

<https://doi.org/10.5817/RPT2018-1-5>

BIOMETRICKÉ ÚDAJE A JEJICH PRÁVNÍ REŽIM¹

JÁN MATEJKA², ALŽBĚTA KRAUSOVÁ³, VOJEN GÜTTLER⁴

ABSTRAKT

Jednou z nejtypičtějších překážek bránících dalšímu rozvoji užívání moderních ICT nástrojů v platné právní úpravě (legislativě) bývá zpravidla absence efektivních, důkazně i bezpečnostně spolehlivých nástrojů umožňující identifikaci či autentizaci uživatelů předmětných služeb informační společnosti. Tyto verifikační nástroje mají zpravidla podobu buď toho, co má osoba u sebe (např. USB token), nebo toho, co zná (typicky přihlašovací údaje), případně toho, čím daná osoba je (tj. biometrická charakteristika); poslední z uvedených prostředků nabývá v moderních technologiích stále více na významu, a to zejména pro svou praktičnost (dostupnost a neměnitelnost), nicméně zároveň však představuje zvláštní a privilegovanou kategorii citlivých osobních údajů, jejich použití je silně limitováno předpisy veřejného práva. Existuje zde tak určitě konflikt mezi veřejným zájmem (či i zájmem jednotlivců) na práci s biometrickými údaji na straně jedné a řadou dalších práv, včetně práva na ochranu soukromého života, na straně druhé. Cílem tohoto článku je tak zmapovat současný český právní rámec regulující využití a zpracovávání biometrických údajů pro různé účely; v souvislosti s tím se bude rovněž zabývat možným využitím biometrických

¹ 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).

² JUDr. Ján Matejka, Ph.D., Ústav státu a práva Akademie věd České republiky. Kontaktní e-mail: jan.matejka@ilaw.cas.cz

³ Mgr. Alžběta Krausová, LL.M., Ústav státu a práva Akademie věd České republiky. Kontaktní e-mail: alzbeta.krausova@ilaw.cas.cz

⁴ JUDr. Vojen Güttler, Ústav státu a práva Akademie věd České republiky. Kontaktní e-mail: vojen.guttler@ilaw.cas.cz

prostředků, a to jak v oblasti práva veřejného, tak i soukromého. Tento příspěvek se tak bude zabývat popisem jednotlivých právních režimů zpracování této privilegované kategorie dat, přičemž zároveň se snaží najít či blíže identifikovat existující právní mantinely a konflikty souvisejících režimů zpracování vyplývající z české i evropské právní úpravy.

KLÍČOVÁ SLOVA

Biometrika, biometrický údaj, osobní údaj, citlivý osobní údaj, soukromí, identifikace, verifikace, ochrana osobnosti, GDPR, biometrický podpis, cestovní doklady

ABSTRACT

One of the most typical obstacles that impede further development in use of modern ICT tools in law is absence of efficient and reliable instruments enabling identification or authentication of users of respective information society services. These verification instruments usually have a form of something that a person possesses (for instance USB token), or something that a person knows (typically login data), or something that a person is (i.e. biometric characteristic). The last of the mentioned instruments is becoming increasingly important in modern technologies due to its practicality (availability and permanence). However, biometric data also represent a special and privileged category of personal data and its use is strongly limited by public laws. There is certainly a conflict between a public interest (or even an interest of individuals) on processing biometric data on one hand and a number of other rights, including the right to privacy, on the other hand. The aim of this paper is to provide an overview of the current Czech legislation that regulates processing biometric data for various purposes. The paper also focuses on possible use of biometric means in the area of public as well as private law. The paper describes individual legal regimes of processing this special category of data while attempting to identify exiting legal limitations as well as conflicts of related regimes of processing that stem from Czech and European laws.

KEYWORDS

Biometrics, biometric data, personal data, sensitive personal data, privacy, identification, verification, personality protection, GDPR, biometric signature, travel documents

1. ÚVOD

Biometrické údaje jsou zvláštním druhem údajů. Jedná se o informace, které vypovídají o individuálních aspektech stavby anebo fungování či chování biologického organismu. Přestože se termín biometrického údaje používá zejména v souvislosti s člověkem, české právo jej užívá i ve vztahu ke zvířatům⁵ a evropské právo například i ve vztahu k rýži.⁶ Jde ale o ojedinělé případy. Ve všech ostatních případech spojuje právo biometrický údaj s fyzickou osobou. Biometrický údaj je specifickým druhem zpravidla osobního údaje, pro jehož zpracování platí kromě obecných pravidel pro zpracování osobních údajů i další pravidla, která se liší v jednotlivých kontextech.

Přestože biometrickým údajem může obecně být jakákoliv měřitelná kategorie stavby nebo fungování biologického organismu, v právu se za biometrický údaj většinou považuje takový údaj, který umožňuje jedinečnou identifikaci fyzické osoby. Typickými biometrickými údaji jsou například zobrazení obličeje nebo daktyloskopické údaje. Právo zároveň u těchto údajů předpokládá, že musí být určitým způsobem technicky zpracovány, aby se staly biometrickými údaji. Prostá fotografie obličeje tak zpravidla

⁵ O biometrických údajích se zmiňuje zákon v souvislosti s odchylem volně žijících zvířat a jejich zpětným vypuštěním do přírody prováděným za účelem sledování stavu volně žijících zvířat. Viz § 14 odst. 6 zákona č. 246/1992 Sb., na ochranu zvířat proti týrání, v platném znění.

⁶ V souvislosti s chráněným zeměpisným označením určitého typu rýže se specifikují biometrické vlastnosti zrn této rýže, a to v kategoriích délka, šířka, tloušťka a tvar. Viz Nařízení Komise (ES) č. 205/2009 ze dne 16. března 2009, kterým se schvalují změny menšího rozsahu ve specifikaci označení zapsaného do rejstříku chráněných označení původu a chráněných zeměpisných označení (*Riso Nano Vialone Veronese* (CHZO)).

nemůže být považována za biometrický údaj,⁷ protože bez zpracování postrádá přesné informace týkající se například vzdálenosti jednotlivých klíčových bodů v obličeji nebo jejich vzájemných poměrů. Jsou to totiž právě tyto odvozené informace, které ve výsledku vytváří systém pro porovnávání jednotlivých rysů a měřených kategorií mezi originální šablonou (např. fotografií obličeje v cestovním pase) a následným měřením (kamerovým snímkem obličeje při pasové kontrole), a umožňují tak ověření identity nebo identifikaci.⁸ Právě určení a ověření identity patří k hlavním, ale nikoliv jediným účelům, ke kterým právo využívá biometrické údaje.

Pojem biometrického údaje je ale používán v různých kontextech napříč celým právním řádem, překrývá se s dalšími oblastmi práva, jako je ochrana osobnosti nebo soukromí, a v souvislosti s různými situacemi jsou osoby nuceny strpět zásah ve formě sdílení svých biometrických údajů v různé míře. Cílem tohoto článku je tak zmapovat současný český právní rámec regulující využití a zpracovávání biometrických údajů pro různé účely. V následující kapitole je nejdříve osvětleno samotné pojetí biometrie a biometrických údajů v širokém smyslu a zároveň je ilustrován přístup práva k biometrice obecně. Další kapitoly se pak věnují konkrétním právním oblastem. Nejprve je vysvětlen obecný právní rámec regulace biometrie. Následují kapitoly týkající se specifik u osobních dokladů, dalších způsobů biometrické verifikace a identifikace, využívání biometrických údajů v trestním právu a Vojenskou policií.

⁷ Odborná literatura nicméně uvádí, že i fotografie zobrazující obličej může být za určitých podmínek považována za biometrický údaj, a to s ohledem na znění vyhlášky č. 415/2006 Sb., kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu. Za biometrický údaj se považuje fotografie obličeje pořízená způsobem podle § 3. Blíže MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 s. ISBN 978-80-7357-322-5. Viz s. 94.

⁸ Ověření identity se rozumí situace, v níž systém porovnává, zda se měřené biometrické údaje osoby shodují s biometrickou šablonou, kterou předkládá na důkaz své identity. Při identifikaci systém změří biometrické údaje osoby a porovná je se svojí databází tak, aby našel shodu. Blíže např. MORDINI, Emilio, TZOVARAS, Dimitros (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. 349 s. ISBN 978-94-007-3891-1. Viz s. 8.

2. POJEM BIOMETRICKÝ ÚDAJ

Biometrický údaj je pojmem, který lze definovat jak obecně teoreticky, tak i technicky a právně. Jednotlivé definice se vždy nemusí úplně shodovat, ale v určité části se překrývají. Biometrika jako taková se „zaměřuje pouze na *‘změřitelné fyzické vlastnosti’*“⁹ žijících organismů. Tyto organismy se totiž vyznačují „*vysoce specifickými kvalitami, které jsou jedinečné a dostatečně stabilní na to, aby byly použity jako identifikátory*“.¹⁰ Současná biometrika tyto identifikátory snímá pomocí senzorů, měří elektrický signál produkováný těmito senzory a měření převádí obvykle do formy počítačového kódu, který následně využívá. Tak dochází k převodu z analogové formy informace do její digitální podoby.¹¹ Ta následně umožňuje její zpracování elektronickými informačními systémy. V současné době jsou tak za biometriku považovány zejména „*automatizované metody rozpoznávání osoby na základě jejich fyziologických nebo behaviorálních charakteristik*“.¹²

Historicky docházelo k biometrickému rozpoznávání osob vždy, nikoliv však automatizovaně. Lidé rozlišují ostatní osoby právě podle jejich vzhledu, chování, typických gest, způsobu řeči apod. Otisky rukou byly údajně používány k ověření autorství zákonů přijatých ve formě hliněných tabulek již za doby krále Chamurappiho.¹³ Automatizované metody biometrického ověření se objevily až na začátku sedmdesátých let 20. století.¹⁴ V současné době se rozšiřují stále více a biometrickou autentifikaci pomocí otisku prstu lze najít v mnoha modelech chytrých telefonů.

Biometrika se zaměřuje na identifikátory založené na biometrických rysech. S ohledem na míru jedinečnosti a stability těchto rysů se dělí do tří

⁹ MORDINI, Emilio, TZOVARAS, Dimitros (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. 349 s. ISBN 978-94-007-3891-1. Viz s. 7.

¹⁰ Tamtéž, s. 8.

¹¹ Tamtéž, s. 7.

¹² VACCA, John R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007, 625 s. ISBN 978-0-7506-7967-1. Viz s. 3.

