Acta Informatica Pragensia, 2019, 8(2), 88–111
DOI: 10.18267/j.aip.126
Original Article

Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů

Analysis of Biometric Data Under the General Data Protection Regulation

Ján Matejka [1,2], **Soňa Matochová** [1,3], **Josef Prokeš** [1,3]

Abstrakt

Příspěvek pojednává o aktuálním tématu současného digitálního věku, jímž jsou otázky spojené s právní ochranou biometrických údajů, včetně možnosti jejich zneužití. Těmto otázkám dosud nebyla v ČR věnována systematická pozornost a neexistují ani statistické údaje týkající se postojů veřejnosti k biometrickým údajům a jejich užití. V rámci tohoto příspěvku tak byla provedena analýza současné právní úpravy, jež klade na zpracování biometrických údajů, které se řadí do zvláštní kategorie osobních údajů, výrazně vyšší standard ochrany než dřívější právní úprava. Zvažovány byly jak konkrétní důsledky dopadu této úpravy na soukromí člověka, včetně jejích principů, tak i subjektivní vnímání většiny významných atributů chování hlavních aktérů. Cílem článku je přispět ke zvýšení povědomí o rizicích používání biometrických údajů, jakož i přispět k vysvětlení klíčových principů obecného nařízení o ochraně osobních údajů při jeho aplikaci v oblasti biometriky. Příspěvek rovněž podrobně informuje o sociologickém průzkumu CVVM, jež obecně ukázal, že česká populace v poměru tři ku jedné upřednostňuje ochranu svého soukromí před uživatelským komfortem. Zhruba 71 % všech respondentů někdy o biometrických údajích slyšelo a téměř polovina z nich má alespoň hrubou představu o tom, co jsou to biometrické údaje. Pouze 70 % respondentů si však uvědomuje, že moderní technologie umožňují shromažďovat, zpracovávat a (zne)užívat osobní údaje, a to i bez jejich vědomí či souhlasu.

Klíčová slova: Biometrika, GDPR, ochrana dat, odpovědnost a prevence, behaviorální analýza, profilování, princip technologické neutrality, princip proporcionality.

Abstract

The article deals with the topical issue of the current digital age, the questions related to the legal protection of biometric data, including the potentiality of their misuse. These issues have not yet been systematically addressed in the Czech Republic and there is no statistical data on public attitudes towards biometric data and its use. This article presents an analysis of the current legal regulation, which places a significantly higher standard than the previous legislation on the processing of biometric data as a special category of personal data. The authors considered both particular consequences of the impact of this regulation on human privacy and principles of this regulation as well as the subjective perception of the most important attributes of the behaviour of the main actors. The aim of the article is to contribute

[1] Institute of State and Law, Czech Academy of Sciences, Národní 18, Prague 1, Czech Republic
✉ matejka@ilaw.cas.cz

[2] Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 49/83, Prague 8, Czech Republic

[3] Office for Personal Data Protection, Pplk. Sochora 27, Prague 7, Czech Republic

to raising the awareness of the risks of using biometric data and to contribute to explaining the key principles of GDPR in its application to biometrics. The article also discusses the related outputs of the sociological survey of CVVM showing that Czech population prefers the protection of their privacy over user comfort (three to one ratio). About 71% of all respondents have heard about biometric data and almost half of them have at least a rough idea what biometric data is. However, only 70% of respondents realize that modern technologies make it possible to collect, process and (mis)use personal data, even without their knowledge or consent.

Keywords: Biometrics, GDPR, Data Protection, Responsibility and Prevention, Behaviour Analysis, Behaviour-based Tracking, Principle of Technological Neutrality, Principle of Proportionality.

1 Úvodní a metodologické poznámky

Technologický rozvoj a globalizace jsou synonymy naší doby. Přes poměrně krátkou dobu jejich existence přináší hluboké ekonomické i společenské změny. Rychlost rozvoje technologií má exponenciální charakter. Předpokládá se, že během následujících dvaceti let dojde k zavedení automatizace, robotizace, umělé inteligence a dalších technologií do výroby a služeb a způsobu jejich řízení. Názory odborníků se liší v tom, jak rychle k těmto změnám dojde a nakolik zásadní budou. Technologický pokrok v každém případě znamená podle expertů velkou příležitost pro zvýšení efektivnosti výroby a služeb a ulehčení práce. Budou se měnit pracovní postupy, formy a podmínky práce a také požadavky na znalosti a dovednosti pracovníků. Nové technologie mají vést zejména k nahrazování rutinních činností, které lze algoritmizovat. Podle odhadů OECD (2016) bude v ČR v průběhu následujících 10-20 let automatizací ohrožena asi desetina pracovních míst, což by představovalo úbytek více než 400 tisíc pracovních míst. Předpokládá se však, že budou vytvořena nová místa, zejména ve službách. V souvislosti s těmito změnami odborníci hovoří o nutnosti posílit klíčové kompetence lidí a připravit stávající i nové generace na přicházející změny a na odlišnou realitu práce i jejich osobního života. Je zřejmé, že změny se dotknou osobních údajů a soukromí, ale i dalších základních práv.

Současné technologie velmi často využívají nebo jsou přímo založeny na zpracování dat a osobních údajů. Rychlé tempo technologických změn a globalizace od základů změnily rozsah a způsob sběru, používání a přenosu osobních informací a také přístupu k nim. Data jsou rozsáhle využívána jak v podnikání, tak ve veřejné správě. Mnohdy byla shromážděna bez vědomí či souhlasu dotčených osob. Pokud velké objemy shromážděných dat neobsahují osobní informace, byly anonymizovány, šifrovány či alespoň pseudonymizovány, nemusí představovat žádná či velká rizika z pohledu soukromí a osobních údajů. Ovšem většina v současnosti generovaných dat zpracovává osobní údaje a rozsáhlé datové soubory zvyšují rizika pro lidské soukromí a ochranu osobních údajů. Často dochází k únikům dat, přičemž zpravidla to dotčené subjekty ani nezjistí. Jak upozorňují někteří autoři (např. Matejka, 2013), tato latentní rizika se týkají zejména zvláštních kategorií osobních údajů. Existují také technologie využívající biometrická data přímo k identifikaci osob. Jedná se např. o používání otisku prstů či rekognici obličeje. I v těchto případech dochází ke shromažďování osobních údajů; vznikají tak legitimní otázky ochrany soukromí a osobních údajů. Právo by mělo být připraveno na tyto změny.

Nástrojem, který má komplexně řešit závažné otázky vztahu mezi technologickým rozvojem a ochranou osobních údajů či stanovit kritéria pro zvažování míry přiměřeného zásahu do

soukromí, je především Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 (NPP, 2016) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (SEP, 1995; dále nařízení), případně další navazující regulace. Z tohoto pohledu se jeví jako nezbytné zkoumat nové technologie v oblasti biometriky, jakož i zvažovat jejich konkrétní důsledky dopadu na soukromí a rodinný život člověka. Nařízení přitom požaduje pro zpracování biometrických údajů výrazně vyšší standard ochrany než dřívější právní úprava, tj. Směrnice 95/46/ES, když je řadí mezi zvláštní kategorie osobních údajů, tj. údaje se specifickým právním režimem.

Cílem tohoto článku je tak za přispění cíleného empirického průzkumu přezkoumat soulad možných způsobů zpracovávání biometrických údajů s novou právní úpravou, implementovat nové nástroje v nařízení a případně zaujmout nové přístupy či doporučení v oblasti biometriky. To vše s cílem postihnout vysoce specifickou podstatu biometrických systémů, a ne zcela transparentních procesů jednotlivých zpracování, včetně klíčových funkcionalit a rizik, jež jsou s nimi spojena, neboť biometrika je založena na složitých technologických postupech, jejichž vývoj je zpravidla natolik dynamický, že odpovědná a komplexní analýza či reakce zákonodárce v normativní rovině jeví se jako prakticky nerealizovatelná. O to důležitější je za této situace právní úprava založená na obecných zásadách a pravidlech, jež lze aplikovat na konkrétní skutkový stav, a to s ohledem na reálná očekávání či obecné povědomí svých adresátů. Pro dosažení takto vymezených cílů byl v souvislosti s tímto příspěvkem zpracován Centrem pro výzkum veřejného mínění Sociologického ústavu Akademie věd ČR, v. v. i. cílený průzkum s názvem Biometrika a její využívání z pohledu české veřejnosti provedený v září 2018, jehož závěry budou v rámci tohoto příspěvku podrobně představeny.

Navazujícím cílem tohoto příspěvku pak je přispět ke zvýšení povědomí o rizicích používání biometrických údajů, jakož i upozornit na další související rizika. K dosažení tohoto účelu postupuje tento článek systematicky od obecného ke zvláštnímu, tedy od vysvětlení cíle a principů obecného nařízení k jeho konkrétní aplikaci v oblasti biometriky. Závěrem jsou formulovány obecné i konkrétní teze obsahující doporučení pro zacházení s biometrickými údaji, včetně principů, na nichž by měly být biometrické systémy založeny. Autoři v příspěvku dále zdůrazňují potřebu analyzovat existující rizika zpracování biometrických údajů, kde je třeba zvláštní pozornost věnovat zranitelným skupinám osob, především dětem, zaměstnancům, seniorům, případně hendikepovaným.

2 Důvody pro vznik obecného nařízení a jeho charakteristika

2.1 Důvody vzniku obecného nařízení

Ve výše uvedeném kontextu se objevuje celá řada otázek týkajících se obecného nařízení, k nimž na prvém místě patří otázka jeho potřeby a důvodů pro přijetí, charakteru právní úpravy, případně schopnosti plnit očekávané zadání v ochraně osobních údajů. V tomto ohledu má význam, že zahájení prací na obecném nařízení v EU předcházel reprezentativní veřejný průzkum, tzv. Eurobarometr, provedený u 28 000 respondentů zvláštním oddělením Evropské komise zabývajícím se veřejným míněním. Dotazník, který zjišťoval názory občanů na ochranu soukromí, byl velmi podrobně strukturován a kladl občanům např. otázky, zda se domnívají, že jejich soukromí je dostatečně chráněno, či zda se obávají zneužití svých dat či podvodů. Velmi stručně lze shrnout, že průzkum dospěl k závěru, že více než 80 % občanů EU považuje současnou ochranu soukromí za nedostatečnou.

Vzhledem k tomu, že právo na ochranu osobních údajů a soukromí představují hodnoty demokratického právního státu chráněné evropským právem, lidskoprávními dokumenty i

právní úpravou a ústavním pořádkem ČR (zejména čl. 16 Smlouvy o fungování EU, čl. 7 a 8 Listiny základních práv EU, čl. 8 Úmluvy o lidských právech a základních svobodách, případně článků 7 odst. 1 a 10 Listiny základních práv a svobod), jejich absence, ohrožení či porušení mohou být považovány za deficit demokracie a právního státu. Také tento důvod vedl na úrovni EU k celkem jednoznačné podpoře přijetí nové legislativy formou nařízení; dle Evropské komise (MEMO, 2014) hlasovalo v Evropském parlamentu hlasovalo 621 poslanců pro návrh nařízení, 10 proti a 22 se zdrželo.

