applications.* Hoboken: John Wiley, 2009. str. 633-637

Autor se domnívá, že decentralizované uložiště poskytuje větší míru ochrany. Velmi často se dnes svět internetu setkává s úniky dat, v důsledku útoků, které zpravidla směřují na centrální uložiště. V samotném důsledku ukládání informací centralizovaně dochází k páchání větších škod v případě jejich uvolnění. Dále z hlediska oblasti, ve které zpracování probíhá. V kontextu zpracování biometrických údajů se k tomuto vyjadřuje WP29: „*existuje riziko vytvoření centralizované databáze obsahující osobní údaje, zejména jednající se o biometrické údaje…"*[122] GDPR v čl. 4 odst. 6 definuje evidenci, kterou lze interpretovat jako uložiště osobních údajů, nicméně nestanovuje doporučení ohledně toho, jakou formu užít, byť zmiňuje jak centralizovanou, tak decentralizovanou formu. Komentář však uvádí, že se bude jednat zejména o spisové kartotéky v listinné podobě, nicméně i přesto se autor domnívá, že v rámci technologického pokroku není nutno se upínat čistě na listinnou formu.[123] Další otázkou, která vyvstává, je zda-li se jedná o soukromý či veřejný sektor? Kdy veřejný sektor bývá považován za ten citlivější z výše zmíněných. V poslední řadě otázka fyziologických a behaviorálních typů biometrických údajů. Fyziologické jsou považovány za více citlivé. Důvod je prostý. Zneužitý otisk prstu dokáže napáchat více škod, a to i bez účasti jeho nositele, prostá dispozice s elaborovanou kopií otisku prstu umožňuje jeho téměř neomezenou aplikaci. Kdežto u behaviorálního typu již je vyžadována participace dotyčného subjektu a mimo jiné se také vyznačují nižší mírou přesnosti.[124] Zde se bude například jednat o podpis, kde je zkoumáno hned několik atributů.[125]

[122]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Opinion on Commission proposals on establishing a Framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration.* [online]. [2019-03-04]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198 Str. 6

[123]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář Str. 88

[124]NIKOLAOS V. BOULGOURIS, KONSTANTINOS N. PLATANIOTIS a Evangelia MICHELI-TZANAKOU. *Biometrics Theory, Methods, and Applications.* Hoboken: John Wiley, 2009. str. 633-637

[125] Více k podpisům v podkapitole 5.2.

5 Biometrické údaje v aplikační praxi

Biometrické údaje se těší velké podpoře. Jejich užívání se rozrůstá. Nicméně, i přes jejich téměř všudypřítomnost se nejedná o technologii, která by nepředstavovala nějaká úskalí. V této kapitole se autor bude zabývat biometrickými údaji a jejich nejčastější aplikaci ve vybraných sférách každodenního života za současného posouzení možných rizik a dopadů, a to jak z technologického, tak z právního hlediska.

5.1 Biometrické údaje a bankovnictví

Z důvodu poskytnutí co největšího komfortu svým klientům, banky v průběhu let začaly umožňovat správu bankovních účtů prostřednictvím internetového bankovnictví. Je zapotřebí si uvědomit, že internetové bankovnictví a jím poskytnuté služby jsou přímo závislé na úrovni vyspělosti informačních technologií. A v současné době je správa jednodušší než kdykoliv předtím. Se zakládáním a pořizováním bankovního účtu je namístě brát v potaz uskutečněná právní jednání, jež jsou nedílnou součástí této správy. A proto jako jedním z hlavních bodů této problematiky je nahlédnutí na bankovnictví se zřetelem k biometrickým údajům. Jak bylo již vysvětleno výše, biometrické údaje fungují, v případě prosté autentizace, na bázi porovnání získaných údajů ze vzorku s databází. Již tento samotný proces má ve vztahu k bankovnictví jisté výhody a nevýhody. Z pohledu banky je výhodou především nízká míra odpovědnosti, pokud dochází k aplikaci procesu autentizace na mobilním zařízení.[126] Tyto údaje jsou uchovávány na takovémto zařízení, a to zpravidla v samostatné hardwarové enklávě (viz. produkty značky Apple). Tato enkláva má za následek úplnou izolaci uloženého údaje od zbytku zařízení, a to nejenom po hardwarové stránce, ale také po stránce softwarové. Přístup do této enklávy si musí každá jednotlivá aplikace vyžádat, což je nespornou předností tohoto způsobu ukládání. Svým způsobem se ale nejedná o přístup per se. V zásadě dochází pouze k ověřování vzorku v dané enklávě. Tento praktický problém lze rozebrat z právního hlediska pro účely GDPR a je proto v tomto případě nezbytné pohlédnout na definici správce, která je obsažena v čl. 4 odst. 7 „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho jmenování;“* Jako správce lze na základě výše uvedené definice tedy označit toho, kdo

[126]TOMÍŠEK, JAN. *Právní jednání biometrickými prostředky v elektronickém bankovnictví.* Právní rozhledy 5/2018 str. 160

určuje účel a prostředky zpracování osobních údajů. Současně je důležité oddělit 2 pojmy, a to přístup a zpracování. Zvolení přístupu k uchovaným biometrickým údajům v tomto případě je v rukou banky, popřípadě v rukou výrobce zařízení, nicméně to samotné ještě nemá za následek úplné vymezení se proti povinnosti správce při zpracovávání biometrických údajů, protože banka je tím subjektem stanovujícím účel a prostředky zpracování a onen pojem přístupu nehraje v definici správce roli.[127] Účelem lze definovat smysl určité aktivity, v tomto případě nabízení služeb svým klientům a prostředkem je již bankovní aplikace a její nástroje či zvolené postupy zpracování biometrických údajů.[128] Další výhodou je také počet uchovaných údajů. V zásadě tento počet je omezen na jednotky, v případě autentizace obličeje je to jediný možný údaj a u otisků prstů 5 a více. Menší počet uchovaných údajů má za následek menší riziko jejich ztráty. Nicméně i přes poměrně nízký počet údajů uchovaných na zařízení vyvstává otázka jejich držitelů. Pokud k jednomu zařízení je možné mít přístup na základě více otisků prstů, znamená to současně, že přístup do aplikace internetového bankovnictví má přístup tentýž počet nositelů těchto otisků, tedy 5 a více osob. V současné době při užívání aplikací internetového bankovnictví lze k přihlašování a stvrzování limitů, popř. plateb užít právě biometrického údaje, kde ale aplikace již nerozlišuje, který z otisků prstů bude použit. Kterýkoliv z oprávněných subjektů, mající přístup k odemčení zařízení, mají taktéž následně přístup do aplikace. Což s sebou skýtá řadu rizik. Jedním z nich jsou například neoprávněné platby. Banka v tomto případě má velmi slabou výchozí pozici prokázat, že její klient opravdu učinil platbu, a nikoliv jiná osoba. Banka totiž fyzicky nedisponuje databází biometrických údajů a ani konkrétním vzorkem, který autorizoval platbu. Je to jedna z podstatných nevýhod tohoto systému.

U mobilních zařízení ale ověřování pomocí biometrických údajů nekončí. V současné době se velmi hojně diskutuje o vytvoření takzvaných biometrických platebních karet, přičemž již jsou na světě existující prototypy a pilotní projekty. Biometrická platební karta, ať už debetní, či kreditní, obsahuje čip a čtečku otisku prstů. Principiálně bude jejich způsob využití a ochrany totožný tomu, jež se nachází v mobilních telefonech, přičemž standard je nazýván EMV (Europay Master Card Visa). Výhodou opět bude uchování dat na konkrétní kartě. Co je však nutno mít na paměti jako podstatnou odlišnost je otázka napájení těchto čipů. Mobilní zařízení mají v sobě zabudovány

[127]MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V. *Biometrické údaje a jejich právní režim.* Revue pro právo a technologie 17/2018 str. 91

[128]NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. str. 89

akumulátory, jež napájí výpočetní jednotky.[129] U platebních karet bude nutno přistoupit k jiné metodě napájení. Při předložení u platebního terminálu držitel karty namísto zadání PIN kódu jednoduše načte svůj otisk prstu jako stvrzení transakce a výpočetní jednotka bude napájena přímo z platebního terminálu. Biometrické ověření by mělo fungovat jak u NFC[130] plateb, tak i s běžným zasunutím karty do platebního terminálu. Další vyvstávající otázkou je, jak dostat biometriku na platební kartu, když sama o sobě není napájena. Zde se počítá se dvěma možnými řešeními. První z nich je vytvoření určitého pouzdra, jež v sobě obsahuje akumulátor, který poskytne platební kartě dostatek energie na uložení otisku prstu. Druhou možností je dostavit se na příslušnou pobočku banky i s platební kartou, kdy prostřednictvím příslušného zařízení dojde k načtení otisku prstu a jeho nahrání na platební kartu.[131] Dalšími z nevýhod, se kterými se setkáváme, ve vztahu k platebním kartám, jsou *phishing* a *pharming*.