¹³ KINDT, Els J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer, 2013, 975 s. ISBN 978-94-007-7521-3. Viz s. 15.

¹⁴ Tamtéž, s. 18.

kategorií: silné biometrické rysy (angl. *strong biometrics*), slabé biometrické rysy (angl. *weak biometrics*) a jemné biometrické rysy (angl. *soft biometrics*).¹⁵ Silná biometrika analyzuje rysy, které jsou jedinečné a stálé, jako např. otisk prstu, rohovka, nebo rozložení žil na ruce. Slabá biometrika oproti tomu využívá méně stálé a méně jedinečné rysy, které mohou podléhat změnám, jako např. chůzi, hlas nebo elektrofyziologické aktivity včetně mozkových vln. Jemná biometrika využívá obecné rysy jako pohlaví, věk, etnickou příslušnost a další informace a může zejména sloužit jako pomocný indikátor pro systémy využívající silnou nebo slabou biometriku.¹⁶

V rámci biometriky se rozvíjí ještě specifické odvětví s názvem behaviorální biometrika. Tento typ biometriky se zaměřuje výhradně na kvantifikování behaviorálních vlastností jednotlivců a vytváření jejich profilů za účelem následné identifikace. Oproti jiným formám biometriky je zvláštní v tom, že může být velmi nenápadná a sběr dat může být prováděn i bez vědomí uživatele.¹⁷ Behaviorální biometrika dokáže identifikovat osobu například na základě analýzy textu a určení autorství, zvláštních znaků vykazovaných osobou při používání počítače, nebo i na základě analýzy schopností, které člověk vykazuje při plnění určitých, zejména kognitivních úloh.¹⁸

Kromě metody rozpoznávání osob může být biometrika definována mimo jiné jako „*aplikace matematických a statistických metod za účelem popsání a analýzy údajů týkajících se změn biologických charakteristik získaných buď pozorováním, nebo pomocí experimentu*“.¹⁹ V tomto smyslu má spíš vě-

¹⁵ MORDINI, Emilio, TZOVARAS, Dimitros (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. 349 s. ISBN 978-94-007-3891-1. Viz s. 8 an.

¹⁶ Tamtéž.

¹⁷ YAMPOLSKIY, Roman V., GOVINDARAJU, Venu. Taxonomy of Behavioural Biometrics. In WNAG, Liang, GENG, Xin (eds.). *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, August 2009. doi:10.4018/978-1-60566-725-6. Dostupné z: <<https://www.igi-global.com/book/behavioral-biometrics-human-identification/99#table-of-contents>> .

¹⁸ Tamtéž.

¹⁹ LI, Ching Chun. Biometrics. In *AccessScience* [online]. 2014 [cit. 2017-10-16]. Dostupné z: <<https://doi.org/10.1036/1097-8542.083700>> .

deckou povahu a slouží k získávání informací o fungování biologického organismu a k případné diagnostice nebo predikci budoucího vývoje zdravotního stavu. V tomto pojetí souvisí s bioinformatikou, vědeckým odvětvím, které se zabývá zkoumáním zdraví a nemocí biologických systémů. K tomu využívá i tzv. biomarkerů. „*Biomarker je ‘charakteristikou, která je objektivně měřena a vyhodnocována jako indikátor normálních biologických procesů, patogenních procesů nebo farmakologických reakcí na terapeutickou intervenci’ (Biomarkers Definitions Working Group, 2001).*“²⁰ Data získaná z jednotlivých aplikací pro rozpoznávání osob mohou být rovněž podrobena analýze na výskyt biomarkerů. Například z analýzy hlasu lze u některých osob indikovat informace o možné neurodegeneraci a brzkých znacích Parkinsonovy nemoci.²¹ Určité biomarkery se na druhou stranu využívají i při monitorování za účelem autentifikace osoby.²²

Kromě výše uvedených teoretických pohledů na biometriku lze pojem biometrického údaje definovat i z čistě technického hlediska. Biometrické systémy podléhají technické standardizaci. Mezinárodní organizace pro standardizaci (ISO) dosud vydala 121 standardů pro biometriku a dalších 30 standardů je v současné době rozpracováno.²³ Tyto standardy se týkají například programovacího rozhraní, zajištění bezpečnosti, rámce pro výměnu biometrických formátů, metodologií testování, nebo jednotlivých typů

²⁰ AZUAJE, Francisco. *Bioinformatics and Biomarker Discovery. “Omic”Data Analysis for Personalized Medicine*. Chichester: John Wiley & Sons, Ltd., 2010, 230 s. ISBN 978-0-470-74460-4. Viz s. 2.

²¹ HLAVNÍČKA, Jan, ČMEJLA, Roman, TYKALOVÁ, Tereza, ŠONKA, Karel, RŮŽIČKA, Evžen, RUSZ, Jan. Automated analysis of connected speech reveals early biomarkers of Parkinson’s disease in patients with rapid eye movement sleep behaviour disorder. *Scientific Reports*, 2017, roč. 7, č. 12. doi:10.1038/s41598-017-00047-5. Dostupné z: < <https://www.nature.com/articles/s41598-017-00047-5> >.

²² JENKINS, Jeffrey, SWEET, Charles, SWEET, James, MOEL, Steven, SZU, Harold. Authentication, privacy, security can exploit brainwave by biomarker. *Proceedings Volume 9118, Independent Component Analyses, Compressive Sampling, Wavelets, Neural Net, Biosystems, and Nanoengineering XII*; 91180U (2014); doi: 10.1117/12.2051323. Dostupné z: < <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9118/1/Authentication-privacy-security-can-exploit-brainwave-by-biomarker/10.1117/12.2051323.short?SSO=1> >.

²³ Viz Standards catalogue – ISO/IEC JTC 1/SC 37 – Biometrics. In: *International Organization for Standardization* [online]. 2017 [cit. 2017-10-16]. Dostupné z: < <https://www.iso.org/committee/313770/x/catalogue/> >.

biometrických aplikací. Definice související s biometrikou jsou obsaženy ve volně dostupném standardu ISO/IEC 2382-37:2017,²⁴ který nahradil standard z roku 2012. Podle tohoto standardu je biometrickým údajem „*biometrický vzorek nebo agregace biometrických vzorků v kterékoliv fázi zpracování*“.²⁵ Biometrický vzorek je pak „*analogickou nebo digitální reprezentací biometrické charakteristiky před extrakcí biometrických prvků*“²⁶ a biometrická charakteristika je definována jako „*biologická nebo behaviorální charakteristika jednotlivce, ze které mohou být extrahovány rozlišující, opakovatelné biometrické rysy*“.²⁷ Biometrickým rysem se následně rozumí „*čísla nebo označení extrahovaná z biometrických vzorků a použítá pro srovnávání*“.²⁸ Bohužel tak zde dochází k definici kruhem. Nicméně sám tento standard stanoví, že biometrický údaj nemusí být přisuzovatelný přímo k jednotlivci. Tím pádem ale nejde o biometrický údaj v tom smyslu, v jakém ho nejčastěji chápe právo.

Termín biometrický údaj používá několik předpisů veřejného práva. Původně se ale objevil v Pracovním dokumentu o biometrii,²⁹ jehož autorem je Pracovní skupina (dále jen WP29) zřízená na základě čl. 29 směrnice o ochraně osobních údajů.³⁰ V tomto dokumentu se za biometrické údaje považují biometrické vzorky, které mohou být zpracovávány jak v původní formě, tak i ve formě šablony vytvořené na základě biometrického vzorku. Pracovní dokument zde zdůrazňuje, že pokud nezpracované údaje obsahují

²⁴ International standard ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics. Second edition 2017-02. In: *International Organization for Standardization* [online]. 2017 [cit. 2017-10-16]. Dostupné z: <<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>>.

²⁵ Tamtéž, bod 3.3.6.

²⁶ Tamtéž, bod 3.3.21.

²⁷ Tamtéž, bod 3.1.2.

²⁸ Tamtéž, bod 3.3.11.

²⁹ Article 29 – Data Protection Working Party. Working document on biometrics. In: *Evropská komise* [online]. 1. 8. 2003 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf>.

³⁰ 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.

citlivé údaje v době zápisu (tzv. enrolment phase), pak i tento zápis musí splňovat požadavky na zpracování citlivých osobních údajů.

Propracovanější definici biometrického údaje obsahuje dokument WP29 z roku 2007 týkající se konceptu osobních údajů. Ten za biometrické údaje považuje „*biologické vlastnosti, fyziologické vlastnosti, životní znaky nebo opakovatelné akce, přičemž tyto rysy a/nebo akce jsou pro daného jednotlivce jedinečné a jsou měřitelné, a to i přestože vzorce používané v praxi k jejich technickému měření zahrnují určitý stupeň pravděpodobnosti*“.³¹

V roce 2012 vydala WP29 zvláštní dokument o vývoji v biometrických technologiích,³² v němž zopakovala předchozí definici, stanovila, že biometrické údaje mohou mít různou formu, ale zároveň vyzdvihla systémy pro biometrickou identifikaci/verifikaci.

Český zákon o ochraně osobních údajů (dále jen ZoÚ)³³ pojem biometrického údaje používá, ale nijak jej nedefinuje. Pokud jde o biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů, pak jej ZoÚ považuje za citlivý osobní údaj (§ 4 písm. b) ZoÚ). Podobný přístup zaujímá i obecné nařízení o ochraně osobních údajů (dále jen GDPR),³⁴ podle něž jsou biometrickými údaji „*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*“

³¹ Article 29 – Data Protection Working Party. Opinion 4/2007 on the concept of personal data. In: *Evropská komise* [online]. 20. 6. 2007 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. Viz s. 8.

³² Article 29 – Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies. In: *Evropská komise* [online]. 27. 4. 2012 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

³³ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění. V souvislosti s účinností GDPR ke dni 25. 5. 2018 a navazujícího adaptačního zákona, který je v době přípravy tohoto článku v připomínkovém řízení, je plánováno zrušení tohoto zákona.

³⁴ 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 (obecné nařízení o ochraně osobních údajů).

(čl. 4 bod 14) GDPR). Právo tedy výslovně reguluje biometrické údaje pouze v užším slova smyslu, tj. pouze pokud vedou k identifikaci osoby.