Bylo totiž zřejmé, že cílů sledovaných zamýšlenou právní úpravou v oblasti ochrany osobních údajů není možné dosáhnout prostřednictvím směrnice, která nevedla k potřebné jednotě právní úpravy v různých státech. Viviane Redingová, místopředsedkyně Komise a komisařka odpovědná za spravedlnost, základní práva a občanství, tehdy prohlásila, že *„účinná ochrana údajů je zcela zásadní pro naši demokracii a je nosným pilířem pro další základní práva a svobody.“* Smyslem přijetí obecného nařízení byla tedy potřeba nalézt rovnováhu mezi obavami o narušení soukromí a umožněním volného pohybu informací, který napomáhá tvorbě ekonomických příležitostí.

2.2 Charakteristika obecného nařízení

O obecném nařízení je třeba především říct, že se vyznačuje velmi dobrou legislativní úrovní. Lze je stručně charakterizovat tak, že jde o komplexní, rozsáhlou a zásadní právní úpravu zajišťující ochranu osobních údajů a souvisejících základních práv. V souvislosti s obecným nařízením je zmiňována jeho architektura, mluví se také o konstrukčních principech. Těch je několik, zejména lze zmínit přístup založený na riziku, jednotnost pravidel, technologickou neutralitu či preventivní působení pravidel. Pokud jde o přístup založený na riziku, jeho podstatou je, že opatření obsažená v nařízení se uplatní v rozsahu a míře závislé na riziku pro práva a svobody subjektu údajů, tedy cíleně a adresně v závislosti na potenciálním ohrožení. Zdůrazňuje se také, že evropská pravidla ochrany osobních údajů a soukromí jsou koncipována jako preventivní, směřují tedy k tomu, aby pokud možno vůbec k ohrožení či porušení ochrany dat nedošlo. Nástroje prevence představují i principy a instituty obecného nařízení, především princip minimalizace a transparentnosti včetně informační povinnosti, záměrná a standardní ochrany osobních údajů (*privacy by design* a *privacy by default*), institut záznamů o činnostech, posouzení vlivu, pseudonymizace, šifrování, předchozí konzultace, pověřenec pro ochranu osobních údajů, ale také právo na uplatnění námitek a účinnou soudní ochranu. Dalším klíčovým principem nezbytným k dosažení cílů obecného nařízení je tzv. mechanismus jednotnosti, jehož cílem je jednotné uplatňování nařízení v celé Unii s cílem chránit fyzické osoby v souvislosti se zpracováním osobních údajů a usnadnit volný pohyb osobních údajů v rámci vnitřního trhu.

V případě zpracování osobních údajů nelze opomenout technologický aspekt, k němuž obecné nařízení zaujalo přístup v podobě tzv. principu technologické neutrality. Ten umožňuje, aby legislativa založená na obecných principech byla uplatňována nezávisle na charakteru technologií a mohla se tedy uplatnit i ve vztahu k nově vznikajícím či vyvíjecím se technologiím, aniž by bylo nutné přijímat novou právní úpravu. To je možné právě prostřednictvím obecných principů, které je možno aplikovat na konkrétní situace zpracování osobních údajů. V preambuli obecného nařízení je výslovně zmíněno, že technologická neutralita musí být cílem, protože jen tak lze chránit fyzické osoby bez ohledu na různé technologie, které mohou být používány. Neexistuje univerzální definice technologické neutrality, ale budou existovat interpretace, jak vhodně postupovat v konkrétních případech. V principu se legislativa zaměřuje na účinky využívání technologií, nikoliv na technologie samotné. V čl. 15 preambule nařízení je to vyjádřeno tak, že *„aby se zabránilo vzniku vážného*

nebezpečí obcházení, ochrana fyzických osob by měla být technologicky neutrální a neměla by záviset na použitých technikách."

Výše uvedené působení nařízení je projevem toho, že jde o legislativu založenou na obecných principech, *principle-based regulation,* na rozdíl od legislativy založené na pravidlech, *rule-based regulation*. Jde o specifickou metodu právní regulace, která již byla použita u jiných evropských předpisů, např. u regulace emisí. Ačkoliv platí, že je v zásadě každé právní odvětví ovládáno určitými obecnými principy, v tomto případě adresáti normy sami aplikují obecné principy nařízení na své konkrétní podmínky, a volí způsoby, jak optimálně dosáhnout cílů právní úpravy. Vztah mezi požadavkem, který stanoví princip, a povinností jej dodržet, je přímý. Regulace založená na principech ponechává oproti regulaci založené na podrobných pravidlech větší prostor správcům (zpracovatelům) k zajištění souladu s obecným nařízením. Mají tak flexibilitu ve způsobu, jakým dosáhnout cílů nařízení. Prakticky se odpovědnost za přijatá opatření přenese v organizaci na vyšší úroveň rozhodování a lze tak propojit ochranu osobních údajů s dalšími souvisejícími oblastmi, jakými jsou kybernetická bezpečnost, řízení rizik či audit. Pro správce tak vzniká benefit, který má podobu výhody (*benefit´s dividend*) spočívající v tom, že může deklarovat soulad s žádoucími pravidly ochrany osobních údajů vůči svým zákazníkům nebo uživatelům.

Výše zmíněné obecné principy zpracování osobních údajů podle obecného nařízení jsou stanoveny v čl. 5 obecného nařízení a rozumí se jimi, že osobní údaje musí být

- zpracovány zákonným, korektním a transparentním způsobem;
- zpracovány v souladu s účelovým určením, tj. pouze pro určité, výslovně vyjádřené a legitimní účely;
- ve vazbě na účel zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah, tj. princip minimalizace;
- musí být přesné a v případě potřeby aktualizované;
- mohou být uloženy pouze po dobu do naplnění účelu, pro který byly shromážděny, což je nazýváno jako omezení uložení;
- musí být přijata technická a organizační opatření odpovídající předpokládanému riziku;
- správce je odpovědný za splnění požadavků na zpracování osobních údajů.

Zde je třeba zdůraznit, že princip odpovědnosti správce, který ač je uveden jako poslední v pořadí, je zároveň principem nejdůležitějším a pro dosažení cílů nařízení zcela zásadním. Vychází z toho, že pouze správce, který zná veškeré konkrétní okolnosti své činnosti, může zajistit, aby zpracování, které provádí, bylo v souladu s požadavky ochrany dat, které na něj klade právní úprava. Tento princip byl sice již součástí dřívější právní úpravy ochrany osobních údajů, nebyl však dostatečně důsledně uplatňován.

Další zásadní skutečnost, která má ovšem řadu důsledků, spočívá v tom, že obecné nařízení chrání základní či lidská práva, tedy hodnoty, kterým je přiznána nejvyšší ochrana jak ve vnitrostátním právu, tak právu EU. V kontextu obecného nařízení jde zejména o ochranu fyzických osob v souvislosti se zpracováním osobních údajů. Toto právo ovšem obecné nařízení nekoncipuje jako právo absolutní, ale zdůrazňuje, že musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy. Preambule obecného nařízení ve svém čl. 4 výslovně uvádí, že nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou EU, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost. Nesnadný úkol spočívá v nalezení rovnováhy

těchto práv v konkrétních případech. Nejvhodnějším nástrojem, který právo pro tento účel používá, je test proporcionality.

Princip proporcionality známý především z ústavního práva lze charakterizovat jako právní princip využívaný při kolizi zájmu společnosti a práva jednotlivce nebo kolizi dvou či více chráněných subjektivních práv. Základem pro jeho používání je více metodologií různé složitosti, nejčastěji se vychází z metodologie Alexyho (1986, str. 75-77). Soudy tento princip používají různě důsledně, což je předmětem kritiky (např. Kosař, 2008, str. 3-19). Jeho podstata je nicméně v určení práv, o která se jedná, poté zvážení, kterému z nich je třeba dát přednost, a konečně jak minimalizovat omezení nutná ve vztahu k druhému právu. Omezení základních práv a svobod je podle testu proporcionality možné pouze tehdy, jedná-li se o zásah, který je pro dosažení sledovaného cíle vhodný, nutný a přiměřený (viz Nález ÚS, 1994). Kritérium vhodnosti zkoumá, zda institut omezující základní právo, umožňuje dosáhnout stanovený cíl. Kritériem pro nutnost zásahu je skutečnost, že ve vztahu k chráněnému zájmu nelze užít jiného objektivně srovnatelného prostředku, jímž by docházelo k menšímu zásahu do chráněných zájmů dotčených subjektů údajů. Za přiměřený je považován takový zásah, kdy je možno očekávat, že prospěch dosažený realizací dané činnosti bude větší než nepříznivý následek jí způsobený, v tomto případě zejména v podobě míry zásahu do práva dotčených subjektů údajů.

Test proporcionality, který používá judikatura Ústavního soudu, a odkazuje na něj i Úřad pro ochranu osobních údajů ve svém rozhodovací praxi (viz ÚOOÚ, 2013), používá již uvedená kritéria vhodnosti, nezbytnosti a přiměřenosti. Na princip proporcionality ovšem nestačí jen odkázat, ale je nutné ho aplikovat na konkrétní konkurující práva a okolnosti. Přesvědčivá argumentace při používání tohoto principu je velmi důležitá a návodná pro další používání v praxi v obdobných případech. Princip proporcionality bude do budoucna rozpracován pro případy kolize práva na ochranu osobních údajů a dalších práv a bude vytyčovat meze jednotlivých konkurujících si práv. Souvisí také s dalšími hodnotami v právu, přinejmenším s hodnotou spravedlnosti, přiměřenosti a rozumnosti. Signifikantní je, že také terminologie obecného nařízení v řadě případů odkazuje na požadavky nezbytnosti, rozumnosti a přiměřenosti. Tyto principy jsou systematicky zapracovány do celého obsahu nařízení v podobě požadavků vztahujících se na jednotlivé instituty jako např. přiměřenost zásahů do osobních údajů z důvodu omezení nezbytných v demokratické společnosti, jimiž jsou kupříkladu bezpečnost a předcházení trestným činům, přiměřenost zpracování osobních údajů ve veřejné správě, přiměřená opatření dozorového úřadu, přiměřenost sankcí, vynaložení přiměřeného úsilí na technická a organizační opatření apod. Tato adjektiva v objektivní rovině znamenají potřebu vyváženého nastavení a poskytují správcům obecná kritéria, jak pracovat s obecným nařízením v konkrétních případech.