Phishing je poměrně starý způsob, jakým jsou oklamáváni držitelé platebních karet. První phishingové útoky lze datovat někdy kolem roku 1995 a to především v USA. Cílem phishingu je získat údaje platební karty za účelem uskutečnění neoprávněných plateb. Těmito údaji jsou 16ti místné číslo, datum platnosti karty a CVC kód. Nejčastější metodou sloužící k získání těchto údajů je prostřednictvím tzv. phishingových e-mailů. Phishingový mail, je odeslán subjektem, který se vydává za některou z legálně ustanovených institucí, typicky bankovní instituce. Tento e-mail žádá držitele karty, aby ze smyšlených důvodů např. obnovení hesla, ověření držitele karty, či falešné namítání nabourání do účtu klienta. Na výzvu držitel karty vyplní požadované údaje platební karty a tím dojde k jejich odcizení. Pojem phishing vychází z pojmu „fishing“, kdy scammeři v zásadě loví/rybaří s cílem, že se někdo chytí na háček. Zajímavostí phishingu je především jeho cílení na lidskou důvěřivost, nedostatek kritického myšlení a nepozornost. K nejjednoduššímu odhalení phishingu dochází zpravidla zkontrolováním e-mailové adresy odesílatele, či zběžným přečtením

[129]VISA company. *Fingerprint authentication moves from phones to payment cards.* [online]. [2019-01-24]. Dostupné z: https://usa.visa.com/visa-everywhere/security/biometric-payment-card.html

[130]Vysvětlení autora: NFC, neboli Near Field Communication standard je druhem bezdrátové technologie, jež umožňuje přenos dat u zařízení, nacházejících se v bezprostřední blízkosti, např. přenos dat z fotoaparátů do telefonů, platby telefony, či platebními kartami u platebních terminálů

[131]BURGESS, MATT. *Biometric bank cards are almost here.* Wired [online]. [2019-01-24]. Dostupné z: https://www.wired.co.uk/article/mastercard-biometric-card-testing-visa-gemalto-scanner-fingerprint-trial

e-mailu. Phishingové e-maily obsahují řadu chyb a také neurčité oslovení klienta, což by mělo posloužit jako jisté vodítko k odhalení falešného e-mailu.[132]

Pharming je velmi blízký způsob phishingu k využití důvěřivosti držitelů platebních karet. Metodika je zprvopočátku stejná. Klient banky obdrží podvodný e-mail. Kde však již nastává změna je propracovanost pharmingových útoků. Podvodníci vytvářejí falešné webové stránky dle originálních předloh s cílem vzbudit co největší míru důvěryhodnosti. E-mail velice často odkazuje prostřednictvím URL na takovéto stránky a zpravidla přímo nasměrovává na formulář, kde nic netušící klient vyplní informace o platební kartě. Následně podvodníci ukrajují kousek po kousku z pomyslného koláče financí nic netušícího klienta.[133]

Dle autorova názoru je však otázkou, jak dlouhou dobu s námi ještě platební karty setrvají. Díky stále populárnějším smartphonům, disponujícími technologií NFC, je možno načíst údaje platební karty přímo do telefonu a vyhnout se tak jejímu nošení. Teoreticky je možno si představit, že banky by nevydávaly platební karty ve fyzické podobě, nýbrž pouze v elektronické s příslušným QR kódem, při jeho naskenování by došlo k nahrání karty do telefonu. I to ale má svá úskalí. A to především opět v záležitostech napájení. Jakmile dojde baterie, klient nemá možnost zaplatit, což se u biometrické platební karty stát nemůže. Navíc řada fintech startupů v posledních letech značně revolucionizuje bankovní odvětví a je nejisté, jaký směr toto odvětví nabere. Mezi krajní situace může patřit například využití technologických implantátů na těle, což je prozatím těžko představitelné.

Závěrem k problematice bankovnictví lze dodat, že právní úprava platebního styku na území Evropské unie je upravena směrnicí o platebních službách na vnitřním trhu.[134] Tato směrnice upravuje postup udělení souhlasu s provedením platební transakce ve svém čl. 64 odst. 4. Ve smyslu tohoto ustanovení se za autorizaci platební transakce považuje elektronický podpis ve

[132]LANCE, J., *Phishing Exposed*. [online]. [2019-02-17]. Dostupné z: http://index-of.co.uk/Hacking-Coleccion/Phishing%20Exposed.pdf str. 10-12

[133]BRODY, RICHARD. MULIG, ELIZABETH VALERIE. *Phishing pharming and identity theft.* Academy of Accounting and financial Studies Journal. 2007. roč. 11, č. 3. str. 46.

[134]Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

formě ověření biometrikami. Požadavkem směrnice dále je, že je na členských státech, aby zajistily, že u platebních transakcí činěných na dálku bude uplatňováno silné ověření klienta, jež zahrnuje prvky dynamicky propojující transakci s konkrétní částkou a konkrétním příjemcem. Je důležité si uvědomit, že tento požadavek není cílený na typ příkazu, ale na samotný mechanismus autorizace. Nutno podotknout, že informace týkající se tohoto ověření budou upraveny terciární úpravou ve formě aktů Evropské komise, která byť byla zveřejněna, nebyla doposud publikována v Úředním věstníku EU.[135] Jak již bylo naznačeno výše, nejčastěji se vyskytujícími se problémy jsou ty, dotýkající se neautorizovaných plateb. Spory vyplývající z neautorizovaných plateb jsou řešeny v čl. 72 odst. 2 směrnice. Kdy je řečeno, že nepostačuje pro prokázání, zda daná platební transakce byla plátcem autorizována nebo zda se plátce dopustil podvodu, pokud klient namítá neautorizovanou platbu. A je tedy na klientovi, aby v těchto situacích prokázal, proč transakci neautorizoval a banka, naopak, musí toto tvrzení vyvrátit. V případě nedostatečných argumentů banky, kdy klient prokáže, že platba byla učiněna z jeho zařízení prostřednictvím jiné osoby, bude situace posuzována dle odpovědnosti za neautorizovanou transakci.[136] V souvislosti s právní úpravou platebního styku je také důležité zmínit činnost Evropského orgánu pro bankovnictví, který v roce 2017 publikoval finální návrh regulatorních technických standardů, které se přímo dotýkají výše uvedené směrnice a to především silného ověření klienta.[137] Standardy vyžadují příslušené charakteristiky prvků silného ověření klienta i ve vztahu k biometrickým čidlům.[138]

5.2 Biometrické údaje a podpisy

V návaznosti na předešlou kapitolu, která se zabývala bankovnictvím je nutno zmínit také problematiku biometrických podpisů, která se však nedotýká přímo transakce jako takové, ale smluvní dokumentace s ní související. Při výkonu dvoustranného právního jednání, tedy při

[135]TOMÍŠEK, JAN. *Právní jednání biometrickými prostředky v elektronickém bankovnictví.* Právní rozhledy/2018, [online]. [2019-01-24]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7gvpxgxzrgyyc4y3mgm&groupIndex=0&rowIndex=0

[136]*tamtéž*

[137]MICHALEC, FILIP, *Silné ověření klienta podle RTS ke směrnici PSD2.* [online]. [2019-01-24]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-podle-rts-ke-smernici-psd2-105724.html

[138]Návrh Nařízení Evropské komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady 2015/236ž, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace. Recitál: 6

uzavírání dvou a vícestranných právních jednání je čím dál tím častější podepisování smluv za pomoci takzvaného dynamického biometrického podpisu. Dynamický biometrický podpis má v současné době stejnou váhu jako podpis učiněný běžným způsobem na list papíru. Jak již bylo uvedeno v předchozích kapitolách, podpis v sobě skrývá poměrně širokou škálu informací o jeho vyhotoviteli.[139] Propůjčené právní účinky elektronickému podpisu lze dovodit evropskou legislativou *„Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu".*[140] Nicméně je nutno si uvědomit, že se nejedná o ustanovení přímo se dotýkající dynamického biometrického podpisu, avšak zesiluje a utvrzuje postavení dynamického biometrického podpisu mezi ostatními typy podpisů.[141]