3. OBECNÝ OPRAVNÍ RÁMEC

3.1 OCHRANA OSOBNOSTI A OCHRANA SOUKROMÍ – SOUKROMOPRÁVNÍ REGULACE

Osobní biometrické údaje se úzce váží na pojem ochrany osobnosti. Osobnost člověka v podstatě představuje specifické vlastnosti a odlišnosti v povaze, vzhledu a chování každého člověka. Právě přirozená individualita člověka je hodnotou, kterou chrání Listina základních práv a svobod v čl. 10³⁵ a občanský zákoník v ustanoveních na ochranu osobnosti (§§ 81-117).³⁶ Osobnost člověka „zahrnuje vše, čím se člověk projevuje navenek ve vztahu ke svému okolí, a to jak po stránce fyzické, tak po stránce duchovní a duševní“.³⁷

Z právního hlediska dochází v souvislosti s biometrickými údaji k překrývání práva na ochranu osobnosti a práva na ochranu osobních údajů.³⁸ Právo na ochranu osobnosti totiž pracuje s pojmem projev osobní povahy, který je stejně jako koncept osobního údaje úzce spjat s konkrétní osobou. Odborná literatura je toho názoru, že „každý projev osobní povahy, který můžeme přiřadit ke konkrétní osobě, je osobním údajem, nicméně osobním údajem mohou být i informace odlišného charakteru, nezávislé na osobnosti jedince, např. rodné číslo nebo číslo bankovního účtu.“³⁹ Pojem osobní údaj je tak širší než pojem projev osobní povahy, přičemž sémanticky je napojen na lidskoprávní koncept osobnosti člověka⁴⁰, resp. jeho rodinný život.

³⁵ Usnesení předsednictva České národní rady ze dne 16. prosince 1992 č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

³⁶ Zákon č. 89/2012 Sb., občanský zákoník, v platném znění.

³⁷ LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654). Komentář*. 1. vydání, Praha: C. H. Beck, 2014, 2400 s. ISBN 978-80-7400-529-9. Viz s. 392.

³⁸ KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0. Viz s. 47 an.

³⁹ Tamtéž.

Soukromí vymezil např. P. Lavický⁴¹ jako „možnost vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti osobního soukromí člověka zpřístupněny jiným subjektům a zároveň možnost se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob“, případně též E. Wagnerová:⁴² “[Soukromí] zahrnuje garanci sebeurčení ve smyslu zásadního rozhodování o sobě samém, včetně rozhodování o uspořádání vlastního života, což můžeme označit jako aktivní seberealizační komponent osobního sebeurčení. Za pasivní oblast soukromého života můžeme označit tu osobní sféru, která je imanentní samotnému lidství, jako je lidská důstojnost, nebo vnitřní potřeba sociálního kontaktu a sociálního začlenění.” Pojem soukromí tak obvykle nepředstavuje jasně a staticky vymezený termín, ale lze na něj hledět jak poměrně široce (např. dle A. Westina⁴³ jako na svého druhu „kontrolu nad informacemi o člověku – informační soukromí“, apod. Ostatně i Soudní dvůr EU dospěl k závěru, že použití výrazu „veškeré informace“ v rámci definice pojmu „osobní údaj“ v čl. 2 písm. a) směrnice 95/46 odráží cíl unijního zákonodárce přiznat tomuto pojmu široký význam, přičemž tento pojem se neomezuje na informace, které jsou citlivé nebo patří do soukromé sféry, ale potenciálně zahrnuje všechny druhy informací, a to jak objektivní, tak subjektivní ve formě názoru nebo hodnocení pod podmínkou, že jsou „o“ dotčené osobě. To je naplněno v případě, že taková informace z důvodu svého obsahu, účelu nebo účinku souvisí s určitou osobou.⁴⁴

⁴⁰ Koncept osobnosti člověka tak úzce souvisí s pojmem soukromí, respektive se definičně překrývá s pojmem soukromého a rodinného života. Pojem soukromí je tak od osobnosti člověka nedělitelný, lze na něj tedy nazírat jako na univerzální hodnotu, které je přiznána obecná ochrana. V určitém sémantickém kontextu však lze rovněž hovořit o „*soukromí právnických osob*“, tzv. „*corporate privacy*“, což však představuje pojem odlišný, směřující spíše k ochraně a důvěrnosti, resp. mlčenlivosti ve vazbě na firemní data či informace; uvedený koncept však není s ohledem na tematické zaměření na biometrické údaje předmětem tohoto článku.

⁴¹ LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654). Komentář*. 1. vydání, Praha: C. H. Beck, 2014, 2400 s. ISBN 978-80-7400-529-9. Viz s. 444.

⁴² WAGNEROVÁ, Eliška. *Právo na soukromí: Kde má být svoboda, tam musí být soukromí*, in: Šimíček, Vojtěch, *Právo na soukromí*. Brno: Muni Press, 2011, s. 54.

⁴³ WESTIN, Alan F. *Freedom and Privacy*, Londen: The Bodley Head, 1967, 508 s.

⁴⁴ K tomu více viz rozhodnutí Soudního Dvora EU ve věci C-434/16 Peter Nowak proti Data Protection Commissioner ze dne 20. 12. 2017.

Ochranu soukromí v užším smyslu, tj. jako zakotvený tradiční právní institut lze hledat a nalézat jak v právu domácím, tak i v právu mezinárodním, konkrétně v mezinárodních smlouvách, jimiž je Česká republika vázána, a jsou součástí právního řádu za podmínek čl. 10 Ústavy České republiky.

Pokud jde o právo domácí, základní právo na ochranu soukromí a na soukromý život upravují v první řadě Listina základních práv a svobod v čl. 7 odst. 1 a v čl. 10 odst. 2, dále nový občanský zákoník zejména v ust. §§ 81 odst. 2 a 86 a v řadě ustanovení i z ZoÚ. Právo mezinárodní (v širším smyslu) zakotvuje ochranu soukromí, resp. ochranu soukromého života zejména v Úmluvě o ochraně lidských práv a základních svobod v čl. 8 odst. 1, v Mezinárodním paktu o občanských a politických právech v čl. 17 odst. 1, a – pro úplnost – i v Listině základních práv Evropské unie v čl. 7 (výhradně pokud je uplatňováno právo Unie).

Do základního práva na ochranu soukromí (soukromého života) přirozeně zasahují či mohou zasahovat i biometrické údaje, tedy jejich sbírání, zpracovávání a uchovávání. Zásah do soukromí jednotlivce musí splňovat požadavky proporcionality (viz níže). V soudní praxi, ať již národní (ústavní soudy) či evropské (Evropský soud pro lidská práva)⁴⁵ se uplatňuje posouzení, v rámci něhož se zkoumá, zda bylo zásahem do soukromí porušeno příslušné ustanovení na ochranu základního práva na soukromý a rodinný život (porušení čl. 8 EÚLP). Soudy se zabývají třemi otázkami, které zní takto:

1. je zásah v souladu se zákonem, který má být dostupný, přesný a s předvídatelnými následky?
2. sledoval zásah legitimní cíl (např. ochranu života, zdraví, majetku třetích osob, ochranu veřejné bezpečnosti)?
3. byl zásah v demokratické společnosti nezbytný (tj. existovala naléhavá společenská potřeba takového zásahu)?

U této poslední otázky se dostáváme již k zmíněnému požadavku proporcionality mezi ochranou soukromí (soukromého života) na straně jedné a zásahem do něho cestou použití biometrických údajů na straně druhé.

⁴⁵ Rozsudek ESLP ze dne 2. září 2010, stíž. č. 35623/05 ve věci Uzun proti Německu.

Analýza nezbytnosti zásahu do práva na soukromí (soukromý život) bývá soudy rovněž prováděna tzv. testem proporcionality;⁴⁶ ten zná tři následující kritéria. Za prvé je to kritérium vhodnosti k dosažení daného cíle. Za druhé je to kritérium potřebnosti zásahu v porovnání s jinými opatřeními (méně omezujícími) umožňujícími dosažení daného cíle. Za třetí je to kritérium proporcionality v užším smyslu, tj. posouzení, zda rozměr (význam) zásahu je dostatečně závažný tak, aby převážil zájem jednotlivce na ochraně jeho základního lidského práva (zde práva na soukromí, resp. na soukromý život).

V souvislosti se základním právem na ochranu soukromí je namístě se zmínit i o právu na informační sebeurčení, jež nelze od soukromí jednotlivce oddělovat. Každý člověk má zásadně sám právo rozhodovat, které údaje z jeho vlastního soukromého života dá k dispozici jiným subjektům a které nikoli. Touto otázkou se zabýval i Ústavní soud České republiky v nálezech pod sp.zn. IV. ÚS 23/05 ze dne 17.7.2007 a pod sp.zn. I ÚS 705/06 ze dne 1.12.2008 a Spolkový ústavní soud německý pod zn. BVerfg GE 65, 1. Na obsah těchto judikátů lze jen pro stručnost odkázat.

Závěrem lze uvést, že základní právo na soukromí, resp. na soukromý život úzce souvisí – a mnohdy se překrývá - s jinými základními právy upravenými dalšími články Listiny základních práv a svobod, Úmluvy o ochraně lidských práv a základních svobod a mezinárodních paktů. Zde je namístě jmenovat zejména základní právo na lidskou důstojnost, osobní čest a dobrou pověst (srov. čl. 10 odst. 1 Listiny) a základní právo na ochranu osobních údajů, které se soukromého života člověka zajisté dotýká; shodně judikoval i Evropský soud pro lidská práva ve věci *Amanna v. Švýcarsko* č. 27798/95. Ochranou osobních údajů a jejím omezením se však zabývá až další část tohoto celkového textu.

3.2 OCHRANA OSOBNÍCH ÚDAJŮ A JEJÍ OMEZENÍ – ZÁKLADY OBEČNÉ VEŘEJNOPRÁVNÍ REGULACE

Ochrana osobních údajů je v současné době zakotvena v ZoÚ, který je tak v současnosti jediným obecným předpisem upravujícím zpracování

⁴⁶ Nález Ústavního soudu ze dne 12. 10. 1994 č. Pl. 4/94 (Anonymní svědek).

osobních údajů. Osobním údajem se podle § 4 písm. a) rozumí „*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*“. Pojem biometrický údaj byl společně s pojmem genetického údaje do ZoÚ zaveden zákonem č. 493/2004 Sb.,⁴⁷ a to v rámci kategorie citlivých údajů. Citlivými údaji jsou takové údaje, jejichž zneužití by mělo na jedince zvlášť závažný dopad, například by na jejich základě mohl být diskriminován.⁴⁸

Od doby účinnosti této novely, tj. od 26. července 2004, až do 1. září 2007 se za biometrický údaj považoval „*jakýkoliv biometrický údaj*“.⁴⁹ Důvodová zpráva k novele⁵⁰ ohledně zavedení tohoto pojmu do kategorie citlivých osobních údajů mlčí. Výslovně se zmiňuje o úpravě kategorie citlivého osobního údaje pouze v souvislosti s údaji vypovídajícími o trestné činnosti. Pojem biometrického údaje byl zpřesněn až novelou⁵¹ v roce 2007, která pro účely určení citlivého osobního údaje pojem biometrického údaje zúžila na „*biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů*“. Důvodová zpráva k této novele uvedla, že ne každý biometrický údaj je sám o sobě schopen identifikovat člověka, a tudíž zařazení takového údaje do kategorie citlivých údajů je neopodstatněné. Citlivým údajem by měl být podle zprávy tedy jen „*ten biometrický údaj, který*

⁴⁷ Zákon č. 493/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

⁴⁸ Kategorii citlivých osobních údajů vymezuje blíže § 4 písm. b) ZoÚ. Kromě biometrických údajů jde v současnosti o následující údaje: „osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuální životě subjektu údajů a genetický údaj subjektu údajů“.