Stranou pozornosti nemohou zůstat ani požadavky týkající se etických pravidel v digitálním věku. Aktuálně byla v souvislosti s obecným nařízením zahájena diskuse o potřebě nastavení etických pravidel v oblasti digitálních technologií. Jak v tomto kontextu uvádí Matochová (2008, str. 17), v obecně rovině platí, že předmět etiky spočívá v základních otázkách praktického rozhodování, a její hlavní zájem zahrnuje povahu konečných hodnot a standardů, podle kterých může být lidské jednání hodnoceno jako správné nebo špatné. Současný vývoj umělé inteligence a informačních technologií nepochybně vyvolává řadu etických otázek. Informační technologie nemají hranice, jsou globální, nerozlišují soukromý a veřejný prostor. Technologické systémy by měly být odpovědně navrhovány a rozvíjeny tak, aby respektovaly základní práva. Rozvíjet digitální etiku znamená zvažovat, jak chceme komunikovat, jaká rizika přináší informační technologie, jak zajistit, že rozhodování zůstane zachováno primárně lidským bytostem, nikoliv technologiím. Zvlášť v souvislosti s přístupem nejmladších generací k technologiím se mluví o jejich přílišné ovlivnitelnosti digitální kulturou na úkor běžné

komunikace. V tomto smyslu je důležitá role vzdělávání a rozvíjení kritického myšlení, jakož i snaha o nalézání nových etických východisek, kde je třeba mít stále na paměti, že soukromí je univerzální hodnota jako svého druhu součást svobody každého člověka; za účelem jejich ochrany by mělo dojít ke generačnímu posunu, který by nastavil digitalizovanou společnost eticky udržitelným způsobem.

3 Biometrika a biometrické systémy

3.1 Úvod

Jak bylo vysvětleno v úvodní části článku, cílem obecného nařízení je ochrana osobních údajů v kontextu dalších základních práv ve věku rychlého technologického rozvoje a globalizace. Tento cíl je obtížný za situace, kdy nový regulatorní rámec ochrany osobních údajů začal platit v době kdy již společnost ve velké míře přistoupila na výhody, které technologie nabízí, ovšem často výměnou za poskytování osobních údajů. Shromažďování osobních údajů a propojování technologií přitom ze své povahy znamená i určitá rizika, kterým se zcela nelze vyhnout a která plynou z toho, že fyzická osoba nemá své údaje pod kontrolou. Pokud obecné nařízení směřuje k tomu, aby subjekt údajů (znovu)získal kontrolu nad svými osobními údaji, což je předpokladem realizace práva na informační sebeurčení, znamená to také přijmout obecné nařízení jako normu potřebnou pro ochranu osobních údajů a dalších základních a lidských práv, či přímo pro zachování dalšího vývoje lidského rodu ve smyslu autonomního rozhodování o sobě samém. Předpokládá to kromě akceptace povinností plynoucích z obecného nařízení správci a zpracovateli také vědomý a poučený přístup občanů k vlastním osobním údajům. V praktické rovině je třeba aplikovat obecné nařízení na jednotlivé oblasti, což vždy předpokládá jak znalost obecných principů nařízení, tak právní úpravy a praxe dotčené oblasti. V tomto ohledu je třeba rozlišovat sféru veřejného a soukromého práva, jednotlivé oblasti veřejné správy (školství, zdravotnictví) či specifika jednotlivých konkrétních oblastí jako jsou zdravotní registry, vědecký výzkum, statistika apod. Ačkoliv již k datu účinnosti obecného nařízení měl být zajištěn soulad s jeho požadavky v jednotlivých oblastech, je skutečností, že takového stavu bude muset být teprve dosaženo.

Ke specifickým oblastem prvořadého významu ve výše uvedeném smyslu patří nepochybně ochrana osobních údajů a soukromí ve spojení s využíváním nových biometrických technologií. Jedná se dokonce o jednu z nejcitlivějších otázek vůbec. V uplynulých letech bylo používání biometrických technologií široce zaváděno ve veřejném i soukromém sektoru a byla vyvinuta řada nových služeb využívajících biometrických technologií. Rychlý rozvoj aplikací biometrických technologií však nebyl doprovázen odpovídajícími opatřeními na ochranu osobních údajů. Rizikům, které přináší biometrické údaje, nelze porozumět bez základních znalostí o jejich fungování. Ačkoliv této oblasti nebyla dosud v ČR věnována systematická pozornost z pohledu ochrany osobních údajů, ve většině členských států EU již došlo v době účinnosti směrnice 95/46/ES k přehodnocení přístupu k biometrickým technologiím a k nastavení citlivějších pravidel, která zohledňují jejich specifické vlastnosti. V tomto kontextu je třeba si zodpovědět celou řadu otázek, počínaje tím, co jsou vlastně biometrické osobní údaje, jaká jsou jejich specifika, jaké jsou jejich výhody a nevýhody, jaká rizika jsou s nimi spojena a jak by se k nim mělo přistupovat z pohledu obecného nařízení. Na tomto základě lze formulovat obecná doporučení, jak přistupovat k biometrickým osobním údajům z pohledu ochrany osobních údajů.

3.2 Základní pojmy

Výchozími pojmy v souvislosti s pojednávanou problematikou jsou kromě pojmu biometrický údaj a biometrická identifikace, se kterými se bude pracovat v dalších částech textu, také pojmy biometrika a biometrie, které je žádoucí si vyjasnit. Základ obou slov je v řeckých slovech „*bios*“, což znamená život, a „*metron*“, což znamená měřit, jde tedy o rozpoznávání a měření určitých vlastností či charakteristik člověka. Pojmy biometrika i biometrie odpovídají anglickému výrazu *biometrics*, německému *Biometrie* a francouzskému *biométrie*. Vzhledem k tomu, že dva rozdílné české výrazy odpovídají pouze jednomu slovu v cizojazyčném překladu, vzniká otázka rozlišení obou pojmů. Definice lze nalézt např. v (Rak et al., 2008, str. 104-105), kde se tímto pojmem rozumí soubor vědních poznatků založených především na statistickém a analytickém přístupu, jejichž předmětem je zkoumání a následné praktické využití měřitelných charakteristik živých organismů s cílem jejich následné jednoznačné identifikace nebo verifikace, zatímco u pojmu biometrika se uvádí, že jde o měřitelné biometrické charakteristiky (obrazce, data apod.) živého organismu, které snímají, zpracovávají, vyhodnocují a uchovávají údaje v procesu identifikace nebo verifikace. Další definice biometriky uvádí (např. Güttler & Matejka, 2016, str. 1033-1056), jež pod tímto pojmem spatřují především techniku či systém, který umožňuje potvrdit totožnost daného uživatele. Z uvedených definic lze tedy usoudit, že biometrie je vědní obor, zatímco biometrikou se mají na mysli konkrétní postupy. V tomto případě je tedy nutno, obdobně jako u slov ekonomika a ekonomie, volit odpovídající ekvivalent podle kontextu; tomuto přístupu neodpovídá současná překladatelská praxe evropské komise, kde je výraz *biometrics* překládán (*promisue*) zpravidla celou řadou synonym, nejčastěji jako biometrie, biometrické technologie, biometrické systémy či biometrické prvky)

Dále je vhodné zabývat se pojmy totožnost a identita. Podle základního principu identity je každá osoba identická jen a pouze sama se sebou. Pojem identita (lat. *identitas*, odvozené od slova *idem* – stejný) je totožnost něčeho s něčím nebo se sebou samým. Potvrzení totožnosti uživatele představuje ověření jeho identity. Identitu osoby obecně prokazujeme pomocí toho, co daná osoba má u sebe (identifikační doklady, karty, čipy, často nazývané v anglické praxi souhrnným názvem *token-based identification*), toho, co daná osoba zná (hesla, identifikační čísla a kódy) a dále tím, co danou osobu představuje, tj. dle měřitelných biologických (biometrických) charakteristik (fyzický vzhled, tvar a rozměry těla a končetin, oči, hlas, vůně nebo zápach, otisky prstů, DNA). Lidská identita je kombinace biologických i psychických, vrozených i získaných individuálních a specifických vlastností a schopnosti vnímat sám sebe. Biometrická identifikace je založena na anatomicko-fyziologických nebo behaviorálních charakteristikách lidského jedince. Jde o automatizované využití jedinečných, měřitelných anatomických nebo fyziologických charakteristik nebo projevů člověka k jednoznačnému zjištění nebo ověření jeho identity.

Jak uvádí Rak et al. (2008, str. 14) k typickým příkladům biometrických údajů patří otisky prstů, struktura sítnice, struktura obličeje či hlas, ale také geometrie ruky, struktura žil nebo některé hluboce zakořeněné dovednosti či jiné behaviorální rysy (například vlastnoruční podpis, případně jak uvádí Smejkal (2017, str. 92) dynamicky biometrický podpis, úhozy na klávesnici, charakteristický způsob chůze nebo řeči atd.). Při biometrické identifikaci se využívá tzv. operačních kritérií biometrických technologií, jimiž jsou jednoznačnost, neměnnost, měřitelnost, uchovatelnost, spolehlivost, exkluzivita, praktičnost, přijatelnost (osobní, společenská, náboženská, praktická, etická atd.). Biometrická identifikace se začala používat v mnoha oblastech jako je ochrana platebních a bankovních karet, ochrana vstupu do objektů a zařízení, cestování a turismus, *customers´ relationship* management, ochrana majetku, telekomunikace, identifikace osob a ochrana před jejím zneužitím, ochrana

elektronických transakcí, kontrola pracovní docházky a přítomnosti na pracovišti, policejně-soudní a znalecké expertízy, vyhledávání pohřešovaných dětí, vězeňství, ochrana zbraňových systémů a individuálních zbraní. V tomto ohledu je ovšem třeba položit si obecnou otázku, v jakém rozsahu a za jakých podmínek je vhodné používat biometrické systémy.

3.3 Vývoj přístupů k biometrickým údajům

Pro pochopení biometrických údajů je důležité vysvětlit, že přístup k nim se vyvíjel postupně a byl podmíněn dynamickým vývojem biometrických technologií. Popis tohoto vývoje odhaluje charakteristiku, podstatu, specifika a problémy spojené s biometrickými technologiemi. Otázky spojené s biometrikou nebyly obsaženy v základních evropských dokumentech o ochraně osobních údajů, tedy v Úmluvě č. 108 Rady Evropy a ve směrnici 95/46/ES, protože v době přijetí těchto norem ještě nebyly diskutovány. K diskusím o biometrice došlo až po roce 2000 v souvislosti s obavami týkajícími se osobních údajů. následně se této problematice věnovalo několik dokumentů Pracovní skupiny 29 (WP29), jež byla ustanovena článkem 29. směrnice 95/46/ES, která účinností GDPR pozbyla platnost. WP29 představovala původně nezávislý evropský poradní orgán na ochranu dat a soukromí, který byl složen z vedoucích zástupců dozorových úřadů členských zemí Evropské unie (s účinností dnem nařízení se změnila v tzv. Evropský sbor pro ochranu osobních údajů (EPDB). Skupina WP29 však za dobu své existence vydala řada významných pracovních i interpretačních dokumentů, a to zejména:

a) Pracovní dokument o biometrice

Pracovní skupina k článku 29 (WP 29) vydala v roce 2003 první pracovní dokument o biometrice (WP29, 2003), ve kterém se pokusila systematicky popsat biometrické systémy, upozornit na jejich specifika a rizika a aplikovat ve vztahu k nim principy ochrany osobních údajů. Východiskem úvah ve stanovisku bylo, že rychlý pokrok biometrických technologií a jejich rozšířená aplikace v posledních letech vyžadují pečlivé prověření z perspektivy ochrany dat. Široké a nekontrolované využívání biometriky zvyšuje obavy ve vztahu k ochraně základních práv a svobod jednotlivců. Tento druh údajů má zvláštní povahu, protože se vztahuje k behaviorálním a fyziologickým vlastnostem jednotlivců a umožňuje jejich jedinečnou identifikaci.