Na základě vydaného stanoviska Úřad ochrany osobních údajů konstatoval, že dynamický biometrický podpis lze považovat za citlivý údaj, pokud z něho lze dovodit identitu jednotlivce.[142] Avšak pokud bude využíván stejně jako podpis běžný a nebude docházet k automatizovanému zpracování údajů, uplatní se stejný právní režim jako při zpracování klasického podpisu. V této situaci bude povaha citlivého údaje, respektive zvláštní kategorie osobních údajů absentující.[143]

Pohled na dynamický biometrický podpis měřítkem GDPR je do jisté míry závislý na tom, zda bude použit k verifikaci či identifikaci subjektu. V kapitole 4.2. se čtenář textu mohl seznámit s tím, co se dle čl. 4 odst. 14 GDPR považuje za biometrický údaj a současně, že jeho zpracování je zakázáno až na výjimky uvedené v čl. 9 odst. 2 GDPR. Proto pro účely dynamického biometrického podpisu bude nezbytné posoudit, zda v jeho kontextu dochází k pouhé verifikaci,

[139]SMEJKAL, VLADIMÍR. *Dynamický Biometrický Podpis a Nařízení GDPR.* [online]. [2019-04-07]. Dostupné z: https://journals.muni.cz/revue/article/view/8282 Str. 97

[140]Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikace a službách vytvářejících důveru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES čl. Čl. 25 (2)

[141]KORBEL František, KOVÁŘ Dalibor. Havel Holásek & Partners. *Changes in regulation of electronic signatures (eIDAS)* [online]. [2019-04-07]. Dostupné z: http://havelpartners.cz/images/stories/publikace/eu_legal_news_en_2015_12.pdf

[142]UUOU. *Stanovisko č. 2/2014* [online]. [2019-04-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22532

[143]SMEJKAL, VLADIMÍR. *Dynamický Biometrický Podpis a Nařízení GDPR.* [online]. [2019-04-07]. Dostupné z: https://journals.muni.cz/revue/article/view/8282 Str. 98

či identifikaci subjektu. Protože při identifikaci dochází k identifikování subjektu oproti jiným osobám.[144]

Z hlediska biometrie podpisu dochází ke zkoumání dvou aspektů, a to statiky a dynamiky.

- Statika
  - Vrcholy
  - Překřížení
  - Křivky a smyčky
  - Uzavřené oblasti
- Dynamika
  - Délka trvání podpisu
  - Signály o tlaku, rychlosti, zrychlení[145]

Výše uvedené prvky by měly být samy o sobě důkazem o bezpečnosti dynamického biometrického podpisu. Dynamický biometrický podpis představuje sloučení všech výše uvedených kroků v jeden akt, který je jen velmi obtížné falzifikovat. A následné zašifrování údajů tuto tezi jen podporuje. Dalším zásadním prvkem je ale taky pravý opak této situace, kdy subjekt, jež podepsal určitý akt, se následně domáhá určení, že nic nepodepsal. V těchto situacích opět bude snadné zjistit pro odborníka, písmoznalce, že daná osoba smlouvu stvrdila svým podpisem. Tudíž ani zde tento druh podpisu nepředstavuje žádná rizika.

5.3 Biometrické údaje a cestovní doklady

Mezi nejčastější typy dokladů obsahujícími biometrický údaj jsou cestovní pasy. Jedná se o běžný cestovní pas, jež obsahuje drobný čip, jež uchovává informace, které umožňují identifikaci jeho držitele. Tento typ cestovních pasů je využíván napříč světem. K jeho časté aplikaci dochází zpravidla na letištních kontrolách, kde držitelé tzv. e-pasů mohou využít automatizované pasové kontroly namísto fyzické kontroly policistou. Osoba přijde k terminálu, přiloží svůj cestovní pas, který je následně naskenován. Po úspěšném naskenování je vpuštěna ke snímání obličeje, kde

[144]UUOU. *Stanovisko č. 2/2014* [online]. [2019-04-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22532
[145]SIGNOSOFT. *Jak to funguje* [online]. [2019-04-07]. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php

dochází ke kontrole sejmutého obličeje kamerou a obrazu obličeje uloženého na čipu pasu, a následně opouští terminál. A to jak v případě úspěšného, tak neúspěšného načtení. V případě neúspěšného načtení je nucena dostavit se za příslušným úředníkem, který provede kontrolu. Užívání biometrických cestovních pasů začalo v EU 1. září 2006 a to na základě nařízení Rady EU č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy. Cílem přijetí tohoto nařízení bylo posílení ochrany před trestnou činností v EU. Jak ze samotného nařízení vyplývá, dalším ze základních směrů harmonizace je posílením vazby mezi držitelem cestovního průkazu a samotným dokumentem. Tedy uplatnění unikátních znaků každého jednotlivce s cílem zabezpečit jejich řádnou autentizaci. Čl. 1 hovoří o tom, že cestovní pasy a doklady musí obsahovat „*médium pro uchování údajů, které obsahuje zobrazení obličeje, jakož i otisky prstů v interoperabilních formátech.“* Média musí být dostatečně zabezpečena, s dostatečnou kapacitou a schopností zaručit neporušitelnost, pravost a utajení údajů. Zároveň se však toto nařízení nevztahuje na průkazy totožnosti. V příloze jsou uvedeny požadavky, resp. minimální bezpečnostní normy uplatňované v souvislosti s vyhotovováním těchto dokladů. Dotýkají se celé řady záležitostí. Použitých materiálů, techniky tisku, ochrany proti kopírování a techniky vydávání.[146] Biometrické pasy obsahují několik typů biometrických údajů.

Prvním, nejvíce zřetelným prvkem, je digitálně zpracovaná černobílá fotografie obličeje, kdy za pomocí evaluace obličeje jako celku dochází k mapování jeho jednotlivých atributů např. položení rtů nebo očí na obličeji. Tato fotografie je vypalována laserem. Není lepená, což zamezuje jejímu případnému zneužití. Typicky, kdyby se pachatel pokusil na fotografii něco dokreslit nebo jinak modifikovat. Mimo to je fotografie také uložena v digitální podobě na samotném čipu uvnitř pasu. Výše uvedené nařízení zakotvovalo od samého počátku ve svém čl. 6 povinnost pro státy použít zobrazení obličeje nejpozději do 18 měsíců od přijetí opatření uvedených v článku 2 nařízení, tedy technických specifikací. Druhým je podpis. Podpis držitele pasu se porovnává s uloženým podpisovým vzorem, důležitá je hlavně dynamika podpisu. Tedy jakou silou je tlačeno na jednotlivá písmena, jaký důraz je jim přikládán a v poslední řadě také rychlost psaní. Třetím jsou otisky prstů, které byly již několikrát diskutovány napříč kapitolami této práce. Je nicméně

[146]Nařízení Rady EU č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy. [online]. [2019-01-24]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32004R2252 čl. 1-6, vč. Příloh.