⁴⁹ MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 s. ISBN 978-80-7357-322-5. Viz s. 87.

⁵⁰ Důvodová zpráva k zákonu č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

⁵¹ Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru. Viz část třináctá.

*umožňuje bezprostřední identifikaci nebo autentizaci subjektu údajů bez spojení s jinými údaji, tj. svou kvalitou obvykle slouží k zajištění bezpečnosti či stanovení určité míry důvěry spojených s nositeli těchto údajů“.*⁵²

Tímto zpřesněním došlo k tomu, že z definice biometrických údajů vypadly například kategorie údajů o krevní skupině nebo o chrupu.⁵³ S tím, jak se postupně vyvíjejí nové techniky analýzy nejrůznějších typů biometrických údajů (a zároveň se rozšiřují i možnosti získat z nich dodatečné informace například o zdravotním stavu), vyvstává navíc otázka, nakolik bude která metoda považována za biometrickou identifikaci, pro niž platí vyšší nároky na zpracování.

Současný ZoÚ bude v květnu 2018 nahrazen přímo použitelným nařízením GDPR. Jak již bylo zmíněno výše, i zde se za biometrický údaj považuje jen takový údaj, který umožňuje přímou identifikaci subjektu.

Co se týče existujícího ZoÚ, tak ten bude nahrazen tzv. adaptačním zákonem. Cílem tohoto zákona bude specifikovat oblasti, v nichž GDPR ponechává prostor národním úpravám, a dále implementovat novou směrnici týkající se zpracování osobních údajů za účelem prevence, vyšetřování, odhalování, či stíhání trestných činů.⁵⁴ Existující návrh adaptačního zákona počítá s umožněním zpracování biometrických údajů pro účely jedinečné identifikace člověka i pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu (§ 15 odst. 2 navrhovaného zákona). Podmínkou však je, že takové zpracování je „*nezbytné k dosažení sledovaného oprávněného cíle*“ a „*zájem na zpracování osobních údajů [převažuje] nad oprávněnými zájmy subjektu údajů*“. Podmínky zpracování biometrických údajů pak určuje GDPR.

⁵² Důvodová zpráva k zákonu č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.

⁵³ MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 s. ISBN 978-80-7357-322-5. Viz s. 88.

⁵⁴ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

3.3 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR)

Již výše několikrát zmiňované nařízení, pro něž se z anglického názvu vžila zkratka GDPR, je přímo použitelným předpisem, který od 25. května 2018 nahradí jak směrnici 95/46/ES, tak i některé stávající národní předpisy členských států v oblasti ochrany osobních údajů. GDPR by tak mělo zajistit rovnocennou ochranu při zpracování osobních údajů, ke kterému dochází v Evropské unii, tak i při zpracování osobních údajů osob nacházejících se v EU, byť ke zpracování dochází jinde než v EU. Oproti směrnici 95/46/ES poskytuje GDPR členským státům jen velmi omezený prostor pro odchylky v národní legislativě. U zpracování biometrických údajů například dává prostor k zachování nebo zavedení dalších podmínek a omezení (čl. 9 odst. 4 GDPR).

GDPR věnuje problematice biometrických údajů zvláštní pozornost. Biometrické údaje definuje a zařazuje je do tzv. zvláštní kategorie osobních údajů, na kterou se vztahují speciální pravidla uvedená v čl. 9 GDPR. Za biometrické údaje jsou podle GDPR považovány jen takové údaje, které „jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby“ (recitál 51 GDPR). Biometrické údaje jsou charakteristické tím, že mohou být poměrně snadno odezírány z těla osoby a zaznamenány například na fotografii, videu nebo na nahrávce hlasového projevu. V tuto chvíli se však tato data považují za tzv. „raw data“, tj. data ještě nezpracovaná a sama o sobě nejsou považována za biometrické údaje. Teprve po jejich zpracování dochází k vytvoření biometrických údajů ve smyslu GDPR, tzv. template. Na tento typ osobních údajů se pak vztahují speciální pravidla zpracování.

Článek 9 vyslovuje v odstavci 1 obecnou klauzuli zákazu zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby; zároveň však stanoví výjimky z tohoto zákazu (viz níže). V této souvislosti je zajímavé, že vynechává termín „autentizace“, který používá ve výše citovaném recitálu 51. Autentizací lze rozumět potvrzení identity (porovnávání one-to-one) oproti jejímu určení (porovnávání one-to-many). Dalo by se tedy říci, že GDPR z této klauzule vyjímá zákaz zpracování biometrických údajů, jakými je například ověření identity majitele telefonu se

čtečkou otisků prstů, protože při tomto zpracování telefon porovnává již uložený template s předloženým identifikátorem (otiskem prstu) a pouze zjišťuje, zda jde o stejnou osobu. Systém tedy sám nevyhledává v databázi otisků prstů a neurčuje identitu osoby předkládající otisk prstu. Na druhou stranu je ale nutno vzít v potaz samotnou definici biometrického údaje v čl. 4 odst. 14, která stanoví, že biometrický údaj „umožňuje nebo potvrzuje jedinečnou identifikaci“, přičemž čl. 9 neuvádí, jakým způsobem by mělo být jedinečné identifikace dosaženo. Přestože tedy může být s ohledem na technické termíny čl. 9 odst. 1 ne zcela jasný, vztahuje se na oba případy, tj. jak na autentizaci, tak i na identifikaci.

Přestože je zpracovávání biometrických údajů obecně zakázáno, čl. 9 stanoví v odst. 2 hned deset výjimek z tohoto zákazu. Biometrické údaje je podle čl. 9 odst. 2 písm. a) možné zpracovávat v případě, kdy „subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen“. Podmínky udělení souhlasu dále stanoví čl. 7 GDPR a recitály.⁵⁵ Správce, který zpracovává biometrické údaje na základě souhlasu, musí být vždy schopen doložit získání tohoto souhlasu. O souhlas musí subjekt údajů požádat takovým způsobem, aby byl subjekt údajů skutečně srozumitelně a jasně obeznámen s faktem, že uděluje souhlas se zpracováním těchto svých údajů. Žádost o souhlas by neměla být součástí dlouhých ujednání, v nichž není udělení souhlasu zřejmé. Zároveň by mělo jít o aktivní potvrzení ze strany subjektu údajů, tedy nikoliv mlčení, nebo naopak nutnosti odškrtnout předem označený souhlas v elektronickém formuláři. Podrobná vodítka by měla k problematice vydat na jaře 2018 WP 29.

Dalšími případy, v nichž může správce zpracovávat biometrické údaje pro účely jedinečné identifikace, jsou následující případy: plnění povinností a výkon práv v oblasti práva pracovního a práva sociálního zabezpečení a

⁵⁵ Zvláštní podmínky týkající se souhlasu dětí stanoví čl. 8. Recitály vztahující se k udělení souhlasu jsou recitály č. 32, 33, 38, 40, 42, 43, 50, 51, 65, 68, 71, 111, 112, 155, 161 a 171.

sociální ochrany pod podmínkou poskytnutí záruk ochrany základních práv a zájmů subjektů údajů (čl. 9 odst. 2 písm. b)), ochrany „životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas“ (čl. 9 odst. 2 písm. c)), zpracování prováděného s vhodnými zárukami neziskovým subjektem (čl. 9 odst. 2 písm. d)),⁵⁶ zpracování osobních údajů zjevně subjektem údajů zveřejněných (čl. 9 odst. 2 písm. e)),⁵⁷ zpracování nezbytného pro „určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednájí v rámci svých soudních pravomocí“ (čl. 9 odst. 2 písm. f)), zpracovávání prováděného z důvodu významného veřejného zájmu (čl. 9 odst. 2 písm. g)), zpracovávání nezbytného „pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče“ (čl. 9 odst. 2 písm. h)), zpracování nezbytného z důvodu veřejného zájmu v oblasti veřejného zdraví (čl. 9 odst. 2 písm. i)) a zpracování nezbytného „pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely“, přičemž subjektům údajů musí být poskytnuty vhodné záruky pro ochranu jejich základních práv a svobod (čl. 9 odst. 2 písm. j)).

Na zvláštní kategorie osobních údajů, mezi něž patří právě biometrické údaje, se vztahují i další pravidla.⁵⁸ Na biometrických údajích by neměla být založena automatizovaná rozhodnutí včetně profilování, která by měla pro subjekt údajů právní účinky nebo by se ho jinak významně dotýkala (čl. 22 GDPR). Ke zpracovávání biometrických údajů vždy z podstaty dochází automatizovaným způsobem. Je ovšem otázkou, zda se subjektu údajů významně dotýká situace, v níž by došlo k případnému odmítnutí přístupu

⁵⁶ Je otázkou, zda je možné tuto výjimku aplikovat na biometrické údaje. Účelem této výjimky je zejména umožnit zpracování jiných kategorií osobních údajů, které čl. 9 v odst. 1 zakazuje, zejm. údaje o politických názorech, náboženském vyznání, filozofickém přesvědčení a členství v odborech.

⁵⁷ Jak již bylo zmíněno výše, biometrickým údajem ve smyslu GDPR je až údaj vytvořený z nezpracovaných dat. Subjekt údajů by tak musel zveřejnit biometrický template, aby správce mohl odkázat na tuto výjimku.