Stanovisko se nevyslovilo jednoznačně k povaze biometrických systémů jako systémů zpracovávajících osobní údaje, když konstatovalo, že ve většině případů se jedná o osobní data. Uznávalo na jedné straně, že biometrická data jsou svou povahou osobní data, protože se vždy vztahují k jednotlivci, který je identifikovatelný, na druhé straně usuzovalo, že biometrická data nemusí vždy být osobní data. Toto pojetí se konkrétně vztahovalo k biometrickým šablonám, ve vztahu ke kterým byl převzat názor některých odborníků, podle něhož se nejedná o osobní data, pokud jsou biometrické údaje uchovávány způsobem, který žádným rozumným prostředkem nemůže být použit správcem nebo jinou osobou k identifikaci subjektu údajů. Jak správně uvádí Kindt (2013, str. 94-123) Pracovní skupina k článku WP 29 nicméně neposkytla jasná kritéria k rozlišení případů, kde biometrické údaje (konkrétně ve formě biometrické šablony) jsou osobní údaje, od případů, kdy tomu tak není. Tato otázka tak zůstala sporná. Např. v ČR zákon č. 101/2000 Sb., o ochraně osobních údajů, definoval jako osobní údaj pouze takový biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů; jakkoliv šlo o nepochybně dobrý úmysl zákonodárce, předmětné ustanovení § 4 písm. b) zákona č. 101/2000 Sb. ovšem obsahovalo potenciální problém v tom, že vyžadovalo kvalifikovanou znalost technologie biometrického zařízení, pokud mělo dojít k rozlišení, zda je umožněna přímá identifikace subjektu údajů.

b) Interpretační stanovisko k vymezení pojmu osobní údaj

K dalšímu posunu došlo až v roce 2007, kdy pracovní skupina WP 29 poskytla definici pojmu biometrický osobní údaj ve stanovisku 4/2007 o pojmu osobní údaj (WP 29, 2007). V tomto stanovisku se k biometrickým údajům přistupovalo z vědeckého pohledu a byly definovány jako „*biologické vlastnosti, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti.*“ Ve stejném stanovisku WP 29 uvedlo, že biometrické údaje mají dvojí povahu: jsou jednak informací o jednotlivci a jednak vytváří (jedinečné) spojení mezi jednotlivcem a jeho biometrickými vlastnostmi. Konkrétně stanovisko k problematice biometrických údajů uvedlo:

> *„Zvláštní pozornost je třeba věnovat biometrickým údajům. Tyto údaje mohou být definovány jako biologické vlastnosti, fyziologické charakteristiky, živé znaky nebo opakovatelné jednání, kdy jsou tyto rysy a/nebo jednání pro daného jedince jedinečné a měřitelné, a to i tehdy, když použité vzorky zahrnují určitý stupeň pravděpodobnosti. Typickými příklady takových biometrických dat jsou otisky prstů, retinální vzorky, struktura obličeje, hlasy, ale také geometrie rukou, vzorky žil nebo dokonce některé hluboce zakořeněné dovednosti nebo jiné charakteristiky chování (například ručně psaný podpis, stisknutí kláves, konkrétní způsob chůze nebo mluvy, atd. ...)*
>
> *Zvláštnost biometrických dat spočívá v tom, že mohou být považovány za obsah informací o konkrétní osobě (Titius má tyto otisky prstů), jakož i za prvek pro vytvoření vazby mezi jednotlivými informacemi a jednotlivci (tento předmět byl dotčen někým s těmito otisky prstů a tyto otisky prstů odpovídají Titiovi, proto se tohoto předmětu dotkl Titius). Jako takové mohou fungovat jako "identifikátory". Vzhledem k jejich jedinečné vazbě na určitou osobu mohou být biometrické údaje použity k identifikaci jednotlivce. Dvojitý znak se objeví také v případě údajů o DNA poskytovat informace o lidském těle a umožnit jednoznačnou a jedinečnou identifikaci osoby. Vzorky lidských tkání (jako vzorek krve) jsou samy zdroji, z nichž jsou extrahována biometrická data, ale samy o sobě nejsou biometrické údaje (například vzor pro otisk prstů je biometrickým údajem, ale samotný prst jím není). Odběr informací ze vzorků je proto shromažďováním osobních údajů, na které se vztahují pravidla směrnice. Shromažďování, skladování a používání samotných vzorků tkáně může být předmětem samostatných souborů pravidel.“*

Ve zvláštním stanovisku (WP 29, 2011) bylo tedy vyřešeno postavení biometrických údajů jako osobních údajů, nezodpovězenou však zůstala otázka jejich charakteru jako citlivých údajů. V tomto ohledu stanovisko zaujalo obecný názor, že biometrické technologie jsou úzce spojeny s určitými vlastnostmi jednotlivce a některé z nich lze využít k zjištění citlivých údajů. Konkrétně uvedlo: „*Některé biometrické údaje lze považovat za citlivé ve smyslu článku 8 směrnice 95/46/ES, zejména údaje odhalující rasový nebo etnický původ či údaje týkající se zdraví. Údaje o DNA určité osoby například často obsahují zdravotní údaje nebo mohou odhalit rasový či etnický původ. V tomto případě jsou údaje o DNA citlivými údaji a kromě obecných zásad ochrany údajů stanovených ve směrnici je nutno použít zvláštní ochranná opatření uvedená v článku 8. Za účelem posouzení citlivosti údajů zpracovávaných biometrickým systémem je nutno vzít v úvahu rovněž kontext, v jakém jsou údaje zpracovávány.“* Otázku charakteru biometrických údajů jako osobních a citlivých údajů řešily také jednotlivé státy ve svých vnitrostátních předpisech, přičemž jejich přístup nebyl jednotný.

c) Stanovisko pracovní skupiny WP 29 č. 3/2012 k vývoji biometrických technologií

K dalšímu posunu v problematice biometrických technologií došlo ve stanovisku pracovní skupiny WP 29 k vývoji biometrických technologií (WP 29, 2012), jež obsahuje podrobnější rozpracování charakteristiky biometrických údajů, definici biometrických pojmů (biometrické údaje, zdroj biometrických údajů, biometrická šablona, biometrické systémy, biometrická identifikace, biometrické ověřování, multimodální biometrie), právní analýzu jednotlivých důvodů zpracování osobních údajů, popis nových technologií a obecné pokyny a doporučení. Za klíčové v tomto stanovisku lze považovat zpracování specifik typických pro biometriku a upozornění na rizika, která jsou s nimi spojena. Rizika, která představují biometrické systémy, vyplývají ze samotné povahy biometrických údajů použitých při zpracování. Zásadní je, že biometrické systémy jsou svou povahou úzce spojeny s konkrétní fyzickou osobou, jelikož mohou využívat určitou jedinečnou vlastnost k identifikaci. To nepředstavuje vždy pouze klad, nýbrž má to i řadu stinných stránek. Technické inovace, které jsou velmi často představovány jako technologie, které pouze zlepšují uživatelské pohodlí při práci s aplikacemi, mohou vést k postupné ztrátě soukromí, nebudou-li zavedena přiměřená ochranná opatření. Jsou proto nezbytná technická a organizační opatření, která mají zmírnit rizika z hlediska ochrany údajů a soukromí a mohou pomoci zamezit negativním dopadům na soukromí evropských občanů a jejich základní právo na ochranu údajů.

Otázka charakteru biometrických údajů zůstala nicméně v evropském kontextu mnoho let předmětem odborných diskusí a sporů. Ačkoliv se jednalo o teoretické spory, měly dopady i na používání biometrických systémů v praxi. Diskuse intenzivně pokračovaly i během příprav obecného nařízení. V letech 2009-2011 Evropská komise uspořádala dvě veřejné konzultace o budoucnosti režimu ochrany osobních údajů. Mezi diskutovanými otázkami byl koncept postavení a charakteru biometrických dat v rámci ochrany dat, kdy bylo sporné, zda by mělo jít o citlivá data. Spory o charakter biometrických údajů trvaly po celou dobu přípravy nařízení. Po čtyřech letech intenzivních a dlouhých diskusí je vyřešil nový rámec ochrany dat v dubnu 2016, který jak v obecném nařízení, tak v bezpečnostní směrnici, zahrnul biometrické údaje mezi zvláštní údaje. Došlo také k rozlišení genetických a biometrických údajů, které jsou nyní definovány samostatně.

3.4 Charakteristika a definice biometrických osobních údajů

Obecné nařízení věnuje v bodech 51, 53 a 91 a čl. 4 odst. 14 a čl. 9 náležitou pozornost problematice biometrických údajů jak ve své preambuli, tak v samotném textu. Biometrické údaje řadí mezi osobní údaje, které jsou svou povahou zvláště citlivé z hlediska základních práv a svobod a vyžadují zvláštní ochranu při jejich zpracování s ohledem na možný vznik závažných rizik pro základní práva a svobody. Pojem biometrický údaj je v obecném nařízení výslovně zakotven, definován a zařazen mezi zvláštní kategorie osobních údajů. Dále nařízení obsahuje nástroje k ochraně biometrických údajů, které je správce povinen použít. Zvláště je třeba upozornit na to, že u biometrických údajů se předpokládá posouzení vlivu na ochranu osobních údajů (Bod 91 preambuli nařízení).

Obecné nařízení výslovně definuje biometrické údaje v článku 4 odst. 14 obecného nařízení, tj. v ustanovení, které obsahuje vymezení pojmů. Biometrické údaje jsou: *„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“*.

Výše uvedená definice biometrických údajů obsahuje následující prvky:

Biometrické údaje jsou považovány za osobní údaje.

Skutečnost, že v současné době jsou biometrické údaje definovány jako osobní údaje, znamená překonání dřívějšího výkladu, kdy bylo rozlišováno, zda lze přímo nebo nepřímo identifikovat subjekt údajů, a teprve v návaznosti na to, zda jde o osobní údaj či nikoli. V praxi se ukázalo jako obtížné až nemožné zjišťovat, zda lze přímo identifikovat subjekt údajů či nikoli, a to z důvodu složitosti či nemožnosti ověřit použitou technologii. Na nemožnost přímo určit fyzickou osobu se přitom odvolávali dodavatelé či prodejci biometrických systémů, kteří uváděli, že nabízené zařízení je založeno na používání biometrické šablony, pracuje tudíž s anonymními údaji, takže není potřebné aplikovat pravidla ochrany osobních údajů. V současné době již byl tento přístup překonán.

Biometrické údaje vyplývají z konkrétního technického zpracování.