na místě podotknout, že stejně jako k fotografiím obličeje, čl. 6 výše uvedeného nařízení stanovuje povinnost členských států uplatnit je v cestovních pasech nejpozději do 36 měsíců od přijetí opatření uvedených v článku 2 nařízení, tedy technických specifikací.[147] U tohoto biometrického údaje v tomto kontextu by se autor rád pozastavil a uvedl, že otisky prstů se také dostaly do kolize s právem na soukromý život dle čl. 7 Listiny základních práv Evropské unie. Spor se týkal především osoby M. Schwarze, který žádal Stadt Bochum o vydání cestovního pasu a současně odmítl, aby mu byly sejmuty otisky prstů. Tímto se spor dostal prostřednictvím řízení o předběžné otázce před Evropský soudní dvůr. Schwarz rozporoval platnost nařízení č. 2252/2004 a tvrdil, že je stiženo vadou postupu a odmítl poskytnout své otisky prstů. Evropský soudní dvůr zde argumentoval, že otisky prstů jsou odebrány bez fyzické či psychické újmy a jedná se o prsty, které jiné osoby běžně vidí, tudíž se nejedná o úkon intimní povahy. Současně ani při následné kumulaci činností, tedy snímek otisku prstu a snímek obličeje, nedochází k nadměrnému zásahu do práva na soukromí.[148] Současně, z hlediska ochrany osobních údajů, se Evropský soud pro lidská práva vyjádřil k uchovávání otisků prstů v centrálním uložišti biometrických údajů s cílem zabránit krádeži identity, že takové to uchovávání by bylo zcela excesivní bez příslušných záruk pro nositele těchto údajů.[149] V návaznosti lze zmínit ještě případ Willems, který se velmi úzce dotýká této problematiky. První z položených otázek Evropskému soudnímu dvoru, byla aplikovatelnost výše uvedeného nařízení na národní identifikační karty, soud rozhodl, že nikoliv. Soud zde uplatnil především jazykový výklad, kdy se zabýval spojkou „ani“ při výčtu dle čl. 1 odst. 3 nařízení č. 2252/2004 *„nevztahuje na průkazy totožnosti… ani na dočasné cestovní pasy a cestovní doklady s platností dvanáct měsíců a méně.“*[150] Druhá otázka směřovala na samotné zpracování a uchovávání biometrických údajů, zda-li jejich uchovávání a zpracování bude použito pouze pro účely pasů, či jiných cestovních dokumentů. Stejně jako v případu Schwarz v. Stadt Bochum,

[147]HEJDUK, MAREK. *Hejduk (Svobodní): Potřebujeme biometrické cestovní doklady?* [online]. [2019-01-24]. Dostupné z: https://www.parlamentnilisty.cz/politika/politici-volicum/Hejduk-Svobodni-Potrebujeme-biometricke-cestovni-doklady-561791

[148]Rozsudek ESD ve věci C-291/12 ze dne 17. října 2013 Michael Schwarz v. Stadt Bochum

[149]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Opinion on Commission proposals on establishing a Framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration.* [online]. [2019-03-04]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198 Str. 6

[150]Nařízení Rady EU č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy. čl. 1 odst. 3

došlo k argumentaci čl. 7 a 8 Listiny základních práv Evropské unie a Evropský soudní dvůr zde ještě rozšířil svůj původní argument, protože otázka směřovala na následné další zpracování těchto údajů členskými státy. Evropský soudní dvůr stanovil, že pokud by členský stát chtěl uchovat tato data pro další účely, učiní tak sám v rámci své autonomie. Toto nařízení tedy explicitně nestanovuje povinnost pro členské státy zaručit ve svých právních řádech, že tyto údaje nebudou shromažďovány či zpracovávány k účelům jiným než k vydání pasu nebo jiného cestovního dokladu.[151]

Výše zmíněné biometrické údaje v cestovních pasech mají nařízením stanovený účel, kdy jsou uplatněny. Čl. 4 odst. 3 nařízení stanovuje, že se použijí pouze k „*ověřování pravosti dokumentu nebo totožnosti držitele pomocí přímo dostupných srovnatelných prvků v případech, kdy musí být cestovní pas nebo jiný cestovní doklad podle právních předpisů předložen.*“[152] Stejně tak mají osoby právo na to ověřit si osobní údaje v cestovním dokladu a také požadovat provedení opravy nebo výmazu.[153] K provedení opravy nebo výmazu je nezbytné reflektovat ustanovení recitálu nařízení, který stanovuje *„Pokud jde o osobní údaje zpracovávané v souvislosti s cestovními pasy a cestovními doklady, použije se směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.“*[154] A jelikož v směrnice byla nahrazena GDPR, uplatní se právní úprava čl. 16 a 17 pro opravu a výmaz.

Jak již bylo naznačeno výše. Cílem vydávání biometrických pasů je prevence před trestnou činností. Nejčastěji se hovoří o tzv. *„identity theft“*, nebo-li krádeži identity. Krádež identity je jedním z moderních druhů trestné činnosti. Pachatel tohoto činu získává citlivé informace o určité osobě, typicky adresu, datum narození, jméno, informace o platebních kartách, či jiné údaje. Cílem této činnosti je vydávání se za cizí osobu nebo výkon jiného podvodného jednání. V zásadě dochází ke krádeži a zneužití dobrého jména nebo reputace určité osoby s cílem se finančně obohatit. Počátky tohoto činu sahají až do 80. let, kdy v průběhu let byl nazýván celou řadou termínů, ale samotný termín identity fraud byl zakotven až v průběhu 90. let. Původně byl nazýván

[151]Rozsudek ESD Ve spojených věcech C-446/12 až C-449/12 ze dne 16. dubna 2015

[152]Nařízení Rady EU č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy. čl. 4 odst. 3

[153]*tamtéž* čl. 4 odst. 1

[154]*tamtéž* recitál 8

především podvodem s kreditními kartami. Po zavedení kreditních karet, získali zločinci zcela nový nástroj, jak z obětí vylákat velké finanční sumy. Metody, jež k tomu uplatňovaly, byly zcela jednoduché. Postačil jim k tomu prostý *„dumpster diving".*[155] Pachatelé prohledávali odpadkové koše s cílem objevení dokumentů, jež by obsahovaly údaje nezbytné k následnému uplatnění karet. Po internetové revoluci dostali kriminálníci zcela nové způsoby, kterými se obohatit a výše uvedené údaje se tak staly náchylnějšími než kdy dříve. A to především díky firemním databázím klientů, které jsou v celé řadě případů slabě chráněny, a velmi často se dnešní svět setkává s úniky dat právě z nich. Nutno podotknout, že identity fraud má dalekosáhlé následky a jeho oběti se s nimi potýkají celou řadu následujících let, zpravidla 2-5 let v závislosti na závažnosti a délce úniku.[156]

Ve vztahu k cestovním dokladům je zapotřebí zmínit další právní úpravu, jež se dotýká členů orgánů Evropské unie a jejich zaměstnanců. Nařízení stanovuje, že tento průkaz se vydává v zájmu Evropské unie a, že úřady jednotlivých členských států mají povinnost průkaz uznávat za platný cestovní doklad. Z hlediska bezpečnostních a technických požadavků je odkazováno na výše uvedené nařízení č. 2252/2005. A stejně také obsahuje jak biografické, tak biometrické prvky. Přičemž biometrické prvky se využívají pouze pro „*ověřování pravosti dokladu a totožnosti držitele pomocí porovnatelných prvků, které jsou přímo k dispozici."*[157]

Závěrem lze jen dodat, že biometrické pasy jsou čím dál tím více všudypřítomné a jejich výhody jsou nesporné. ePasy poskytují nejenom vyšší míru bezpečnosti a ochrany před krádežemi identity, ale i vysokou míru flexibility a také umožňují rychlejší řešení pasových kontrol, čímž dochází k předcházení tvoření velkých davů, které představují další bezpečnostní rizika. Zároveň je ale nutno dodržovat technická a bezpečnostní opatření, aby nedocházelo ke zneužití v nich uvedených citlivých osobních údajů.

[155]Pozn. Autora: Jedná se o činnost, kdy dochází k prohledávání košů s odpadky, či kontejnerů s odpadky, ale není nutně spojena s kriminální činností.

[156]BIEGELMAN, Martin T. *Identity theft handbook: detection, prevention, and security*. Hoboken, N.J.: Wiley, c2009. str. 1-10

[157]Nařízení Rady (EU) č. 1417/2013 ze dne 17. prosince 2013, kterým se stanoví vzor průkazu vydávaného Evropskou unií. Recitál 1-10, čl. 5

5.4 Biometrické údaje a Schengenský informační systém

V souvislosti s přechodem hranic lze zmínit také Schengenský informační systém. Schengenský informační systém představuje evropský systém bezpečnosti a správy hranic. Jeho hlavním účelem je umožnit příslušným národním autoritám, aby společně postupovali při ochraně společných hranic. Kterýkoli stát účastnící se na Schengenském informačním systému má tak přístup do sdílené databáze a tím je mu umožněno získat údaje o záznamu, jež je v této databázi obsažen. Tento systém je upraven třemi základními akty: nařízením o zřízení provozu a využívání Schengenského informačního systému druhé generace[158], rozhodnutím Rady o zřízení, provozování a využívání Schengenského informačního systému druhé generace[159] a nařízením o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace.[160]

S cílem zesílení tohoto systému Evropská komise 21. prosince 2016 navrhla, aby do stávajícího systému byly zavedeny nové prvky. Jedním z těchto prvků je uplatňování obrazů obličeje pro účely biometrické identifikace. Dalšími jsou pak otisky dlaně, prstů, či DNA týkající se pohřešovaných osob.[161] Jedním ze zásadních nedostatků spočívajícím v užívání Schengenského informačního systému je však sběr a uchování biometrických údajů. Často dochází k ukládání biometrických údajů, jež nejsou dostačující z kvalitativního hlediska. Tímto dochází k porušování povinnosti vycházející z nařízení *"členský stát pořizující záznam odpovídá za zajištění toho, že údaje jsou správné, aktuální a jsou vložené v SIS II v souladu se zákonem."* Přičemž právě pro zpracování fotografií a otisků prstů se ještě uplatní zvláštní kontrola kvality pro zajištění minimálního kvalitativního standardu. Tento nedostatek, respektive jeho řešení, na sebe však váže vysokou finanční nákladnost, protože je zapotřebí zcela nepochybně vybalancovat tyto problematické aspekty především aplikací modernějšího hardwaru.