⁵⁸ Ke zvláštní kategorii osobních údajů se vztahují zejm. recitály 10, 51, 52, 53, 54, 71, 80, 91 a 97.

buď k určité službě, nebo do určitého prostoru. Nově přijatá vodítka WP 29 stanoví, že účinky takového zpracování údajů „musí být dostatečně rozsáhlé nebo závažné, aby stálo za pozornost. Jinými slovy, rozhodnutí musí mít potenciálně významný vliv na okolnosti související s dotčenými osobami nebo na jejich chování či výběr. V krajním případě může takové rozhodnutí vést k vyloučení nebo diskriminaci jednotlivců“.⁵⁹ Pokud by tomu tak bylo, pak by bylo možno biometrické údaje zpracovávat pouze za podmínky, že k tomu subjekt údajů udělil výslovný souhlas nebo jde o zpracování nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu. Zároveň musí být v obou případech pomocí vhodných opatření zajištěna práva, svobody a oprávněné zájmy subjektů údajů.

Další významnou povinností při zpracování biometrických údajů je pak povinnost provést posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR. V případě, že hlavní činnost správce nebo zpracovatele spočívá v rozsáhlém zpracovávání biometrických údajů, pak jsou tyto subjekty také povinny jmenovat pověřence pro ochranu osobních údajů dle čl. 37 GDPR.

3.4 BIOMETRIKA A OSOBNÍ DOKLADY

3.4.1 CESTOVNÍ DOKLADY

Pro cestovní pasy a cestovní doklady platí v Evropské unii unifikovaná pravidla, která pro tyto doklady stanoví minimální bezpečnostní normy.⁶⁰ V cestovních pasech a dokladech jsou povinně obsaženy biometrické prvky, a to zobrazení obličeje a otisky prstů. Otisky prstů musí být zahrnuty v interoperabilních formátech. Tyto údaje musí být zabezpečeny a v dokladu jsou uloženy na médiu pro uchování údajů. Toto médium „*musí mít dostatečnou kapacitu a schopnost zaručit neporušitelnost, pravost a utajení údajů*“ (čl. 1 odst. 2 nařízení). Biometrické údaje obsažené v dokladu se mohou po-

⁵⁹ Pracovní skupina podle článku 29. Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679. Úřad na ochranu osobních údajů [online]. 3. 10. 2017 [vid. 2017-12-08]. Dostupné z: < https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30197 > .

⁶⁰ Nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy.

užít pouze pro ověřování „pravosti dokumentu“ a „totožnosti držitele pomocí přímo dostupných srovnatelných prvků v případech, kdy musí být cestovní pas nebo jiný cestovní doklad podle právních předpisů předložen“ (čl. 4 odst. 3 nařízení). Osoby mají právo „ověřit osobní údaje obsažené v cestovním pase nebo cestovním dokladu a případně požadovat provedení opravy nebo výmazu“ (čl. 4 odst. 1 nařízení). Nařízení v příloze stanoví konkrétní pravidla a opatření, jaká by měla být přijata a dodržována při výrobě cestovních pasů a dokladů. Ta se ale týkají zejména stránky s biografickými údaji.

Problematiku cestovních dokladů upravuje i české právo. Podle zákona o cestovních dokladech⁶¹ se údaje o zobrazení obličeje a o otiscích prstů ukládají do dokladu ve strojově čitelné formě. U některých osob se zaznamenává pouze zobrazení obličeje (viz § 5 odst. 4). Zákon upravuje pořizování biometrických údajů (§ 21a) a kontrolu funkčnosti nosiče dat s biometrickými údaji (§ 21b). Biometrické údaje se zaznamenávají i do služebních a diplomatických pasů.

Držitelé cestovních dokladů mají právo „požádat o ověření funkčnosti nosiče dat a správnosti v něm zpracovaných biometrických údajů“ a v případě nesrovnalostí mají tyto osoby právo na vydání nového cestovního dokladu (§ 32a). Neoprávněné zpracovávání osobních údajů z nosiče biometrických údajů se považuje za přestupek. Další podrobnosti týkající se biometrických údajů ve veřejných dokladech a cestovních dokladech stanoví další právní předpisy.⁶²

⁶¹ Zákon č. 329/1999 Sb., o cestovních dokladech, v platném znění.

⁶² Viz Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji a o změně některých zákonů, v platném znění, vyhláška č. 415/2006 Sb., kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu, vyhláška č. 400/2011 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech, v platném znění, metodický pokyn Ministerstva vnitra č.j. SC - 243/2006 ze dne 6. září 2006 k postupu obecních úřadů obcí s rozšířenou působností při zpracovávání žádostí a vydávání cestovních pasů se strojově čitelnými údaji a s nosičem dat s biometrickými údaji, směrnice Ministerstva vnitra k zákonu č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, zákonu č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a zákonu č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), ve znění pozdějších předpisů.

3.4.2 PRŮKAZY VYDÁVANÉ EVROPSKOU UNIÍ

Členům orgánů Evropské unie a jejich zaměstnancům se na základě zvláštního nařízení vydává speciální průkaz, který se uznává za platný cestovní doklad.⁶³ Tento speciální průkaz musí být v souladu s již zmíněným Nařízením Rady č. 2252/2004. Obsahuje jak biografické, tak i biometrické údaje. Biometrickými prvky jsou zobrazení obličeje a dva digitální otisky prstů. Držitelé tohoto speciálního průkazu mají specifická práva definovaná v čl. 5 nařízení.⁶⁴ Držitelé průkazů mají zejména právo „ověřit si osobní údaje, které jsou v průkazu uvedeny, a v případě potřeby požádat o jejich opravu nebo vypuštění“. Biometrické prvky v průkazu mohou být použity pouze pro ověřování „pravosti dokladu“ a „totožnosti držitele pomocí porovnatelných prvků, které jsou přímo k dispozici“.

3.4.3 BIOMETRICKÉ ÚDAJE CIZINCŮ

Biometrické údaje se používají i pro identifikaci cizinců vstupujících na území České republiky. Základním předpisem je v tomto ohledu zákon o pobytu cizinců,⁶⁵ který stanoví povinnost strpět ověření biometrických údajů při vstupu na české území (§ 5 odst. 2 písm. b)), strpět pořízení biometrických údajů při podání žádosti o povolení k dlouhodobému pobytu (§ 44) nebo o povolení k trvalému pobytu (§ 74). Cizinci mají obecně povinnost strpět aktuální pořízení biometrických údajů za účelem ověření pravosti průkazu (§ 103 písm. t)). Zvláštní pravidla se vztahují k vydávání cizineckého pasu (§ 113). Na základě žádostí o povolení k pobytu se cizincům vydává průkaz o povolení k pobytu. Ten obsahuje nosič dat s biometrickými údaji o zobrazení obličeje a otisků prstů. Průkaz o povolení k pobytu s biometrickými prvky se vydává rovněž dle § 35 zákona o dočasné ochraně cizinců⁶⁶ a podle § 59 zákona o azylu.⁶⁷ Tento zákon provádí speci-

⁶³ Nařízení Rady (EU) č. 1417/2013 ze dne 17. prosince 2013, kterým se stanoví vzor průkazu vydávaného Evropskou unií.

⁶⁴ Tamtéž.

⁶⁵ Zákon č. 326/1999 Sb. o pobytu cizinců na území České republiky a o změně některých zákonů.

⁶⁶ Zákon č. 221/2003 Sb., o dočasné ochraně cizinců, v platném znění.

⁶⁷ Zákon č. 325/1999 Sb., o azylu, v platném znění.

ální vyhláška, která stanoví podmínky pro pořizování biometrických údajů týkajících se zobrazení obličeje, otisků prstů a vlastnoručního podpisu.⁶⁸

3.4.4 ŘIDIČSKÉ PRŮKAZY S MIKROČIPEM

V Evropské unii je zaveden vnitrostátní řidičský průkaz na základě směrnice o řidičských průkazech.⁶⁹ Volitelně mohou členské státy zavést jako součást řidičského průkazu mikročip, který obsahuje harmonizované údaje. Doplňkovou datovou skupinou u těchto řidičských průkazů jsou i biometrické údaje týkající se otisku prstů nebo oční duhovky.⁷⁰ Zahnutí těchto datových skupin je na volbě jednotlivých členských států EU.

3.5 ZPRACOVÁNÍ BIOMETRICKÝCH ÚDAJŮ V OBLASTI VÝKONU VEŘEJNÉ MOCI

3.5.1 ZPRACOVÁVÁNÍ BIOMETRICKÝCH ÚDAJŮ POLICIÍ ČESKÉ REPUBLIKY A V RÁMCI TRESTNÍHO ŘÍZENÍ

Policie České republiky zpracovává informace a osobní údaje v souladu se svým zvláštním zákonem (dále jen ZPČR).⁷¹ Práce s informacemi je upravena v §§ 60–80 ZPČR. Tento zákon nepoužívá termín biometrický údaj jako takový, ale umožňuje Policii „*snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy a odebírat biologické vzorky umožňující získání informací o genetickém vybavení*“ (§ 65 odst. 1 ZPČR) u osob obviněných ze spáchání úmyslného trestného činu, osob, kterým bylo sděleno podezření pro spáchání takového trestného činu, osob ve výkonu trestu odnětí svobody za spáchání úmyslného trestného činu, osob, jimž bylo uloženo ochranné léčení nebo zabezpečovací detence, nebo u nalezených osob, po nichž bylo vyhlášeno pátrání a jejichž

⁶⁸ Vyhláška č. 88/2011 Sb., o technických podmínkách a postupu při pořizování biometrických údajů a podpisu cizince pro účely vydání průkazu o povolení k pobytu, v platném znění.

⁶⁹ Směrnice Evropského parlamentu a Rady 2006/126/ES ze dne 20. prosince 2006 o řidičských průkazech (přepřacované znění) (Text s významem pro EHP).

⁷⁰ Nařízení Komise (EU) č. 383/2012 ze dne 4. května 2012, kterým se stanoví technické požadavky týkající se řidičských průkazů, které zahrnují paměťové médium (mikročip).

⁷¹ Zákon č. 273/2008 Sb., o Policii České republiky, v platném znění.

svéprávnost je omezena (§ 65 odst. 1 ZPČR). Takovéto získávání údajů ale musí být prováděno pouze za účelem budoucí identifikace. Policista může údaje získat po předchozí marné výzvě i přes odpor osoby, od které údaje získává, s výjimkou situací, kdy by mělo být zasaženo do tělesné integrity jednotlivce (např. při odběru krve). Policie ČR může dále získávat informace z evidencí provozovaných na základě zvláštního právního předpisu (§ 66 ZPČR), včetně evidence cestovních dokladů, která obsahuje biometrické údaje osob. Zákon umožňuje Policii ČR zpracovávat osobní údaje včetně citlivých údajů bez souhlasu osoby, pokud tak činí v rámci plnění svých úkolů (§ 79 ZPČR).