Definice uvádí, že biometrické údaje vyplývají z konkrétního technického zpracování, nekonkretizuje však, co by se mělo myslet technickým zpracováním s výjimkou toho, že dalším účelem zpracování měla být jedinečná identifikace jednotlivce. Za účelem porozumění technickému zpracování biometrických znaků a jejich přeměně na data je nutné porozumět technickým krokům biometrické rekognice a z nich vyplývajících biometrických šablon. Za technické kroky biometrické rekognice jsou považovány následující:

- První fáze zpracování je registrace biometrických údajů v rámci biometrického systému. Biometrické údaje jsou zachyceny formou obrázku, např. obrázku otisku prstu.
- Ve druhé fázi jsou informace obsažené ve vzorku extrahovány, redukovány a transformovány na štítky nebo čísla pomocí algoritmu. Tato fáze se nazývá extrakce vlastností. Jsou zachovány pouze zásadní rozlišovací informace, které jsou nezbytné pro rozpoznání osoby. Extrahované vlastnosti jsou uchovávány v biometrické šabloně ve formě matematické reprezentace původní biometrické charakteristiky. Referenční šablona je pak uložena pro účely porovnání.
- Ve třetím kroku je biometrický vzorek (například špička prstu) prezentovaný u snímače porovnán s předem zaznamenanou šablonou (např. šablona otisku prstů).

Pro vysvětlení je třeba uvést, že biometrický vzorek a biometrická šablona představují biometrické formáty vyplývající z technického zpracování. Vzorek je obraz biometrické charakteristiky, zatímco šablona je redukovanou a kódovanou formou informací obsažených ve vzorku. V rámci režimu směrnice o ochraně údajů hrála otázka biometrických formátů důležitou roli v diskusi o právní kvalifikaci biometrických údajů. Biometrické vzorky byly v minulosti považovány za osobní údaje. Naproti tomu na biometrické šablony nebyly jednotné názory, navíc se vyvíjely v návaznosti na vývoj technologií. V raných diskusích o povaze biometrických šablon se předpokládalo, že biometrické šablony nemohou být převedeny zpět do biometrických vzorků, ze kterých pocházejí, podle některých názorů představovaly dokonce anonymní data. Podle jiných vědců byly biometrické šablony ve skutečnosti částečně reverzibilní a bylo možné případně obnovit informace obsažené v biometrických vzorcích. V posledních vědeckých studiích o právním postavení biometrických dat autoři dospěli k závěru, že biometrické šablony jsou přinejmenším částečně reverzibilní a nemohou být nadále považovány za anonymní data. Navíc s vývojem biometrických technologií bylo čím dále více zřejmě, že rozlišování identifikace pomocí toho, zda biometrická šablona umožňuje identifikaci jednotlivce, naráží na faktickou nemožnost ověřit mechanismus fungování biometrických technologií. Proto již nový rámec ochrany dat biometrické formáty nerozlišuje. To plyne z toho, že obecné nařízení je založeno na principu technologické neutrality a právní definice se nevážou

k nějakému speciálnímu formátu. V každém případě pojem informace obsažený v definici osobních údajů pokrývá jakýkoliv typ formátu.

Biometrické údaje se vztahují k fyzickým, fyziologickým nebo behaviorálním znakům fyzické osoby.

Toto kritérium uznává široké spektrum měřitelných lidských údajů, které mohou být použity pro biometrickou registraci: jedná se o fyzické a fyziologické znaky (jako otisk prstů, obličej nebo duhovku), stejně jako znaky chování (jako znak, hlas, chůze nebo podpis). Jak uvádí (např. Herrmann et al., 2013, str. 17-21) charakteristické znaky chování (tj. behaviorální charakteristika) mohou být značně nepřímé (např. záznam profilu DNS provozu, apod.), avšak zároveň velmi spolehlivé. Rozdíl mezi fyzickými a fyziologickými znaky není zcela jasný a mnoho expertů tyto znaky nerozlišuje.

Biometrické údaje umožňují nebo potvrzují jedinečnou identifikaci osoby

Toto kritérium je klíčovým prvkem právní kvalifikace biometrických údajů. Popisuje účel použití biometrických znaků, z nichž jsou biometrické údaje extrahovány. Stanovuje také prahovou hodnotu identifikace platnou pro biometrické údaje jako kategorii osobních údajů. Vychází z pochopení rozdílu významu mezi biometrickou identifikací a identifikací v kontextu ochrany údajů. Pro biometrickou komunitu má identifikace velmi specifický a úzký význam. Jedná se o proces identifikace jednotlivce porovnáním biometrického vzorku s dříve uloženými šablonami, které existují v různých databázích. To je tzv. shoda jednoho s mnoha. Identita v biometrickém kontextu nevyžaduje stanovení občanské či právní identity jednotlivce, ale stanovení toho, že vzorek a dříve zaznamenaná šablona pocházejí od téže osoby. Identita je stanovena, když je nalezena shoda mezi biometrickou charakteristikou a biometrickou šablonou.

Lze ještě doplnit, že biometrické systémy jsou úzce spojeny s konkrétní osobou, jelikož jsou založeny na využívání určité jedinečné vlastnosti jednotlivce pro účel identifikace a/nebo autentizace/ověření. V kontextu biometrické problematiky se nelze vyhnout zejména objasnění pojmů identifikace, autentizace či ověření totožnosti. Ověření totožnosti bývá často nazýváno autentizace. Nicméně používání tohoto pojmu není vhodné v kontextu ochrany osobních údajů z důvodu terminologické nepřesnosti a nedoporučuje se. Nelze totiž odvodit funkčnost, na kterou autentizace odkazuje. Pokud jde o identifikaci a ověření, jak uvádí Kindt (2013, str. 36-39), jedná se o dvě odlišné funkcionality, přičemž jejich rozlišení je klíčové a má velký význam pro porozumění biometrickým systémům. Účelem procesu ověření není určit identitu jednotlivce, ale pouze ji ověřit. Proces srovnávání v tomto případě označován jako shoda jednoho k jednomu. Biometrický vzorek jedince je porovnán pouze s biometrickými informacemi obsaženými v jednom zařízení, např. čipové kartě, v pasu nebo v jediné databázi. Až do zavedení pojmu biometrická data v rámci právních předpisů o ochraně údajů nebylo důvodné rozlišovat obecný význam identifikace od jejího specifického významu v biometrickém kontextu. Přijetím nového rámce na ochranu údajů taková potřeba vznikla. Identifikace v kontextu ochrany údajů je širší než biometrická identifikace, která spočívá v konkrétním ověření identity.

3.5 Výhody, nevýhody a rizika biometrických systémů

Biometrické systémy dosud nebyly v ČR předmětem systematického odborného zájmu ani veřejné diskuse, pokud jde o jejich dopad na ochranu osobních údajů a soukromí. Jako i v případě jiných technologií, začaly být fakticky používány, aniž by byly řešeny právní a etické důsledky. Pokud se v ČR objevují informace o biometrických technologiích, jedná se často o informace odborníků firem dodávajících biometrické systémy. Vesměs se neuvádí žádná

negativa biometrických systémů s výjimkou toho, že běžně používaná biometrika neposkytuje jistotu jednoznačné identifikace. Ovšem znalost výhod a nevýhod používání biometrických systémů je při jejich používání velmi důležitá.

Právě na úrovni pracovní skupiny WP 29, kde se problematika biometrických systémů stala předmětem intenzivnějšího zájmu přibližně od roku 2000, byla nejvíce rozpracována problematika výhod a nevýhod používání biometrických systémů. Jako hlavní pozitiva používání biometriky se uvádí:

- Efektivní prokazování skutečné identity uživatelů, identita se dokazuje s velkou mírou pravděpodobnosti;
- poskytnutí většího komfortu fyzické osobě, která tak identifikátor nemůže zapomenout, jako tomu může být u hesla, nelze ho ztratit a zcizit;
- osobní údaje lze velmi obtížně padělat nebo falšovat;
- po přihlášení lze osobu propojit s její další aktivitou, takže v případě narušení bezpečnosti lze velmi rychle identifikovat odpovědnou osobu v rámci firmy.

Biometrické systémy jsou ovšem spojeny i s řadou negativ, které nemusí být na první pohled zřejmé. Od počátku zavádění biometrických systémů pracovní skupina WP 29 upozorňovala, že biometrické systémy mohou vyvolávat velké obavy v řadě oblastí včetně soukromí a ochrany údajů. Biometrické údaje představují riziko v tom, že jsou založeny na vztahu mezi tělem a identitou, jelikož zajišťují, že jsou znaky lidského těla strojově čitelné a mohou být dále použity. Rizika, která představuji biometrické systémy, vyplývají z jejich samotné povahy. K nim patří množnost skrytého shromažďování, uchovávání a zpracování údajů, jakož i shromažďování materiálů s velmi citlivými informacemi, které mohou narušovat nejintimnější prostor jednotlivce. Jak uvádí (např. Matejka et al., 2018, str. 124) využívání biometrických údajů může mít rovněž významné dopady zejména v lidskoprávní či ústavněprávní rovině, typicky pak v oblasti lidské důstojnosti, tedy základního práva, k jehož naplnění prakticky téměř všechna ostatní lidská práva přímo či nepřímo směřují; uvedené je patrné zejména u zranitelných osob, jako jsou malé děti, starší osoby a osoby, které nejsou s to provést úplnou (tj. práv ně bezvadnou) registraci. Jak rozvoj stávajících systémů, tak nové systémy, tedy vyvolávají řadu obav.

Lze shrnout následující rizika biometrických údajů:

- Biometrické technologie nemohou zajistit úplnou přesnost, vždy existuje riziko vplývající z nesprávné identifikace. To může být způsobeno např. rozdíly v prostředí při pořizování údajů (osvětlení, teplota atd.) či rozdíly v použitém zařízení (kamery, skenovací zařízení atd.). Nejčastěji používanou metodou k hodnocení výkonnosti biometriky je ukazatel chybného přijetí a ukazatel chybného odmítnutí. Falešně pozitivní i falešně negativní výsledky mohou mít za následek rozhodnutí, která se dotýkají práv jednotlivce.
- Existují potenciální diskriminační důsledky pro osoby, které systém odmítne, nebo které nemohou biometrický údaj z nějakých důvodů poskytnout.
- Přímé spojení s fyzickou osobou má řadu stinných stránek v tom, že se dotýká osobních údajů a soukromí. Jedná se o konec anonymity a nesledovaného pohybu fyzických osob. To se týká např. rozpoznávání obličeje, kde lze biometrické údaje snadno získat.
- Permanentní sběr a uchovávání dat o všech uživatelích je v občanech schopné vyvolat nejasný pocit neklidu a ohrožení způsobené neustálým sledováním. Dopad na soukromí se zvyšuje s rostoucím zaváděním technologií.