---

[158]Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II)

[159]Rozhodnutí Rady 2007/533/SV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II)

[160]Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II)

[161]Evropská komise. *The Commission will propose to reinforce the Schengen Information System (SIS) ze dne 21. prosince 2018*. [online]. [2019-03-10]. Dostupné z: http://europa.eu/rapid/press-release_AGENDA-16-4447_en.htm

Nově uplatňovaným systémem v rámci Schengenu se stal Automatizovaný systém identifikace podle otisků prstů. Tento systém byl vytvořen především z toho důvodu, že byť schengenská databáze již obsahovala otisky prstů osob, byly používány pouze k potvrzení identity osoby, nikoliv k identifikaci osoby pouze na základě otisku prstů. Jedná se však prozatím o první fázi spuštění tohoto systému.[162]

5.5 Biometrické údaje a národní identifikační karty

Jedním z hojně diskutovaných témat v Evropské unii je také zavedení národních identifikačních karet, de facto občanských průkazů, jež by obsahovaly biometrické údaje. Tento návrh sleduje v zásadě stejné cíle jako je tomu u cestovních dokladů. Tedy potírání kriminality. Evropská komise, strůjce tohoto návrhu, v dubnu 2018 představila program s cílem omezit pole působnosti a možnosti jednání teroristům a zločincům. Hlavním požadavkem je, v případě, že členský stát vydává občanské průkazy, pak jejich nezbytnou součástí budou 2 biometrické údaje – otisky prstů a obrazy obličeje, uchovávány na čipu daného průkazu.[163] Je tedy o to zbavit se jednoduše modifikovatelných dokumentů v současné podobě. Jak již vyplývá z výše uvedeného, prozatímním cílem Evropské komise není stanovit členským státům povinnost zavést občanské průkazy. Povinnost bude dopadat pouze na státy, jež tyto průkazy vydávají. Nicméně, zaznívají i takové názory, např. od J. P. Albrechta, který tvrdí, že *„i otisky prstů mohou být padělány a, že i teroristé a jím podobní si obstarají peníze a zbraně bez toho, aniž by se prokázali občanským průkazem.“*[164] Je tedy otázkou, jakým směrem se tato oblast bude vyvíjet. Autor této práce se však domnívá, že přijetí této právní úpravy by dozajista posílilo prevenci před protiprávním jednáním, byť otisky prstů mohou být padělány, samotný proces je náročnější než ten u běžných občanských

[162]eu-LISA. *AFIS for SIS II to be deployed this month 2. března 2018.* [online]. [2019-03-10]. Dostupné z: https://www.eulisa.europa.eu/Newsroom/News/Pages/AFIS-deployment-March-2018.aspx

[163]Evropská Komise. *Security Union: Commission presents new measures to deny terrorists and criminals the means and space to act, Brusel 17. dubna 2018*. [online]. [2019-03-04]. Dostupné z: http://europa.eu/rapid/press-release_IP-18-3301_en.htm

[164]BLENKINSOP, PHILIP. KOESTER, SAMANTHA. *EU Commission proposes making fingerprints mandatory in ID cards.* Reuters [online]. [2019-01-19]. Dostupné z: https://www.reuters.com/article/us-eu-security/eu-commission-proposes-making-fingerprints-mandatory-in-id-cards-idUSKBN1HO23A

průkazů, a proto méně osob bude disponovat prostředky a metodami, jež by vedly k úspěšnému dokončení takového procesu.

5.6 Biometrické údaje a pracovněprávní praxe

Dalším a pro účely této práce posledním z možných polí působnosti biometrických údajů jsou právě pracovněprávní vztahy. Historicky byla kupříkladu evidence, respektive docházka zaměstnanců na pracovišti řešena pomocí tzv. „píchaček“, při příchodu a odchodu z pracoviště, tehdy se používalo především papírových výkazů. V současné době se uplatňují především ve formě elektronické, za pomoci čipů. I do této oblasti však postupně začaly pronikat modernější technologie a ke sledování pracovní doby a docházky se začala užívat právě biometrická data.

Mezi nejčastěji v úvahu přicházející jsou biometrická data, jež jsou zpracovávána, jako otisky prstů a skeny duhovky.

Pro případ evidence docházky a pohybu zaměstnanců na pracovišti si autor dovolí otisky prstů a skeny duhovky postavit na roveň. V obou dvou případech je nicméně nesporné, že získáváním těchto údajů dochází k narušování soukromí zaměstnance ve značné míře, a proto je možno uchýlit se k takovým metodám pouze v důvodných případech. Soukromý život zaměstnanců představuje esenciální hodnotu, která musí být dodržována a zaměstnavatel musí mít řádný důvod pro aplikaci těchto prostředků. Příkladmo lze uvést situaci, kdy zaměstnavatel má v rámci svých prostor místo, ve kterém je koncentrována veškerá výpočetní technika (serverovna). Tam dochází k uchovávání veškerých informací, jež jsou značně citlivé, vyžadující obezřetnost při jejich zacházení, typicky databáze klientů, či osobních údajů zákazníků. K tomu, aby zaměstnavatel dodržel zákonem mu uložených povinností, vytvořil systém kontroly vstupu, který zaznamenává aktivitu zaměstnanců, jež pro tyto účely mají určitou diskreci. V případě ztráty dat, je zaměstnavatel schopný nejenom analyzovat kdy a k jakému úniku došlo, ale současně dle přístupu zaměstnanců do místnosti evaluovat, který zaměstnanec za únik může. Právo na soukromí zaměstnance se zde tedy dostává do kolize se zájmem zaměstnavatele na zpracování osobních údajů a současně se jedná o zpracování zvláštní kategorie osobních údajů, jež je obecně zakázáno, z důvodu zpětné

identifikace osoby zaměstnance.[165] Proto v tomto případě nezbývá než konstatovat, že byť GDPR posvěcuje možnost v čl. 9 odst. 2 písm. b) pro uplatnění výjimky v oblasti pracovního práva, pak jenom, pokud je taková povolena právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, a proto v rámci právní úpravy *de lege ferenda* se jeví jako vhodné implementovat možnost výjimky například právě do zákoníku práce.[166] Jako další problematický aspekt se může jevit situace vstupu do určitých prostor například právě u zaměstnavatele, kdy správci často namítají, že údaje, jež zpracovávají, nejsou biometrickými údaji, byť se zaměstnanec prokazuje příslušnými zařízeními. Tato obsahují jeho biometrické údaje, avšak takovým způsobem, že je nelze zpětně přiřadit k určité osobě, tzn. postrádají znak identifikovatelnosti. Zde je nutno nahlédnout zpět do GDPR, a to konkrétně do definice biometrického údaje v čl. 4 odst. 14, kde je mimo jiné stanoveno *„…které umožňuje nebo potvrzuje jedinečnou identifikaci.“* Pokud se na toto ustanovení však nahlédne optikou výkladu stanoviska WP29, ta pak stanovuje, že *„biometrická data nejsou určena jen pro účely identifikace, ale také pro účely autentifikace/verifikace.“*[167] A proto v samotném důsledku je nutno pohlížet na argumentaci správců jako zcestnou.[168] Co již může být představováno za diskutabilní ze znění nařízení, je, jestli za svobodně udělený souhlas lze považovat ten, který byl udělen po podpisu pracovní smlouvy. Pro zaměstnance v rámci pracovního práva platí postavení slabší smluvní strany a již samotné znění „výkon závislé práce“ může být návodné. Zaměstnanec je závislý na mzdě a je otázkou do jaké míry je tato jeho existenční závislost na mzdě určující pro udělení souhlasu.[169]