Biometrické údaje hrají roli i ve vykonávacím řízení zakotveném v trestním řádu (dále jen TŘ).⁷² V případě nařízení výkonu trestu domácího vězení je při kontrole výkonu tohoto trestu *„odsouzený povinen umožnit orgánu zajišťujícímu kontrolu vstup do místa výkonu trestu a strpět pořízení svých biometrických údajů orgánem zajišťujícím kontrolu na jeho žádost při zahájení elektronické kontroly, a dále v jejím průběhu, existuje-li podezření na porušení kontrolovaných povinností. Pořizovanými biometrickými údaji jsou otisky prstů, rysy obličeje a záznam hlasu“* (§ 334b odst. 1 TŘ).

Strpět pořízení biometrických údajů musí i obviněná osoba v rámci výkonu elektronické kontroly plnění povinností uložených v souvislosti s některým opatřením nahrazujícím vazbu (§ 360a odst. 2 TŘ). I zde se biometrickými údaji rozumí otisky prstů, rysy obličeje a záznam hlasu. Samotný postup při pořizování a ověřování je detailněji popsán v důvodové zprávě k novele TŘ z dubna 2016.⁷³ Biometrické údaje by měly být podle této zprávy snímány buď za účelem *„dvojitěho ověření totožnosti, či za účelem následného měření přítomnosti alkoholu v dechu (v souvislosti s případně uloženým omezením zdržet se požívání alkoholických nápojů)“*.

⁷² Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), v platném znění.

⁷³ Důvodová zpráva k zákonu č. 150/2016 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů, a zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Pojem biometrického údaje se objevuje i v zákoně o Rejstříku trestů.⁷⁴ Podle § 10 odst. 5 zákona se biometrické údaje neuvádí ve zvláštní části opisu z Rejstříku trestů, kam se podle § 4a uvádí „údaje o pravomocných odsouzeních občanů České republiky soudy jiného členského státu Evropské unie v trestním řízení a údaje navazující na tato odsouzení, a to na základě informací zaslaných jinými členskými státy Evropské unie“. S ohledem na přijetí zvláštní evropské směrnice⁷⁵ bude muset být zmíněná regulace zrevidována a případně uvedena v soulad s pravidly v této směrnici, a to do 6. května 2018.

3.5.2 ZPRACOVÁVÁNÍ BIOMETRICKÝCH ÚDAJŮ VOJENSKOU POLICIÍ

Osobní údaje zpracovává na základě zvláštního zákona i Vojenská policie.⁷⁶ Nakládání s informacemi je v tomto zákoně upraveno v §§ 10-20. Vojenská policie je podle těchto ustanovení oprávněna zejména pořizovat zvukové, obrazové nebo jiné záznamy z veřejně přístupných míst (§ 11), požadovat informace z určených informačních systémů (§ 12), či zpracovávat osobní údaje včetně citlivých údajů bez souhlasu subjektu údajů (§ 13). Zvláštní pravidla platí při zpracování osobních údajů v rámci předcházení a odhalování trestné činnosti (§ 14) a při pátrání po vojácích (§ 15). V současné době se projednává novela zákona o Vojenské policii,⁷⁷ která se výslovně věnuje i zpracovávání biometrických údajů.

Na základě této novely by mělo být do zákona vloženo ustanovení § 11a, které by Vojenské policii umožnilo získávat osobní údaje pro účely budoucí identifikace u fyzických osob obviněných ze spáchání úmyslného trestného činu nebo těch osob, kterým bylo sděleno podezření pro spáchání

⁷⁴ Zákon č. 269/1994 Sb., o Rejstříku trestů, v platném znění.

⁷⁵ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

⁷⁶ Zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů, v platném znění.

⁷⁷ Sněmovní tisk č. 973/0 ze dne 29. 11. 2016, vládní návrh zákona, kterým se mění zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [cit. 2017-10-16]. Dostupné z: <<http://www.psp.cz/sqw/historie.sqw?t=973>>.

takového trestného činu. Toto ustanovení v podstatě do určité míry kopíruje § 65 ZPČR. Vojenská policie by na jeho základě byla oprávněna „snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy a odebírat biologické vzorky umožňující zpracování genetických údajů fyzické osoby a tyto údaje dále zpracovávat“, a to i přes odpor této osoby. Vojenský policista by směl tento odpor překonat způsobem přiměřeným intenzitě odporu, to by neplatilo v případech, kdy by šlo o zásah do tělesné integrity osoby, např. při odběru krve.

3.5.3 TRESTNÉ ČINY SOUVISEJÍCÍ S BIOMETRICKÝMI ÚDAJI

V souvislosti s biometrickými údaji lze uvažovat o spáchání několika trestných činů. Prvním z nich je neoprávněné nakládání s osobními údaji, které postihuje § 180 trestního zákoníku.⁷⁸ Ten v prvním a druhém odstavci obsahuje dvě samostatné skutkové podstaty. První se týká neoprávněného zpracování osobních údajů shromážděných v souvislosti s výkonem veřejné moci. Druhá se týká neoprávněného zveřejnění, sdělení nebo zpřístupnění osobních údajů získaných v souvislosti s výkonem povolání, zaměstnání nebo funkce třetí osobě při současném porušení povinnosti mlčenlivosti.

Dalším trestným činem, který lze spáchat za pomoci biometrických údajů je trestný čin dle § 230 odst. 1 trestního zákoníku, kterého se dopustí ten, kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části. Bezpečnostní opatření lze překonat za pomoci neoprávněně sejmutého nebo neoprávněně užitého otisku prstu. Pachatel nemusí bezpečnostní opatření překonat. Trestní je i opatření, přechovávání a další nakládání s nástrojem nebo jiným prostředkem vytvořeným nebo přizpůsobeným k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části (§ 231 trestního zákoníku).

Dále lze uvažovat o neoprávněném odebrání tkání a orgánů, které postihuje § 164 trestního zákoníku. Přestože bylo toto ustanovení zařazeno do

⁷⁸ Zákon č. 40/2009 Sb., trestní zákoník, v platném znění.

trestního zákoníku v návaznosti na Úmluvu o lidských právech a biomedicíně⁷⁹ a dalších dokumentech a zákonech (zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů, zákon č. 227/2006 Sb., o výzkumu na lidských embryonálních kmenových buňkách a souvisejících činnostech, nebo zákon č. 296/2008 Sb., o zajištění jakosti a bezpečnosti lidských tkání a buněk určených k použití u člověka),⁸⁰ může se vztahovat na neoprávněný odběr vzorku DNA, které se následně použije jako biometrický identifikátor.

Dalším trestným činem, který lze v souvislosti s biometrickými údaji spáchat, je trestný čin podvodu podle § 209 trestního zákoníku. Například u behaviorálních biometrických údajů je, byť stěžší, ale přeci jen možné tyto údaje napodobit a přisvojit si cizí identitu za účelem uvedení jiného v omyl a následně neoprávněném obohacení se.

4. BIOMETRICKÁ IDENTIFIKACE A AUTENTIZACE

4.1 DOBROVOLNÁ (SMLUVNÍ) IDENTIFIKACE A AUTENTIZACE

Biometrické údaje jsou čím dál populárnějším prostředkem pro zajištění bezpečnosti při vstupu do objektů (odemykání domu pomocí otisku prstu místo klíče, zajištění vstupu na pracoviště nebo do škol, apod.), pro zajištění přístupu do přístrojů (chytrých telefonů, notebooků) či pro autentizaci při používání zejména platebních služeb. V těchto případech dochází ke zpracování osobních údajů na základě souhlasu subjektu údajů. Na tento souhlas se budou vztahovat podmínky blíže popsané v části týkající se obecného nařízení pro ochranu osobních údajů (GDPR). Ke zpracování údajů může docházet i k ochraně oprávněných zájmů správce nebo třetích osob. Chráněným zájmem zde bude ochrana zdraví nebo majetku osob, které se v budově nachází, či ochrana dat uložených v takto zabezpečených zařízeních. Následující text se zaměří na zpracování biometrických údajů rovněž již ve světle GDPR.

⁷⁹ Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny. Sdělení Ministerstva zahraničních věcí č. 96/2001 Sb.m.s.

⁸⁰ ŠÁMAL, Pavel a kol. *Trestní zákoník*. 2. vydání. Praha: C.H.Beck, 2012, 3614 s. ISBN 978-80-7400-428-5. Viz s. 1790 an.

V souvislosti s tímto způsobem zpracovávání osobních údajů se objevují zejména dva praktické problémy. Prvním problémem je tvrzení správců, že údaje, které v této souvislosti zpracovávají, nejsou biometrickými údaji. Jedná se o situace, kdy se například zaměstnanec nebo student prokazuje při vstupu do budovy kartou, na níž jsou uloženy údaje založené na jeho biometrických charakteristikách, které však byly zpracovány tak, že nejdou samostatně analýzou zpětně přiřadit k určité osobě a původní nezpracovaná data byla ze systému vymazána. Správce argumentuje tím, že již nezpracovává žádné osobní údaje, protože na základě těchto údajů nelze nikoho zpětně identifikovat, pouze jej zařadit do skupiny osob, které buď mají, nebo nemají přístup. Pracovní skupina WP 29 však v této souvislosti ve svých vodítkách č. 191 zmínila, že „*umožnění jedinečné identifikace*“ není v souvislosti s biometrickými údaji přesné, protože biometrické údaje lze využít i pro autentifikaci bez toho, aniž by došlo k identifikaci osoby.⁸¹ V tomto světle je tak nutné vykládat i pojem biometrického údaje, který nemusí být zpětně dekodovatelný. Zároveň je nutné upozornit na fakt, že správci musí být schopni osobu ze skupiny osob s povoleným přístupem vyloučit například při změně statusu dané osoby, kdy přestane být zaměstnancem nebo studentem.

Dalším problémem je otázka týkající se osoby správce. Například u bankovních aplikací využívajících biometrickou identifikaci se biometrické údaje zpracovávají v aplikaci poskytnuté bankou uživateli, avšak data sama zůstávají v zařízení uživatele a banka k nim nemá přístup. Argumentem pro nezpracovávání biometrických údajů je pak absence přístupu. V tomto směru je však nutné podívat se důkladně na definici správce, kterým je podle čl. 4 odst. 7 GDPR osoba, která určuje účely a prostředky zpracování osobních údajů. Definice neurčuje jako podmínku přístup k samotným údajům, ke kterým tak jako tak dochází povětšinou automatizovaně. Důležitým je zde tedy účel a prostředky. Je na vůli banky nebo případně jiného subjektu určit, zda bude mít k datům přístup nebo ne. Omezení pří-

⁸¹ Article 29 Data Protection Working Party. Opinion No. 1/2012 on the data protection reform proposals. *European Commission* [online]. 23. 3. 2012 [vid. 2017-12-08]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.

stupu k biometrickým údajům může být opatřením k zajištění jejich bezpečnosti, nikoliv však k vyhnutí se povinností správce při zpracovávání biometrických údajů.