- Krádež identity na základě použití zfalšovaných nebo odcizených zdrojů biometrických údajů může vést k vážným škodám. Na rozdíl od jiných identifikačních systémů nelze jednotlivci poskytnout novou identifikaci, pokud dojde k jejímu narušení.
- Některé biometrické údaje mohou odhalovat fyzické údaje o jednotlivci, které nezamýšlel poskytnout.
- Mnoho biometrických technologií umožňuje automatické sledování osob nebo vytváření jejich profilů. Nové biometrické systémy umožňují shromažďovat údaje z určité vzdálenosti nebo v pohybu, aniž by byla nutná spolupráce nebo činnost ze strany jednotlivce. Skryté techniky umožňují identifikaci jednotlivců bez jejich vědomí, což má za následek vážné ohrožení soukromí a postupnou ztrátu kontroly nad osobními údaji.
- Skryté techniky mohou tajně shromažďovat informace o emocionálním stavu nebo tělesných znacích a poskytovat zdravotní údaje, což vede k nepřiměřenému zpracování údajů o zpracování citlivých údajů. Tyto údaje mohou být použity k diskriminaci, stigmatizaci nebo konfrontaci.
- Biometrické technologie, přes jejich stále větší dostupnost (technickou i finanční), nejsou plnou náhradou jiných bezpečnostních řešení a samy o sobě nezajišťují větší bezpečnost. Lze to vyjádřit tak, že používání biometrických prvků samo o sobě nezajišťuje větší bezpečnost. Čím vyšší je plánovaná úroveň bezpečnosti, tím méně budou samotné biometrické údaje schopny dosáhnout tohoto cíle.
- Problematické je také to, že mnoho biometrických údajů lze shromažďovat bez vědomí dotčené osoby. V tomto ohledu by použití biometrických údajů mělo být vyhrazeno pro závažné bezpečnostní účely, nikoliv pro standardní situace pohybu ve veřejném prostoru.
- Od doby, kdy se biometrické technologie a systémy začaly používat, představovalo vážnou hrozbu využití k jiným účelům. Vyšší technický potenciál nových počítačových systémů zvyšuje riziko toho, že údaje budou použity v rozporu se svým původním účelem.
- Upozorňuje se na rizika spojená s používáním biometrických údajů pro účely identifikace ve velkých centrálních databázích. Centrální uchovávání biometrických údajů zvyšuje riziko používání biometrických údajů, které mohou být používány jako klíč k propojování více databází.
- Biometrické systémy často obsahují více informací, než je pro funkce porovnávání zapotřebí. To znamená zvýšené riziko pro osobní údaje.

Nadto je třeba zdůraznit, že rozšiřování používání biometrických údajů může vést k tomu, že veřejnost může přestat být citlivá na účinky, které zpracování údajů může mít pro denní život. To platí obzvláště v případě dětí. Např. použití biometriky ve školních knihovnách může způsobit, že děti si budou méně vědomi rizik, které je mohou ovlivňovat v dalším životě. Tato obava je opodstatněná a platí i obecně ve vztahu k používání informačních technologií, zejména pokud jde o mladší generaci a děti.

3.6 Aplikace obecného nařízení na oblast biometrických údajů

Zatímco v předchozí části byl objasněn vývoj, současný status a rizika biometrických osobních údajů, nyní je třeba položit si otázku, jak přistupovat k biometrickým údajům z pohledu obecného nařízení. Obecně platí, že v případě biometriky, biometrických systémů a biometrických technologií je po účinnosti obecného nařízení třeba nově posoudit či zkontrolovat soulad s obecným nařízením. Konkrétně se jedná o posouzení souladu s obecnými principy ochrany dat a implementaci nových institutů obecného nařízení. Platí, že vždy je nutné

brát v úvahu konkrétní povahu biometrických dat, které jsou předmětem zpracovávání. Dále je třeba zdůraznit, že biometrické údaje jsou nově zařazeny do zvláštní kategorie osobních údajů, pro kterou je stanoven přísnější režim zacházení. Vychází se přitom z toho, že tyto údaje mají citlivou povahu a jejich zpracování je spojeno s riziky, takže vyžadují vyšší stupeň ochrany než běžné údaje. Jejich zpracování se zakazuje podle čl. 9 odst. 1 obecného nařízení, pokud není na místě některá z výjimek podle čl. 9 odst. 2. To vede k závěru, že vždy je nutné nejprve zvážit, zda je skutečně nezbytné použít biometrickou technologii a zpracovávat biometrické údaje. Takové zvážení bude obzvlášť na místě, pokud se bude jednat o některou ze skupin, které obecné nařízení považuje za zranitelné, např. děti a zaměstnanci.

Obecně tedy platí, že při zpracování biometrických údajů je třeba vždy nejprve zvážit, zda je jejich zpracování skutečně nezbytné. Pokud by tomu tak nebylo, je třeba dát přednost jiné alternativě. Zdůvodnění, že použití biometrických údajů je pohodlné, nelze považovat za dostatečné. Dále je potřebné respektovat veškeré obecné principy ochrany dat. K těmto principům patří především zákonnost, korektnost a transparentnost, dále účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost a odpovědnost správce.

Zákonnost

Zpracování biometrických dat bude považováno za zákonné jednak, pokud vyhoví některé z deseti podmínek uvedených v čl. 9 odst. 1 obecného nařízení, tj.

(1) subjekt údajů udělil výslovný souhlas;
(2) zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany;
(3) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
(4) zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
(5) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
(6) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů;
(7) zpracování je nezbytné z důvodu významného veřejného zájmu;
(8) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.;
(9) zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků;
(10) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

a dále pokud probíhá na základě některého z šesti právních důvodů zpracování uvedených v čl. 6 nařízení

(1) souhlas subjektu údajů, smlouva, jejíž stranou je subjekt údajů;
(2) splnění právní povinnost správce;
(3) ochrana životně důležitých zájmů subjektu údajů nebo jiné osoby;
(4) úkol prováděný ve veřejném zájmu;

(5) úkol prováděný při výkonu veřejné moci;
(6) oprávněné zájmy správce nebo třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů.

S ohledem na citlivý charakter zpracování nemohou být podmínky a právní důvody zpracování vykládány extenzivně. Právní důvody zpracování je vždy třeba pečlivě zvažovat. Obecně platí, že obecné nařízení v tomto ohledu zúžilo rozsah právních důvodů zpracování biometrických údajů, když je zařadilo do zvláštní kategorie osobních údajů.

Korektnost

Zpracování biometrických dat a konkrétně jejich shromažďování by se mělo uskutečnit korektním způsobem. Správce by měl postupovat v souladu s právní úpravou a měl by informovat subjekt údajů o zpracování údajů v souladu s informační povinností podle nařízení. Je třeba se vyhnout systémům, které shromažďují biometrická data bez vědomí subjektu údajů. V tomto ohledu představují větší rizika např. biometrické systémy založené na vzdáleném rozpoznávání obličeje, shromažďování otisku prstů či nahrávání.

Transparentnost

Transparentnost navozuje důvěru občanů vůči postupům, které se dotýkají jejich dat tím, že jim umožní těmto postupům porozumět a v případě nutnosti vznést námitku. Souvisí s ostatními principy a doplňuje je. Vede k tomu, že by měly být vytvářeny a podporovány biometrické systémy, které jsou vytvářeny způsobem přátelským ochraně dat, měla by se minimalizovat rizika a bránit zneužití biometrických dat. Zdůrazňuje se podpora používání technologií zvyšujících soukromí, tj. tzv. PETS – *private enhancing technologies (Guidelines on Transparency under Regulation 2016/679*).

Princip účelového omezení

Osobní data musí být shromažďována pro konkrétní, výslovné a legitimní účely a nesmí být dále zpracovávána způsobem, který je s těmito účely neslučitelný. Respektování tohoto principu znamená nejprve jasné určení účelu, pro který byla biometrická data shromážděna a zpracována. Dále je třeba posoudit, zda by zamýšleného účelu nemohlo být dosaženo méně narušujícím způsobem s použitím principu proporcionality a při zohlednění rizik pro ochranu základních práv a svobod jednotlivce.

Pokud jde o účel kontroly přístupu do objektu, WP 29 zastává názor, že biometrické systémy vztahující se k fyzikálním vlastnostem, které nenechávají stopy (např. tvar ruky, ale ne prsty), nebo biometrické systémy vztahující se k fyzikálním vlastnostem, které nechávají stopy, ale nepoužívají memorizaci dat ve vlastnictví někoho jiného než dotčeného jednotlivce (jinými slovy, data nejsou uložena do paměti kontrolního přístupového zařízení nebo centrální databáze), vytváří méně rizik pro ochranu základních práv a svobod jednotlivce. Některé dozorové úřady zohlednily tento názor a konstatovaly, že biometrika by přednostně neměla být uložena v databázích, ale spíše v objektu výlučně dostupném uživateli jako je mikročipová karta, mobilní telefon nebo bankovní karta. Jinými slovy, aplikace ověření, které může být provedeno bez centrálního uložení biometrických dat, by neměla být prováděna s použitím nikoliv nezbytné identifikační techniky. Proto by mělo být pečlivě zvažováno použití aplikací založených na šablonách digitálních otisků prstů v terminálu nebo v centrální databázi. Zavedení takového typu zpracování by mělo být považováno za zpracování, které představuje riziko *per se*.

Zákaz zpracování pro jiný účel

Obecné nařízení zakazuje další zpracování, které by bylo neslučitelné s účelem, pro který byla data shromažďována. Například, pokud jsou biometrická data zpracovávána pro účel kontroly přístupu, použití takových dat k hodnocení emocionálního stavu zaměstnance nebo dohledu na pracovišti by nebylo slučitelné s původním účelem shromažďování. Musí být proto přijata veškerá opatření, aby se zabránilo takovému opakovanému použití dat. Obecné nařízení stanoví v čl.5 odst. 1 písm. b) jasné výjimky ze zákazu dalšího zpracování pro neslučitelné účely.

Je obecně přijímáno, že riziko opětného použití biometrických dat získaných z fyzikálních stop nevědomě zanechaných jednotlivcem (např. otisky prstů) pro neslučitelné účely je relativně nízké, pokud data nejsou uchovávána v centralizovaných databázích, ale má je v držení subjekt údajů a nejsou přístupná třetí osobě. Jak uvádí (např. Krausová, 2018, str. 163). Centralizované uchování biometrických údajů také zvyšuje riziko použití biometrických údajů jako klíče ke spojení různých databází, které by mohly vést k vytvoření podrobných profilů zvyků jednotlivce jak ve veřejném, tak soukromém sektoru. Navíc, otázka slučitelných účelů vznáší otázku interoperability různých systémů užívajících biometriku. Nezbytná standardizace pro interoperabilitu by mohla vést k většímu spojení mezi databázemi.

Minimalizace údajů

Při zpracování biometrických údajů by měl být důsledně uplatňován princip minimalizace údajů. Specifický problém může vzniknout, pokud biometrická data obsahují více informací, než je nezbytné pro funkci identifikace. Proto by biometrická šablona měla být technicky vytvořena tak, aby zabránila zpracování dat, která nejsou nezbytná. Data, která nejsou nezbytná, by měla být zničena.

Omezení uložení

Data by měla být uložena pouze po dobu do naplnění účelu, pro který byly osobní údaje shromažďovány. Po uplynutí této doby by měla být automaticky vymazána. Subjekt údajů by měl být informován o tom, jak dlouho budou data uchovávána.