[165]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti, 8. červen 2017.* [online]. [2019-03-04]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30203 str. 15-17

[166]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. 9 odst. 2 písm. a) a b)

[167]Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Opinion 01/2012 on the data protection reform proposals.* [online]. [2019-03-04]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf Str. 10

[168]MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V. *Biometrické údaje a jejich právní režim.* Revue pro právo a technologie 17/2018 str. 91

[169]SLABÝ, T., AK Kříž a partneři s.r.o. *Docházkové systémy využívající biometrických údajů zaměstnanců z pohledu GDPR.* [online]. [2019-03-04]. Dostupné z: https://www.epravo.cz/top/clanky/dochazkove-systemy-vyuzivajici-biometrickych-udaju-zamestnancu-z-pohledu-gdpr-108322.html?mail

Závěr

Diplomová práce se zabývala tématem, jež je velmi hojně diskutováno, a to nejenom odborníky, ale i širší, laickou veřejností. Ochrana osobních údajů i nadále představuje poměrně dynamicky se vyvíjející oblast práva, jež reaguje na rovněž dynamický technologický vývoj.

Autor si v úvodu práce vytyčil jako cíl představení právní úpravy ochrany osobních údajů ve vztahu k biometrickým údajům, a to hned pro několik oblastí nejčastějšího výskytu užití biometrických údajů, dle autorova názoru.

Nutno dodat, že problematika biometrických údajů je velice komplexní téma a autor textu se v průběhu práce setkal s mnoha úskalími, tím nejzásadnějším nejspíše je, že se mu zcela nepodařilo omezit se čistě na rovinu ochrany osobních údajů. Jak již bylo mnohokrát zmíněno výše, v této oblasti dochází ke konjunkci práva a technologií a výběrově, pojmy jako autentifikace, verifikace nebo biometriky nelze zmiňovat, bez toho, aniž by došlo k jejich technickému rozboru.

V průběhu práce se autor dopracoval k několika dílčím cílům. V podkapitole 1.3. se autor zaměřil na porovnání právní úpravy ochrany osobních údajů v USA a Evropské unii, přičemž došel k jednoznačnému závěru, že právní úprava ochrany osobních údajů v USA představuje velmi rozkouskovanou právní úpravu dotýkající se vždy specifických odvětví, což činí podstatný rozdíl vzhledem k současné legislativě v Evropské unii.

Dále autor zanalyzoval právní úpravu ochrany osobních údajů v Evropské unii ve vztahu k biometrickým údajům, její právní principy a obecné ukotvení v systému práva.

A v samotném jádru práce se autor zaměřil především na palčivé otázky vyvstávající u jednotlivých oblastí, kde dochází k využívání biometrických údajů. V oblasti bankovnictví autor, především z hlediska GDPR, dospěl k závěru, že banka, poskytující klientovi službu smartbankingu, pomocí mobilní aplikace, se považuje za správce, protože stanovuje účel a prostředky. V návaznosti na bankovní sféru autor řešil vnímání dynamického biometrického podpisu dle GDPR a dospěl k závěru, že rozhodujícím pro určení, zda-li dynamický biometrický podpis je nutno vnímat jako citlivý osobní údaj, je kritérium identifikovatelnosti subjektu a není tudíž nutno se odchylovat od současného výkladu Úřadu ochrany osobních údajů. U problematiky cestovních dokladů a národních identifikačních dokumentů autor této práce nedospěl k zásadním

závěrům, zde se jeví postup dle GDPR jako optimální. U problematiky Schengenského informačního systému lze spatřovat onu konjunkci práva a technologií, kdy v současné době hardwareové nároky a finanční nákladnost brání plnému nasazení tohoto systému. V závěru jádra práce se autor zabýval problematikou pracovněprávní, a to především docházkových systémů, ale také svobodně uděleným souhlasem. Autor u biometrických docházkových systémů odkazuje na nutnost upravení výjimky dle čl. 9 odst. 2 písm. b) GDPR v národní legislativě pro dosáhnutí uspokojivé právní úpravy. Co se týče svobodně uděleného souhlasu, nezbývá než konstatovat, že budoucí vývoj bude do jisté míry závislý na budoucí praxi a dospělosti národní úpravy vůči GDPR.

Seznam zkratek

COREPER	Výbor stálých zástupců
ESD	Evropský soudní dvůr
ESLP	Evropský soud pro lidská práva
FTC Akt	Federal Trade Commission Act
GDPR	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.
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OSN	Organizace spojených národů
Sb.	Sbírka zákonů
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
VDLP	Všeobecná deklarace lidských práv
WP29	Pracovní skupina WP 29 (Article 29 Working Party)

Seznam použitých zdrojů

1. Seznam použité literatury

BIEGELMAN, MARTIN, T. *Identity theft handbook: detection, prevention, and security*. Hoboken, N.J.: Wiley, c2009. ISBN 978-0-470-17999-4. Str. 1-10

BRODY, RICHARD. MULIG, ELIZABETH VALERIE. *Phishing pharming and identity theft.* Academy of Accounting and financial Studies Journal. 2007. roč. 11, č. 3.

GERLOCH, ALEŠ. *Teorie práva*. 5., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-233-2. Str. 19-34

KINDT, ELS J. *Privacy and Data Protection Issues of Biometric Applications.* A Comparative Legal Analysis. Springer. 978-94-007-7522-0. Str. 76-78

KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D., *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

NEZMAR, LUDĚK. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4. Str. 14, 115-118

NIKOLAOS V. BOULGOURIS, KONSTANTINOS N. PLATANIOTIS a Evangelia MICHELI-TZANAKOU. *Biometrics Theory, Methods, and Applications.* Hoboken: John Wiley, 2009. ISBN 9780470522349. Str. 633-637

NULÍČEK, MICHAL. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. Str. 73, 78, 79-83, 88, 106, 107, 114, 162-169, 296, 297

POTOČNÝ, MIROSLAV; ONDŘEJ, JAN. *Mezinárodní právo veřejné: zvláštní část*. 6. dopl. a rozš. vyd. V Praze: C.H. Beck, 2011. Beckovy právnické učebnice. ISBN 978-80-7400-398-1. Str. 100

TOMÁŠEK, MICHAL, TÝČ, VLADIMÍR a MALENOVSKÝ JIŘÍ. *Právo Evropské unie*. Praha: Leges, 2013. Student (Leges). ISBN 978-80-87576-53-3, str. 107-110

USTARAN, EDUARDO. *European privacy: law and practice for data protection professionals.* Portsmouth, NH: International Association of Privacy Professionals, c2012. ISBN 978-0979590153. Str. 3-15

VOIGT, PAUL. von dem BUSSCHE, AXEL. *The EU General Data Protection Regulation (GDPR).* Spring International Publishing 2017. ISBN 978-3-319-57958-0. Str. 87

2. Seznam použitých internetových zdrojů

Odborné články a výkladová stanoviska

ARROWS advokátní kancelář, s. r. o. *ePrivacy a nařízení a GDPR.* [online]. [2019-01-19]. Dostupné z: https://www.epravo.cz/top/clanky/eprivacy-narizeni-a-gdpr-107391.html

Article 29 Working Party. *Working document on biometrics.* Adopted on 1 August 2003; 12168/02/EN, WP 80 [online]. [2018-03-12]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

KORBEL FRANTIŠEK, KOVÁŘ DALIBOR. Havel Holásek & Partners. *Changes in regulation of electronic signatures (eIDAS).* [online]. [2019-04-07]. Dostupné z: http://havelpartners.cz/images/stories/publikace/eu_legal_news_en_2015_12.pdf

KRAUSOVÁ A., HAZAN H., MATEJKA J., *Biometric Data Vulnerabilities: Privacy Implications,* [online]. [2019-01-24] Dostupné z: www.noveaspi.cz

MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V. *Biometrické údaje a jejich právní režim.* Revue pro právo a technologie 17/2018 str. 91[online]. [2019-04-11]. Dostupné z: https://www.beck-online.cz

MICHALEC, FILIP, *Silné ověření klienta podle RTS ke směrnici PSD2.* [online]. [2019-01-24]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-podle-rts-ke-smernici-psd2-105724.html

Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko č. 4/2007 k pojmu osobního údaje přijaté dne 20. června 2007.* [online]. [2019-02-01]. Dostupné z: https://www.uoou.cz/files/wp29-stanovisko_4-2007.pdf

Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko 5/2014 o Anonymizačních Technikách, přijato 10. dubna 2014.* [online]. [2018-04-11]. Dostupné z: https://www.pdpjournals.com/docs/88197.pdf

Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti, 8. červen 2017.* [online]. [2019-03-04]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30203

Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Opinion on Commission proposals on establishing a Framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration.* [online]. [2019-03-04]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198 Str. 6

Pracovní skupina pro ochranu osobních údajů zřízená podle čl. 29. *Opinion 01/2012 on the data protection reform proposals.* [online]. [2019-03-04]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf Str. 10

SLABÝ, T., AK Kříž a partneři s.r.o. *Docházkové systémy využívající biometrických údajů zaměstnanců z pohledu GDPR.* [online]. [2019-03-04]. Dostupné z: https://www.epravo.cz/top/clanky/dochazkove-systemy-vyuzivajici-biometrickych-udaju-zamestnancu-z-pohledu-gdpr-108322.html?mail

Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – *„Komplexní přístup k ochraně osobních údajů v Evropské unii“* (2011/C 181/01) [online]. [2018-03-14]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:181:FULL:CS:PDF

TOMÍŠEK, JAN. *Právní jednání biometrickými prostředky v elektronickém bankovnictví.* Právní rozhledy/2018, [online]. [2019-01-24]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7gvpxgxzrgyyc4y3mgm&groupIndex=0&rowIndex=0

UUOU. *Stanovisko č. 2/2014* [online]. [2019-04-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22532

Press release

Evropská Komise. *Security Union: Commission presents new measures to deny terrorists and criminals the means and space to act, Brusel 17. dubna 2018*. [online]. [2019-03-04]. Dostupné z: http://europa.eu/rapid/press-release_IP-18-3301_en.htm

Evropská komise. *The Commission will propose to reinforce the Schengen Information System (SIS) ze dne 21. prosince 2018*. [online]. [2019-03-10]. Dostupné z: http://europa.eu/rapid/press-release_AGENDA-16-4447_en.htm

Evropský parlament. *New EU rules on data protection put the citizen back in the driving seat.* Press release. [online]. [2019-01-19]. Dostupné z: http://www.europarl.europa.eu/news/en/press-room/20151217IPR08112/new-eu-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat

Ostatní zdroje

Agentura Evropské unie pro základní práva. *Handbook on European data protection law*. Belgie, 2014. [online]. [2018-03-12]. Dostupné z: http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

Berkeley Lawschool. *Research Guide to European Data Protection Law*. [online]. [2018-03-12]. Dostupné z: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1001&context=leg_res

BLENKINSOP, PHILIP. KOESTER, SAMANTHA. *EU Commission proposes making fingerprints mandatory in ID cards.* Reuters [online]. [2019-01-19]. Dostupné z: https://www.reuters.com/article/us-eu-security/eu-commission-proposes-making-fingerprints-mandatory-in-id-cards-idUSKBN1HO23A

BURGESS, MATT. *Biometric bank cards are almost here.* Wired [online]. [2019-01-24]. Dostupné z: https://www.wired.co.uk/article/mastercard-biometric-card-testing-visa-gemalto-scanner-fingerprint-trial

CNIL. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC.* [online]. [2018-04-12]. Dostupné z: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Council of Europe. *Handbook on European data protection Law.* 2018, [online]. [2019-02-01]. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf

Council of Europe. *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*. 2005. [online]. [2018-03-12]. Dostupné z: https://rm.coe.int/16806840ba

Debate in Council 2012/0011 (COD) – 25/10/2012 [online]. [2019-01-19]. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1232253&l=en&t=E

EDPS. *Opening a new Chapter for Data Protection.* [online]. [2019-01-19]. Dostupné z: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2015-06-edps_gdpr_en.pdf

eu-LISA. *AFIS for SIS II to be deployed this month 2. března 2018.* [online]. [2019-03-10]. Dostupné z: https://www.eulisa.europa.eu/Newsroom/News/Pages/AFIS-deployment-March-2018.aspx

European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law 2018 edition.* [online]. [2019-01-24]. Dostupné z: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf str. 99

European Parliament. 2012. Directorate-General for Internal Policies. *Reforming the Data Protection Package.* [online]. [2018-04-10]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET(2012)492431_EN.pdf

European Parliament. 2012. Dostupné z: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en

FLEMING, JEREMY. *EU lawmaker warns of data protection rules delay till 2016.* [online]. [2019-01-19]. Dostupné z: https://www.euractiv.com/section/digital/news/eu-lawmaker-warns-of-data-protection-rules-delay-till-2016/

Gesellschaft für Datenschutz und Datensicherheit. *Einheitliches Datenschutzrecht in Europa durch Verordnung*. Kolín, 2011. [online]. [2018-03-14]. Dostupné z: https://www.gdd.de/aktuelles/startseite/news/einheitliches-datenschutzrecht-in-europa-durch-verordnung

HEJDUK, MAREK. *Hejduk (Svobodní): Potřebujeme biometrické cestovní doklady?* [online]. [2019-01-24]. Dostupné z: https://www.parlamentnilisty.cz/politika/politici-volicum/Hejduk-Svobodni-Potrebujeme-biometricke-cestovni-doklady-561791

HOGAN LOVELLS. *EU draft Data Protection Regulation: the LIBE Committee amendments*. [online]. [2019-01-19]. Dostupné z: https://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf

HOLDEN, MICHAEL. *Attorney General Lynch Chides EU decisions to restrict data sharing.* Reuters. [online]. [2019-01-19]. Dostupné z: https://www.reuters.com/article/us-usa-security-europe/attorney-general-lynch-chides-european-decisions-to-restrict-data-sharing-idUSKBN0TS0UV20151209

ICLG. *The International Comparative Legal Guide to: Data Protection 2018*. 5th Edition [online]. [2019-03-18]. Dostupné z: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Implications of the European Commision´s proposal for a general data protection regulation for business, London Economics [online]. [2019-01-19]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

JOAS, HANS. *Max Weber and the Origin of Human Rights: A Study on Cultural Innovation*. [online]. [2018-03-14]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=923846

JOLLY, IEUAN. *Data protection in the United States: overview.* 2017. [online]. [2018-04-12]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/6-5020467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

KOMÍNKOVÁ, MAGDA. *Jak vznikalo GDPR*. [online]. [2019-01-19]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

KUNER, CHRISTOPHER. *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law.* 2012. [online]. [2018-03-12]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781

LANCE, J., *Phishing Exposed*. [online]. [2019-02-17]. Dostupné z: http://index-of.co.uk/Hacking-Coleccion/Phishing%20Exposed.pdf

LANG, JAMES C. *The Legislative History of the Federal Trade Commission Act*. 1974. [online]. [2018-04-13]. Dostupné z: http://heinonline.org/HOL/LandingPage?handle=hein.journals/wasbur13&div=14&id=&page=

MAYHEW, STEPHEN. *History of Biometrics*. 2018. [online]. [2018-04-11]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

MCKANE, JAMIE. *The average gaming PC – 5 years ago vs today.* [online]. [2018-12-31]. Dostupné z: https://mybroadband.co.za/news/gaming/262481-the-average-gaming-pc-5-years-ago-vs-today.html

MŠMT. *Metodická pomůcka k aplikace obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství.* [online]. [2019-02-01]. Dostupné z: http://www.msmt.cz/file/44592/

OECD. *„Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [online]. [2019-04-10]. Dostupné z: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

RUSSEL, JOHN. *China's CCTV surveillance network took just 7 minutes to capture BBC reporter.* 2017. [online]. [2018-04-10]. Dostupné z: https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/

SHIMANEK, ANNA E. *Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles*. Journal of Corporation Law, 2001. [online]. [2018-03-12]. Dostupné z: https://www.questia.com/read/1P3-73978673/do-you-want-milk-with-those-cookies-complying-with

SIGNOSOFT. *Jak to funguje.* [online]. [2019-04-07]. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php

SMEJKAL, VLADIMÍR. *Dynamický Biometrický Podpis a Nařízení GDPR.* [online]. [2019-04-07]. Dostupné z: https://journals.muni.cz/revue/article/view/8282