4.2 POVINNÁ BIOMETRICKÁ IDENTIFIKACE A AUTENTIZACE

České právo výslovně vyžaduje biometrickou identifikaci osob pro vstup do vymezených a fyzicky ohraničených prostor jaderných zařízení. Tyto prostory mají čtyři soustředné úrovně, které jsou „odlišené typem ochranných opatření“,⁸² a patří mezi ně střežený prostor, chráněný prostor, vnitřní prostor a životně důležitý prostor.⁸³ Podle prováděcí vyhlášky k atomovému zákonu⁸⁴ „každý, kdo je oprávněn vstupovat do střeženého, chráněného, vnitřního nebo životně důležitého prostoru, musí být vybaven identifikační kartou umožňující automatickou kontrolu vstupu. Pro kontrolu vstupu fyzických osob musí být nejméně při vstupu do vnitřního nebo životně důležitého prostoru použita biometrická identifikace. Aktuální databáze vstupů musí být dostupná nejméně 1 měsíc a musí být zajištěno její trvalé uchování“ (§ 11 odst. 2). Vyhláška v § 11 rovněž stanoví podmínky uchování informací o identifikačních kartách, vstupech a průchodech osob, zaznamenávání hlasové komunikace pracovníků a sledování pohybu osob v případě mimořádné radiací události. Povinnost biometrické identifikace osob je dále stanovena i v § 13 odst. 1 a 4 vyhlášky, který se týká pouze vnitřního a životně důležitého prostoru. Tyto prostory jsou dále povinně vybaveny systémem detekujícím narušení a systémem průmyslové televize.

Další oblastí, v níž bude vyžadována biometrická identifikace, je oblast platebního styku. Dne 21. 3. 2017 předložila vláda Poslanecké sněmovně Parlamentu ČR návrh zákona o platebním styku jako sněmovní tisk č. 1059/0.⁸⁵ Tento návrh zákona počítá v § 223 s tzv. silným ověřením uživatele osobou oprávněnou poskytovat platební služby v případech, kdy

⁸² Důvodová zpráva k zákonu č. 263/2016 Sb., Atomový zákon, k § 161.

⁸³ Zákon č. 263/2016 Sb., atomový zákon, v platném znění. § 161 odst. 1.

⁸⁴ Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu.

⁸⁵ Sněmovní tisk č. 1059/0 ze dne 21. 3. 2017, vládní návrh zákona o platebním styku. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [cit. 2017-10-16]. Dostupné z: <<http://www.psp.cz/sqw/historie.sqw?o=7&t=1059>>.

bude např. uživatel přistupovat ke svému účtu prostřednictvím internetu, nebo bude zadávat platební příkaz elektronicky. Silné ověření je pak definováno v § 223 odst. 3 tohoto návrhu zákona, podle nějž se jím „rozumí ověření, které je založeno na použití alespoň 2 z těchto prvků: a) údaje, který je znám pouze uživateli, b) věci, kterou má uživatel ve své moci, c) biometrických údajů uživatele“. Biometrický údaj je tedy jen jednou z variant ověření a nemusí tedy být nutně povinnou formou. Návrh zákona byl dne 16. 10. 2017 doručen prezidentovi republiky k podpisu a měl by vstoupit v účinnost dne 13. 1. 2018. Biometrické údaje bere mimochodem v potaz i zákon o účetnictví,⁸⁶ který v § 33 odst. 2 písm. c) počítá s tzv. smíšenou formou účetního záznamu, kterou je „záznam v listinné formě obsahující též informace v technické formě pro fyzickou osobu nečitelné, který umožňuje jeho převedení do formy, v níž je jeho obsah pro fyzickou osobu čitelný“ a jako příklad takovéto smíšené formy uvádí důvodová zpráva k novele pas s biometrickými údaji.⁸⁷

O povinné biometrické identifikaci se uvažovalo i v důvodové zprávě k zákonu o hazardních hrách,⁸⁸ kdy biometrická identifikace hráčů měla být zahrnuta v tzv. *precommitment* systému a měla sloužit k dodržování hráčských limitů. Od tohoto požadavku ale bylo nakonec upuštěno.

4.3 (DYNAMICKÝ) BIOMETRICKÝ PODPIS

Praktické využití biometrické identifikace jako jedné z klíčových behaviorálních (biometrických) metod lze najít v celé řadě právně-relevantních oblastí. Jednou z možných využití bude nepochybně analýza ručně psaného písma, zejména pak podpisu, kde lze v rámci forenzních písmoznaleckých oborů, a na základě shora uvedených metod, rozhodnout s určitou pravděpodobností o identitě či autentizaci konkrétní osoby. Použití těchto metod pak vede k automatizovanému vyhodnocení nejen výsledného statického obrazu vlastnoručního podpisu, ale i vysoce detailně zaznamenanému pro-

⁸⁶ Zákon č. 563/1991 Sb., o účetnictví, v platném znění.

⁸⁷ Důvodová zpráva k zákonu č. 304/2008 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a některé zákony. Viz k bodu 32-34.

⁸⁸ Důvodová zpráva k zákonu č. 186/2016 Sb. o hazardních hrách.

cesu vytváření⁸⁹ (psaní) vlastnoručního písma či podpisu, jejímž výsledkem je relativně přesné a automatizované určení pravosti písma či podpisu.

Tyto verifikační metody tak pro svou relativní spolehlivost a automatizovanost vedou k hledání dalších možností jejich využití, včetně úvah o jejich celkové důkazní spolehlivosti a možnostech jejich využití v současné platné právní úpravě. V tomto ohledu se jeví jako nezbytné důkladně zvážit jejich použitelnost, resp. dovolenost jejich použití v právu hmotném i procesním, a to zejména v kontextu nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále jen nařízení eIDAS), jakož i v zákoně č. 297/2016 Sb., o službách vytvářejících důvěru v elektronických transakcích, ve znění pozdějších předpisů (dále jen ZoSVD), tak i v ustanovení zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen NOZ). S ohledem na samotnou podstatu i význam metod dynamické verifikace tohoto druhu podpisu je nutno rovněž odpovědně posoudit i související problematiku dalšího zpracování těchto behaviorálních osobních údajů generovaných v rámci procesu vytváření (psaní) podpisu, a to jak na základě současné dosluhující právní úpravy dle ZoÚ, tak i nastávající úpravy vzešlé z nařízení GDPR.

Výše uvedeným úvahám již byla věnována pozornost jak v právní teorii, tak i v praxi, přičemž klíčové dílčí úvahy k otázkám biometrických možností (elektronického) podepisování, včetně otázek důkazní spolehlivosti se podrobně věnuje publikace autorů J. Matejky a V. Güttlera,⁹⁰ úvahám k otázkám samotné elektronické kontraktace, jakož i jednotlivým náležitostem

⁸⁹ Hovoříme o metodách dynamické verifikace podpisu, které vyhodnocují v reálném čase rychlost psaní podpisu, tlak hrotu pera v jednotlivých fázích rukopisu, směr a posloupnost psaní některých prvků, jako je škrtnání, zdůrazňování určitých partií, psaní teček, a to včetně celé řady dalších typických odlišností, které mohou k identifikaci konkrétní osoby či podpisu kvalitativně přispět.

⁹⁰ MATEJKA, Ján., GÜTTLER, Vojen: Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. In: *The Lawyer Quarterly*, 2018, roč. 8, č. 1, str. 38 – 50.

podpisu a jeho jednotlivým funkcím se blíže věnovali např. R. Polčák,⁹¹ F. Korbel s F. Melzerem,⁹² J. Matejka⁹³ a K. Čermák,⁹⁴ případně též V. Kment.⁹⁵

Ve vztahu k závěrům učiněným v těchto publikacích lze dovodit, že současná právní úprava neobsahuje sama o sobě jakékoliv kvalitativní požadavky směrem k identifikaci či určení totožnosti podepisující osoby; jedinou kvalitativní náležitostí je vysoce obecný odkaz na svého druhu zvyklost podepisující osoby připojit „data užívaná k podepsání“, což mohou být v zásadě jakákoliv data v elektronické podobě, včetně dat biometrických. Tento poměrně liberální přístup zákonodárce tak nejenom naplňuje principy vyplývající z nařízení eIDAS, ale také potvrzuje tradiční respekt k autonomii vůle stran jako svého druhu nezastupitelné hodnoty účastníků soukromého práva. Elektronickému podpisu, lhostejno zda je založen na metodách fyzické či behaviorální biometrie, tak nejsou upírány právní účinky a není odmítán jako důkaz v soudním řízení. Má-li být komunikace prostřednictvím těchto moderních forem efektivní, je třeba při jejich aplikaci důsledně vycházet z historicky osvědčených a ustálených zásad a principů soukromého práva. Samotné elektronické formy podepisování ve formě připojení biometrických (fyzických či behaviorálních) dat k elektronickým písemnostem (právním jednáním), tak nejenom že důsledně navazují na toto tradiční (tj. především grafické) pojetí podpisu, ale zároveň představují zdánlivě ideální propojení tradičního a elektronického pojetí podepisování směřující k tolik žádoucímu přirozenému rozvoji práva. Připuštění možnosti užití těchto moderních forem podpisu tak v mnoha ohledech posiluje jak postavení elektronických písemností a jejich využití v právním styku, tak i zcela ne-

⁹¹ POLČÁK, Radim. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*, 2013, č. 10, str. 34-40, str. 36, případně též POLČÁK, Radim. Praxe elektronických dokumentů. In: *Bulletin advokacie*, 2011, č. 7-8, str. 55.

⁹² KORBEL, František, MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. In: *Bulletin advokacie*, roč. 2014, č. 12, str. 31-36, str. 32.

⁹³ MATEJKA, Ján. Úprava elektronického podpisu v právním řádu ČR. In: *Právník*, 2001, roč. 140, č. 5, s. 582 – 611.

⁹⁴ ČERMÁK, Karel ml. Elektronický podpis: pohled soukromoprávní. In: *Bulletin advokacie*, roč. 2002, č. 11, str. 64-77.