Integrita a důvěrnost

Správce musí přijmout veškerá vhodná technická a organizační opatření k ochraně osobních dat proti náhodnému nebo nezákonnému zničení, náhodné ztrátě, změně, neoprávněnému zveřejnění nebo přístupu, konkrétně pokud zpracování zahrnuje přenos biometrických dat přes síť. Musí být přijata bezpečnostní opatření, pokud jsou zpracovávána biometrická data zpracovávána, zejména, pokud správce přenáší data přes internet. Bezpečnostní opatření mohou zahrnovat např. šifrování šablon a ochranu šifrovacích klíčů kromě kontroly přístupu a ochrany, která učiní skutečně nemožným rekonstruovat originální data z šablony. Nezbytná bezpečnostní opatření by měla být zavedena od počátku zpracování, a zvláště během období registrace, kde jsou biometrická data transformována do šablony nebo obrázku. Správci by si měli uvědomit, že jakákoliv ztráta biometrických údajů způsobí subjektům údajů nenahraditelnou škodu.

Odpovědnost správce

Obecné nařízení výslovně stanoví, že správce odpovídá za dodržení zásad zpracování osobních údajů a za to, že je schopen dodržení souladu doložit. K opatřením, kterými může správce doložit, že věnoval dostatečnou pozornost povinnostem stanoveným v obecném nařízení, patří např. záznamy o činnostech zpracování, posouzení vlivu nebo kodex chování.

Práva subjektu údajů

K těmto právům patří transparentnost, právo na přístup k osobním údajům, právo na výmaz, právo vznést námitku, právo nebýt předmětem automatizovaného rozhodování včetně profilování. Konkrétně k tomuto právu lze uvést, že omyly vyskytující se uvnitř biometrického systému mohou mít závažné důsledky pro jednotlivce, např. falešné odmítnutí oprávněné osoby a přijetí neoprávněné osoby může způsobit vážné problémy na mnoha různých úrovních. Použití biometrických údajů by mělo snížit rizika takových omylů, může však vytvořit iluzi, že identifikace nebo verifikace subjektu údajů je vždy správná. Subjekt údajů může shledat obtížným nebo nemožným prokázat opak. Například systém může chybně identifikovat subjekt údajů jako někoho, komu není umožněno nastoupit do letadla nebo vstoupit do konkrétní země a nebude mít možnosti, jak takový problém řešit. V takových případech by jakékoliv rozhodnutí, které právně ovlivňuje jednotlivce, mělo být přijato po opětném potvrzení výsledku automatizovaného zpracování v souladu s obecným nařízením.

Posouzení vlivu na ochranu osobních údajů

Jak již bylo zmíněno, je třeba podporovat použití biometrických systémů, které nezanechávají stopy v zařízení přístupového terminálu ani v centrální databázi. Pokud však mají být takové systémy používány a existuje riziko opětného použití pro odlišné účely či konkrétní nebezpečí v případě neoprávněného přístupu, mělo by být provedeno posouzení vlivu na ochranu osobních podle čl. 35 obecného nařízení, protože tento druh zpracování pravděpodobně představuje konkrétní rizika pro práva a svobody subjektu údajů. Před tím než budou taková opatření zavedena by měl být také konzultován vnitrostátní dozorový úřad.

Kodexy chování

Zdůrazňuje se důležitost kodexů chování, které mohou přispět ke správné implementaci principů ochrany dat v jednotlivých specifických oblastech. Kodexy chování jsou rovněž jedním z prvků, jimiž správce může prokázat svou odpovědnost.

4 Biometrika a její využívání z pohledu české veřejnosti – statistický průzkum, jeho metodologie a závěry

4.1 Metodologie průzkumu

Centrum pro výzkum veřejného mínění Sociologického ústavu Akademie věd ČR (CVVM) realizovalo v září 2018 z podnětu i objednávky řešitelského týmu shora uvedeného projektu (GA ČR č. 16-26910S) výzkum pracovně nazvaný Biometrika a její využívání z pohledu české veřejnosti. Samotný průzkum zpracovala pracovnice Iva Štohanzlová a probíhal ve dnech 8.-20. září 2018 a metodologicky byl realizován formou osobních rozhovorů tazatele s respondentem, a to na vzorku obyvatelstva ČR ve věku od 15 let; počet oslovených byl 1230, z toho dotázaných bylo 1037. Pro formu tohoto rozhovoru byla zvolena metoda kombinace dotazování PAPI[1] (71 %) a CAPI[2] (29 %); jako výzkumný nástroj pak standardizovaný dotazník s počtem 60 proměnných. Tomuto reprezentativnímu výběrovému souboru byly

[1] Z hlediska kvalitativních standardů využívaného nástroje představuje PAPI dotazování pomocí papírových dotazníků (z ang. "*Paper Aided Personal Interview*")

[2] Kvalitativní standard CAPI (z. ang. „*Computer Assisted Personal Interviewing")* představuje technika dotazování, kdy v rámci osobního kontaktu pokládá tazatel respondentovi otázky a získané odpovědi značí do elektronického dotazníku, zobrazeného na přenosném multimediálním zařízení (tablet, notebook, apod.).

položeny otázky zaměřené na problematiku tzv. biometriky a jejího rychle se rozšiřujícího využívání v různých oblastech, zejména v informačních technologiích.

Šetření se konkrétně zabývalo tím, zda a nakolik má česká veřejnost povědomí o tom, co jsou biometrické údaje, zda je informována o tom, že tyto údaje jsou často automaticky a nezávisle na souhlasu fyzických osob snímány, registrovány, zpracovávány a využívány různými technologiemi a aplikacemi, a zda lidé v souvislosti s využíváním biometrických údajů preferují spíše uživatelský komfort, nebo zda upřednostňují ochranu svého soukromí, jež technologie založené na biometrii nepochybně narušují. Na závěr byly položeny otázky týkající se jevů souvisejících s monitorováním a využíváním biometrických údajů v běžném životě.

4.2 Celkové zaměření otázek výzkumu a dílčí statistické výsledky

Všem respondentům byla nejprve položeny obecné otázky zaměřené na míru jejich povědomí o biometrických údajích, resp. konkrétně zda tento pojem už slyšeli a zda vědí, co znamená. Série dalších otázek zjišťovala, zda lidé vědí, že moderní technologie umožňují sbírat, zpracovávat a různým způsobem využívat velké množství dat o každém člověku, a to jak s jeho vědomím a souhlasem, tak i zcela nezávisle na něm. Následně byly respondentům položeny otázky zjišťující, zda preferují při využívání různých technologií spíše uživatelský komfort i za cenu toho, že k tomu jsou využívány jejich osobní údaje, nebo zda upřednostňují ochranu svého soukromí i za cenu určitého uživatelského nepohodlí, případně omezení některých služeb uzpůsobených individuálnímu uživateli na míru.

Další otázky se podrobněji zaměřily na některé běžné situace, které nastávají v souvislosti s technologiemi využívajícími shromažďování dat. Jednalo se celkem o devět dvojic výroků, kdy respondenti odpovídali pomocí pětibodové škály, přičemž z odpovědí respondentů vyplynuly níže uvedené převažující odpovědi:

- při nákupu přes internet zákazníkům vadí shromažďování údajů o jejich chování;
- respondentům dále vadí, když se internetové stránky osobně přizpůsobují podle jejich přístupu;
- při posuzování toho, zda respondenti dávají přednost přístupovým heslům a ověřovacím kódům namísto automatické identifikace na základě biometrických údajů, se názory rozložily téměř vyrovnaně; k výroku upřednostňujícímu automatickou identifikaci na základě biometriky se přiklánělo 29 % respondentů, zatímco k výroku preferujícímu přístupová hesla a ověřovací kódy se přiklánělo 31 % dotázaných;
- v rámci otázky, zda se zákazníci u nových služeb zajímají o to, jaké údaje se o nich budou sbírat, převažoval jednoznačně příklon k výroku, že se o to vždy zajímají (42 %);
- při vyhledávání zboží a služeb na internetu respondentům vadí nebo nevadí uvádět osobní údaje, které mohou vest bezprostředně k identifikaci (zde byly názory rozloženy rovnoměrně);
- u dvojice možných odpovědí, zda nevadí nebo vadí při nakupování zboží a služeb přes internet uvádět osobní údaje, podle kterých je lze dále identifikovat, se lidé častěji přiklánějí k výroku, že to vadí (36 %);
- při odpovědi, zda uživatel může nebo nemůže ovlivnit to, jak aplikace nebo webové stránky, které používá, sbírají údaje o jeho chování a preferencích, mírně převážila skeptická varianta, že to ovlivnit nelze;
- v případě dvojice výroků týkající se toho, zda by technologie založené na využívání biometrických údajů a údajů o chování jednotlivce v soukromé a komerční sféře měly být zakázány, nebo povoleny (z důvodu, že umožňují zlepšovat nabídku služeb), se veřejnost poměrně jednoznačně přiklonila na stranu zákazu (dvě pětiny dotázaných);

- poslední dvojice výroků, jež se týkala možnosti zabezpečení před případným únikem a zneužitím údajů o člověku a jeho chování uložených na internetu a v elektronických zařízeních, se česká veřejnost jednoznačně přiklonila ke skeptické variantě, že to zabezpečit nelze (46 %).

Z výsledků dále vyplývá, že o biometrických údajích alespoň slyšelo přibližně sedm z deseti lidí ve věku od 15 let (71 %) a že téměř polovina (47 %) podle svého vyjádření má alespoň hrubou představu o tom, co to jsou biometrické údaje. Podrobnější analýza ukázala, že o něco častěji povědomí o biometrických údajích deklarují muži oproti ženám, lidé ze skupiny od 30 do 44 let, lidé s nejvyšším stupněm dokončeného vzdělání, s příznivým hodnocením životní úrovně vlastní domácnosti a uživatelé internetu. Vyšší povědomí o biometrických údajích mají také lidé ve velkých městech s populací nad 80 tisíc a v Praze. Z hlediska zaměstnání vyšší povědomí o biometrických údajích vykazují vysoce kvalifikovaní odborní nebo vedoucí pracovníci.

Z pohledu průzkumem testované znalosti české veřejnosti dále plyne, že 70 % lidí podle vlastního vyjádření ví, že moderní technologie umožňují takové zpracování, 30 % to neví. Přitom podíl těch, kdo takovou vědomost měli, v podstatě odpovídal povědomí o tom, co jsou biometrické údaje. Ani sociodemografické rozdíly v rozložení odpovědí na danou otázku se příliš nelišily od rozdílů zaznamenaných v případě úvodních otázek zkoumajících povědomí o pojmu biometrické údaje.

Celkově vzato tak výsledky ukazují, že v české populaci starší 15 let v poměru tři ku jednomu převažují lidé, kteří upřednostňují ochranu svého osobního soukromí před maximálním uživatelským pohodlím, jež mohou nabízet moderní technologie s využitím osobních údajů. Názor, že je důležité, aby používané technologie poskytovaly maximální uživatelské pohodlí a služby přizpůsobené na míru i za cenu využití dostupných informací o své osobě, zastává přibližně pětina (21 %) oslovených, zatímco podíl těch, kdo preferují ochranu svého soukromí i za cenu nižšího pohodlí a omezení osobně zaměřených služeb, převyšuje tři pětiny (63 %). Přibližně šestina (16 %) dotázaných se nedokázala rozhodnout. Statisticky významný rozdíl v preferencích uživatelského komfortu na úkor podílu nerozhodnutých se objevuje mezi Čechami a Moravou, když v Čechách uživatelský komfort preferovalo 24 % dotázaných při 13 % nerozhodnutých, zatímco na Moravě to bylo jen 16 % při 20 % nerozhodnutých.