STIGLER, STEPHEN M. *Perspectives; Galton and Identification by Fingerprintes*. Statistics Department, Chicago. [online]. [2018-04-11]. Dostupné z: http://www.genetics.org/content/140/3/857

ŠČUREK, RADOMÍR. *Biometrické metody identifikace osob v bezpečnostní praxi*. Ostrava, 2008. [online]. [2018-04-11]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

ŠKORNIČKOVÁ E. *Anonymizace a pseudonymizace.* [online]. [2019-02-01]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/

The European Data Protection Board. *Endorsement 1/2018.* [online]. [2019-04-08]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

TÜRK, ALEX. *The Future of Privacy*. 2009. [online]. [2018-03-14]. Dostupné z: http://194.242.234.211/documents/10160/10704/WP168++The+Future+of+PrivacY

UOOU, Q&A *Ze školství.* [online]. [2019-02-01]. Dostupné z: https://www.uoou.cz/ze-skolstvi/ds-5088/p1=5088

Visa company. *Fingerprint authentication moves from phones to payment cards* [online]. [2019-01-24] Dostupné z: https://usa.visa.com/visa-everywhere/security/biometric-payment-card.html

WARREN, SAMUEL, BRANDEIS, LOUIS. *The Right to Privacy.* Harvard Law Review, Vol. 4, No. 5, 1890. [online]. [2018-03-12]. Dostupné z: https://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

WILHELM, ERNST-OLIVER. *A brief history of the General Data Protection Regulation.* [online]. [2018-03-12]. Dostupné z: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

YU, P. K. *An Introduction to the EU Directive on the Protection of Personal Data*. 2001. [online]. [2018-03-13]. Dostupné z: http://www.peteryu.com/gigalaw0701a.pdf

3. Seznam použitých právních předpisů

110 STAT. 1936 PUBLIC LAW 104-191, 104th Congress, The Health Information Portability and Accountability Act.

113 STAT. 1338 Public Law 106-102, 106th Congress, The Gramm Leach Billey Act.

117 STAT. 2708 PUBLIC LAW 108-187, CAN-SPAM Act.

15 U.S.C. 6501-6506, The Children's Online Privacy Protection Act.

Convention for the Protection of the Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28. 1. 1981.

Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství, publikováno jako Sdělení Ministerstva zahraničních věcí č. 111/2009 Sb.m.s., s přihlédnutím k opravám uveřejněným ve sděleních č.40/2010 Sb.m.s. a č. 68/2010 Sb.m.s.

Listina základních práv a svobod Evropské unie, publikovaná v Úředním věstníku Evropské unie, č. (2012/C 326/02).

Mezinárodní pakt o občanských a politických právech ze dne 19. 12. 1966.

Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II).

Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II).

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.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikace a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

Nařízení Rady (EU) č. 1417/2013 ze dne 17. prosince 2013, kterým se stanoví vzor průkazu vydávaného Evropskou unií.

Nařízení Rady EU č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy.

Návrh Nařízení Evropské komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady 2015/236ž, pokud jde o

regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace.

Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů).

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES.

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 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. In: EURLex [právní informační systém]. Úřad pro publikace Evropské unie.

Úmluva o ochraně lidských práv a základních svobod ve znění protokolů 3, 5 a 8 ze dne 4. 11. 1950. V ČR publikováno jako Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb.

Všeobecná deklarace lidských práv ze dne 10. 12. 1948.

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

4. Seznam použitých rozhodnutí soudů a jiných orgánů

ESLP ve věci 13710/88 ze dne 16. prosince 1992 Niemietz v. Germany

ESLP ve věci 30562/04 a 30566/04 ze dne 4. prosince 2008 S. and Marper v. the UK

Rozsudek ESD Ve spojených věcech C-446/12 až C-449/12 ze dne 16. dubna 2015 (ECLI:EU:C:2015:238)

Rozsudek ESD ve věci C-213/15 ze dne 19. října 2016 Patrick Breyer v. Spolková republika Německo (ECLI:EU:C:2016:779)

Rozsudek ESD ve věci C-291/12 ze dne 17. října 2013 Michael Schwarz v. Stadt Bochum (ECLI:EU:C:2013:670)

Rozsudek ESD ve věci C-553/07 ze dne 7. května 2009 ve věci College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer (ECLI:EU:C:2009:293)

5. Další rozhodnutí orgánů EU

Rozhodnutí Rady 2007/533/SV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II)

Abstrakt

Ochrana osobních údajů v EU – Biometrické údaje

Tato práce se zabývá ochranou osobních údajů zaměřenou především na biometrické údaje.

V první kapitole této práce se autor zabýval především historickým kontextem. Právo na soukromí představuje i dnes základní stavební kámen ochrany osobních údajů. A proto jeho vymezení a následné navázání na ochranu osobních údajů se jevilo jako nezbytné pro správné pochopení kontextu problematiky. Autor se dále v rámci této kapitoly zabýval právem na ochranu osobních údajů nejen v rovině evropského kontextu, ale nastínil také nejednotnou právní úpravu ochrany osobních údajů pro daná odvětví v Americe, kde v současné době zcela absentuje legislativa typu obecného nařízení ochrany osobních údajů.

Druhá kapitola představovala zakotvení nejen právních principů z hlediska jejich relevance pro jejich právní řád, ale také zvláštní principy zakotvené v obecném nařízení, jež je nezbytné dodržovat pro řádné zpracování osobních údajů.

Třetí kapitola pojednávala o samotném pojmu osobních údajů. Současně bylo však zapotřebí vymezit i další pojmy, jež nelze opomenout ve vztahu k pojmu osobních údajů. Tedy zakotvení anonymního údaje jako osobního údaje, jež prošel procesem anonymizace, dále také pojmu zvláštní kategorie osobních údajů, který je fundamentální pro problematiku biometrických údajů a v poslední řadě také samotný pojem zpracování osobních údajů.

Ve čtvrté kapitole se autor zaměřil na pojednání o pojmu biometrického údaje jak z hlediska právního, tak z hlediska technického. Tyto dvě roviny se v rámci této oblasti vzájemně prolínají. Autor vymezil biometrický údaj z hlediska technického spolu s nezbytnou vazbou na příslušné technologické procesy a jejich úskalí. V právní rovině nadefinoval pojem biometrického údaje a současně stanovil, za jakých situací je zpracování této zvláštní kategorie osobního údaje možné.

V páté a závěrečné kapitole se autor této práce zaměřil především na biometrické údaje a jejich aplikaci v praxi. Autor nastínil současné metody využití biometrických údajů v bankovnictví, ve vztahu k podpisům, dále ale i k cestovním či identifikačním dokladům, v Schengenském informačním systému a závěrem v rámci pracovněprávní praxe.

Klíčová slova: biometrické údaje, ochrana osobních údajů, právo Evropské unie

Data protection in the EU – Biometric data

The main aim of this thesis is to deal with the data protection in connection with the biometric data.

In the first chapter, the author of this work deals with the historical context. The right to privacy even nowadays represents the solid ground of the data protection. Therefore, its delimitation and subsequent connection with the data privacy is of an upmost importance for a proper understanding of this problematics. The author also deals with the data protection not only in the european context, but also with the disunited legislation in the US, where a legislation in the context of general data protection regulation is absent.

The second chapter mainly dealt with stating the general legal principles and their relevance to the legal order as well as with the special principles laid down in the regulation, which are mandatory to be upheld.

The third chapter dealt with the term of personal data. Moreover, it was also important to define the other terms, which goes hand in hand with the personal data term. Therefore, anonymous data as a personal data, which went through the anonymisation process, as well as the special category of personal data, which represents the fundament of the problematics of the biometric data and lastly also the term of data processing.

In the fourth chapter the author's interest inclined to describe the term of biometric data from the legal and technological perspective. These two dimensions go hand in hand in this branch. The author laid down the biometric data term from the technological perspective with the neccessary explanation of the technological processes and their downsides. In the legal branch, the author laid down the term of the biometric data and at the same time stated, in which cases is the data processing possible as it represents the special category of the personal data.

In the fifth and the last chapter the author of this work dealt with the biometric data and their application. The author laid down the nowadays methods of implementing biometric data in the banking sphere, in regards with the biometric signatures, as well as in the travel and national identification documents, in the Schengen informational system and lastly in regards with the labour law.

Key words: biometric data, data protection, law of the European Union