4.3 Celkové shrnutí výzkumu „Biometrika a její využívání z pohledu české veřejnosti“

Závěrem lze shrnout, že se jednalo o první a exkluzivní průzkum názorů veřejnosti v České republice na biometriku zaměřený na povědomí o biometrických údajích, povědomí o zpracování dat prostřednictvím moderních technologií vůbec a na preferenci respondentů v případě střetu mezi ochranou soukromí a uživatelským komfortem. Přináší informace o tom, že převažující část veřejnosti má povědomí o tom, co jsou biometrické technologie a moderní technologie vůbec a zachycuje převažující názor veřejnosti na preferenci ochrany soukromí na úkor uživatelského komfortu.

Samotný výzkum poukázal na širokou škálu sociodemografických faktorů, rovněž však faktorů geografických a dalších skutečností, které umožňují postoje veřejnosti citlivěji diferencovat. Za důležité lze považovat údaje o vysokém počtu nerozhodných odpovědí. Relevance uskutečněného výzkumu je dána především tím, že byly zkoumány názory fyzických osob, k jejichž ochraně jsou určeny současné předpisy v této oblasti, přičemž za klíčové (shrnující) poznatky výzkumu lze označit především níže uvedené skutečnosti:

- biometrických údajích alespoň slyšelo přibližně sedm z deseti (71 %) lidí ve věku od 15 let a téměř polovina (47 %) podle svého vyjádření má alespoň hrubou představu o tom, co jsou biometrické údaje.
- 70 % lidí podle vlastního vyjádření ví, že moderní technologie umožňují sbírat, zpracovávat a různým způsobem využívat data o každém člověku, a to i bez jeho vědomí a souhlasu.
- V české populaci v poměru tři ku jednomu převažují lidí, kteří upřednostňují ochranu svého osobního soukromí před maximálním uživatelským pohodlím, jež mohou nabízet moderní technologie s využitém osobních údajů.

Poměrně zajímavý rozdíl se objevil z hlediska náboženské orientace mezi věřícími katolíky, kteří méně často preferují uživatelský komfort (9 %) a naopak ve zvýšené míře preferují ochranu soukromí (72 %), zatímco u lidí bez vyznání se objevuje zvýšený podíl preferujících uživatelský komfort (25 %) o něco méně často, než je průměr. Z hlediska pravolevé politické orientace se podobně jako katolíci vyjadřovali lidé, kteří sami sebe řadí do levého středu. Tyto rozdíly CVVM při hodnocení odpovědí respondentů interpretoval tak, že jedním z diferencujících faktorů pro postoj k dané otázce může být hodnotový postoj na ose konzervatismus – liberalismus, přičemž konzervativní postoje se mohou spojovat s tendencí preferovat vice ochranu soukromí a odmítat moderní technologie založené na využívání osobních dat, zatímco liberální postoje inklinují ve zvýšené míře k přijímání nových technologií s optimistickým výhledem, že budou přinášet pozitivní věci a nebude docházet ke zneužívání nebo negativním dopadům mj. na oblast soukromí.

Realizovaný výzkum tak nepřímo potvrdil aktuálnost a potřebnost současného zvýšeného standardu ochrany osobních údajů a soukromí fyzických osob, jakož i potřebu dalšího vzdělávání veřejnosti v této oblasti.

5 Závěr

Z výše uvedeného textu vyplývají obecné závěry pro zacházení s biometrickými údaji, které lze doporučit:

- Biometrické údaje je třeba chápat v kontextu vývoje biometrických technologií. Teprve s jejich rozvojem došlo k zařazení biometrických údajů mezi osobní údaje, a ještě později převážilo pojetí, že jde o citlivé údaje.
- Biometrické údaje mají zvláštní povahu, protože se vztahují k behaviorálním a fyziologickým vlastnostem jednotlivců a umožňují jejich jedinečnou identifikaci.
- To představuje výhodu, ale také značná rizika, která vyplývají ze samotné povahy biometrických údajů. Tyto údaje mohou být zneužity k diskriminaci, stigmatizaci nebo konfrontaci. Na rozdíl od jiných identifikačních údajů nelze jednotlivci poskytnout novou identifikaci, pokud dojde k jejímu narušení.
- Obecné nařízení přineslo významné změny ve vztahu k biometrickým údajům. Biometrické údaje jsou řazeny mezi osobní údaje, které jsou svou povahou zvláště citlivé z hlediska základních práv a svobod a vyžadují zvláštní ochranu při jejich zpracování.
- Nově je posuzování biometrických údajů založeno na principu technologické neutrality, což prakticky znamená, že se opouští rozlišování založené na přímé a nepřímé identifikaci subjektů údajů a uplatní se tak širší pojetí biometrických údajů.
- Biometrické údaje byly nově definovány a zařazeny do zvláštní kategorie osobních údajů. Jejich zpracování je zakázáno, pokud neexistuje výjimka pro jejich zpracování.

- Při úvahách o zpracování biometrických údajů je vždy třeba nejprve zvážit, zda je zpracování osobních údajů s pomocí biometrických technologií skutečně nezbytné a zda nepřichází v úvahu použití jiných řešení, které by biometrické údaje nepoužívaly.
- Pokud nikoliv, lze alespoň doporučit, aby biometrické údaje nebyly uloženy mimo sféru dispozice fyzické osoby. Ověření, které může být provedeno bez centrálního uložení biometrických dat, by nemělo být prováděno s použitím nikoliv nezbytné identifikační techniky.
- Je třeba vzít v úvahu, že velké centrální databáze jsou samy o sobě rizikem. Jejich používání musí být doprovázeno adekvátními technickými a organizačními zárukami pro ochranu osobních údajů a soukromí v souladu s obecným nařízením.
- Obecné nařízení přináší řadu nových nástrojů směřujících k ochraně osobních údajů a soukromí, které lze využít rovněž ve vztahu ke zpracování biometrických údajů. V tomto ohledu lze odkázat jak na principy, tak na nástroje obecného nařízení. Zvlášť je třeba upozornit na institut posouzení vlivu na ochranu osobních údajů, předběžné konzultace s dozorovým úřadem a kodexy chování. Biometrické údaje lze užívat pouze k účelu, který byl deklarován. Zvlášť je třeba zdůraznit princip transparentnosti, jehož součástí je informační povinnost. Platí ovšem, že by mělo dojít k celkovému Celkově by mělo být zvýšeno povědomí veřejnosti o charakteru biometrických údajů a rizicích jejich používání.
- Teprve poučený uživatel by se měl rozhodnout, zda poskytne své osobní údaje pro účely jejich zpracování v biometrických systémech, nebo zda zvolí jinou alternativu, o které byl předem informován. Mělo by být zavedeno obecné pravidlo, že fyzickým osobám, které nemohou nebo nechtějí používat biometrické údaje, bude nabídnuta alternativa v jiné formě, např. karta, jmenovka, čip.
- V některých situacích bude jediným možným právním titulem pro používání biometrických údajů souhlas, který ovšem musí být svobodný a informovaný. I v těchto případech by však měla být nabídnuta alternativa bez použití biometrických údajů.
- V kontextu biometrických údajů je třeba vždy věnovat zvláštní pozornost zranitelným kategoriím, jimiž jsou např. děti, zaměstnanci, senioři a hendikepované osoby.

Při používání biometrických údajů je třeba brát ohled na to, že zejména děti mohou ztratit citlivost ve vztahu k používání biometrických údajů, zvlášť při jejich nadměrném používání. Je skutečností, že děti si neuvědomují rizika používání biometrických údajů, a preferují jednoduchou formu ověření. V tomto ohledu je potřebné poskytovat dostatečné, transparentní a srozumitelné informace vztahující se k používání biometriky včetně případných rizik. Na tomto úkolu zásadního významu by se měla podílet jak rodina, tak vzdělávací a osvětové instituce.

Poděkování

Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-26910S s názvem *Biometrické údaje a jejich zvláštní právní ochrana* (*Biometric Data and Their Specific Legal Protection*).

Seznam použité literatury

Alexy, R. (1986). *Theorie der Grundrechte*. Berlin: Suhrkamp Verlag AG.

Güttler, V., & Matejka, J. (2016). K otázkám některých základních práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*, 155(12), 1033-1056.

Herrmann, D., Banse, C., & Federrath, H. (2013). Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security*, 39(Part A), 17-33. doi: 10.1016/j.cose.2013.03.012

Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. Netherlands: Springer. doi: 10.1007/978-94-007-7522-0

Kosař, D. (2008). Kolize základních práv v judikatuře Ústavního soudu ČR. *Jurisprudence*, 2008(3).

Krausová, A. (2018). Online Behavior Recognition: Can We Consider It Biometric Data under GDPR? *Masaryk University Journal of Law and Technology*, 12(2), 161-178. doi: 10.5817/MUJLT2018-2-3

Matejka, J. (2013). *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC.

Matejka, J., Krausová, A., & Güttler, V. (2018). Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, 9(17), 91-129. doi: 10.5817/RPT2018-1-5

Matochová, S. (2008). *Etika a právo v kontextu lékařské etiky*. Brno: Masarykova univerzita.

MEMO. (2014). Progress on EU data protection reform now irreversible following European Parliament vote. European Commission MEMO, Strasbourg, 12 March 2014. Retrieved October 25, 2019, from: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

Smejkal, V. (2017). Dynamický biometrický podpis a nařízení GDPR. *Revue pro právo a technologie*, 8(16), 89-112. doi: 10.5817/RPT2017-2-5

OECD. (2016). *OECD Employment Outlook*. Paris: OECD Publishing.

Nález ÚS. (1994). Nález Ústavního soudu Pl. ÚS 9/94. Retrieved October 25, 2019, from: http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-9-94

NPP. (2016). 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. Retrieved October 25, 2019, from: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679

SEP. (1995). 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. Retrieved October 25, 2019, from: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31995L0046

Rak, R., Matyáš, V., Říha, Z. a kolektiv. (2008). *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada.

ÚOOÚ. (2013). K principu proporcionality při zpracování osobních údajů na základě zákona o svobodném přístupu k informacím, čj. SPR-5137/12. Retrieved October 25, 2019, from: https://www.uoou.cz/k-nbsp-principu-proporcionality-pri-nbsp-zpracovani-osobnich-udaju-na-zaklade-zakona-o-nbsp-svobodnem-pristupu-k-nbsp-informacim/d-5511/p1=1099

WP29. (2003). Article 29 Data Protection Working Party: Working document on biometrics. Retrieved October 25, 2019, from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

WP29. (2007). Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. Retrieved October 25, 2019, from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

WP29. (2011). Article 29 Data Protection Working Party: Advice paper on special categories of data ("sensitive data"). Retrieved October 25, 2019, from: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

WP29. (2012). Article 29 Data Protection Working Party: Opinion Nr. 3/2012 on Developments in Biometric Technologies. Retrieved October 25, 2019, from: https://www.pdpjournals.com/docs/87998.pdf

The article has been reviewed. | **Received:** 25 September 2019 | **Accepted:** 9 November 2019

Academic Editor: Zdenek Smutny