⁹⁵ KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? In: *Bulletin advokacie*, roč. 2016, č. 12, s. 5.

pochybně povede ke standardizaci nových praktických postupu kombinujících metody biometrické (jako ideální autentizační či kvasi-identifikační nástroj) a kryptologické (kvalifikovaný elektronický podpis).⁹⁶

Navzdory současnému liberálnímu pojetí této soukromoprávní materie promítnuté do NOZ, nutno respektovat i poměrně zásadní omezení vyplývající z veřejnoprávní regulace ochrany osobních údajů, stanovící, že podepisování elektronických dokumentů za současného využití biometrických metod (biometriky fyzické i behaviorální) musí být realizováno v souladu se všemi principy ochrany osobních údajů, tj. včetně existence a prokázání právních titulů, principů transparentnosti a proporcionality (balanční test), a dalších.⁹⁷

5. ZÁVĚR

Cílem tohoto příspěvku bylo především analyzovat, resp. identifikovat rozdíly vyplývající z jednotlivých režimů zpracování biometrických údajů jako svého druhu privilegované kategorie osobních údajů v rámci české právní úpravy. Ze shora uvedených závěrů vyplývá, že dosavadní právní úprava je sice značně roztržštěná, nezřídka na sebe navenazuje a místy je významně ovládána určitým resortismem, nicméně i tak ji lze považovat za funkční, a to zejména s ohledem na obecně aplikovatelné principy veřejnoprávní ochrany, požadavků vyplývajících z Listiny základních práv a svobod a z mezinárodního práva.

Z pohledu zásadní ochrany poskytované předpisy veřejného práva nutno akcentovat skutečnost, že platná právní úprava řadí mezi citlivé osobní údaje biometrické údaje ve chvíli, kdy jsou využívány k identifikaci či autentizaci člověka (jako subjektů těchto údajů). Samotné nařízení GDPR pak nově pro zařazení mezi takto privilegované (citlivé⁹⁸) osobní údaje požaduje jejich využití pouze pro identifikaci; z pohledu informační bezpečnosti

⁹⁶ Viz MATEJKA, Ján., GÜTLER, Vojen. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. In: *The Lawyer Quarterly*, 2018, roč. 8, č. 1, str. 44.

⁹⁷ K problematice využití biometrických systému při kontraktaci blíže viz MATEJKA, Ján., GÜTLER, Vojen. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. In: *The Lawyer Quarterly*, 2018, roč. 8, č. 1, str. 38–50.

však představuje identifikace a autentizace zásadně odlišné procesy zpracování. Zatímco správce (zpracovatel), který využívá biometrické údaje toliko k autentizaci, bude zpravidla v nějaké podobě tyto údaje schopen využít i pro identifikaci (*a vice versa*); praktický dopad této změna je tak v mnoha ohledech limitovaný.

Využití biometrických údajů má své legitimní místo napříč systematikou celého právního řádu, a to včetně elektronické kontraktace, resp. přesněji podpisu písemností na základě biometrických metod, kde je však třeba důsledně vycházet z historicky osvědčených a ustálených zásad a principů soukromého práva tak, aby došlo k ideálnímu propojení tradičního a elektronického pojetí podepisování směřující k tolik žádoucímu přirozenému rozvoji práva; to vše s respektem k ochraně soukromí a s důrazem na ochranu před potencialitou zneužití biometrických údajů podepisujících osob.

Celkově vzato tak nutno učinit závěr, že efektivita právní regulace oblasti ochrany biometrických osobních údajů je nedílně svázána se schopností pružně, a především efektivně reagovat na rozvoj informačních a komunikačních technologií, jakož i operativně řešit existující problémy či rozpor jednotlivých dotčených hodnot či práv v této oblasti. Současná právní úprava a ani nařízení GDPR nestanoví konkrétní postup řešení či podrobnější interpretační vodítka existujících právních konfliktů mezi veřejným zájmem (či i zájmem jednotlivců) na práci s biometrickými údaji na straně jedné a řadou dalších práv, včetně práva na ochranu soukromého života, na straně druhé. Normativním základem řešení těchto konfliktů by mělo být především lepší využívání a posilování principu proporcionality; a to včetně náležitého poměrování ochrany základního práva na soukromý život na straně jedné a ochrany veřejného zájmu a práv třetích osob cestou sběru, zpracovávání a uchovávání biometrických údajů na straně druhé. Právě důsledné využití principu proporcionality by mělo vycházet ze zása-

⁹⁸ Nařízení GDPR již pojem „citlivé osobní údaje“ nepoužívá, nahrazuje jej synonymickým pojmem „zvláštní kategorie osobních údajů“; plně však přejímá definiční výčet této kategorie (privilegovaných či citlivých) údajů z dosavadní Směrnice č. 95/46/ES, přičemž k němu výslovně přidává právě genetické a biometrické údaje. Současný ZoÚ však již tyto údaje za citlivé považoval, a tedy by nemělo jít o změnu s významnými praktickými dopady.

dy, že sbírat, zpracovávat a uchovávat lze biometrické údaje jen pro takové účely, které by rozumný člověk považoval za konkrétních okolností za vhodné a nezbytně nutné. Zároveň nutno pamatovat na to, že biometrické údaje mají ve srovnání s jinými osobními údaji svá rizika, představují totiž jedinou kategorii osobních údajů, jež (až na výjimky) nelze po dobu života člověka, jakkoliv změnit, jsou tedy zranitelné a v mnoha ohledech zneužitelné, nezřídka pak zcela nevratně. Nutno tak trvat i na důsledné aplikaci všech souvisejících právních i technologických záruk proti zneužití této privilegované kategorie osobních údajů i současné existence jasného právního titulu pro jejich zpracování; to vše se zřetelem na právní rámec veřejnoprávní regulace a se zřetelem k ochraně lidských práv, kde, jak ostatně trefně poznamenal V. Güttler,⁹⁹ na vedoucím místě nutně stojí ochrana základního práva na lidskou důstojnost, tedy práva, k jehož naplnění prakticky téměř všechna ostatní lidská práva přímo či nepřímo směřují.

6. SEZNAM LITERATURY

6.1 ODBORNÉ KNIHY A ČLÁNKY

[1] ČERMÁK, Karel ml. Elektronický podpis: pohled soukromoprávní. In: *Bulletin advokacie*, roč. 2002, č. 11, str. 64-77.

[2] GÜTTLER, Vojen, MATEJKA, Ján. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. In: *Právník*, 2016, roč. 155, č. 12, s. 1055.

[3] HLAVNIČKA, Jan, ČMEJLA, Roman, TYKALOVÁ, Tereza, ŠONKA, Karel, RŮŽIČKA, Evžen, RUSZ, Jan. Automated analysis of connected speech reveals early biomarkers of Parkinson's disease in patients with rapid eye movement sleep behaviour disorder. *Scientific Reports*, 2017, roč. 7, č. 12. doi:10.1038/s41598-017-00047-5. Dostupné z: <<https://www.nature.com/articles/s41598-017-00047-5>> .

⁹⁹ Güttler, V. in GÜTTLER, Vojen, MATEJKA, Ján. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. In: *Právník*, 2016, roč. 155, č. 12, s. 1055.

- [4] JENKINS, Jeffrey, SWEET, Charles, SWEET, James, MOEL, Steven, SZU, Harold. Authentication, privacy, security can exploit brainwave by biomarker. *Proceedings Volume 9118, Independent Component Analyses, Compressive Sampling, Wavelets, Neural Net, Biosystems, and Nanoengineering XII*; 91180U (2014); doi: 10.1117/12.2051323. Dostupné z: <<https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9118/1/Authentication-privacy-security-can-exploit-brainwave-by-biomarker/10.1117/12.2051323.short?SSO=1>>.
- [5] KINDT, Els J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer, 2013, 975 s. ISBN 978-94-007-7521-3.
- [6] KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? In: *Bulletin advokacie*, roč. 2016, č. 12.
- [7] KORBEL, František, MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. In: *Bulletin advokacie*, roč. 2014, č. 12, str. 31-36.
- [8] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0.
- [9] LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654). Komentář*. 1. vydání, Praha: C. H. Beck, 2014, 2400 s. ISBN 978-80-7400-529-9.
- [10] LI, Ching Chun. Biometrics. In *AccessScience* [online]. 2014 [cit. 2017-10-16]. Dostupné z: <<https://doi.org/10.1036/1097-8542.083700>>.
- [11] AZUAJE, Francisco. *Bioinformatics and Biomarker Discovery. "Omic" Data Analysis for Personalized Medicine*. Chichester: John Wiley & Sons, Ltd., 2010, 230 s. ISBN 978-0-470-74460-4.
- [12] MATEJKA, Ján, GÜTTLER, Vojen. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. In: *The Lawyer Quarterly*, 2018, roč. 8, č. 1.
- [13] MATEJKA, Ján. Úprava elektronického podpisu v právním řádu ČR. In: *Právník*, 2001, roč. 140, č. 5, s. 582 – 611.
- [14] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 s. ISBN 978-80-7357-322-5.
- [15] MORDINI, Emilio, TZOVARAS, Dimitros (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. 349 s. ISBN 978-94-007-3891-1.
- [16] POLČÁK, Radim. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*, 2013, č. 10, str. 34-40.
- [17] POLČÁK, Radim. Praxe elektronických dokumentů. In: *Bulletin advokacie*, 2011, č. 7–8.
- [18] ŠÁMAL, Pavel a kol. *Trestní zákoník*. 2. vydání. Praha: C.H.Beck, 2012, 3614 s. ISBN 978-80-7400-428-5.
- [19] VACCA, John R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007, 625 s. ISBN 978-0-7506-7967-1.

[20] WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí, in: Šimíček, Vojtěch, Právo na soukromí. Brno: Muni Press, 2011.

[21] WESTIN, Alan F. *Freedom and Privacy*, Londen: The Bodley Head, 1967, 508 s.

[22] YAMPOLSKIY, Roman V., GOVINDARAJU, Venu. Taxonomy of Behavioural Biometrics. In WNAG, Liang, GENG, Xin (eds.). *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, August 2009. doi:10.4018/978-1-60566-725-6. Dostupné z: <<https://www.igi-global.com/book/behavioral-biometrics-human-identification/99#table-of-contents>>.

6.2 PRÁVNÍ PŘEDPISY, DŮVODOVÉ ZPRÁVY A JUDIKATURA

[23] Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny. Sdělení Ministerstva zahraničních věcí č. 96/2001 Sb.m.s.

[24] 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 (obecné nařízení o ochraně osobních údajů)

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

[26] Nařízení Komise (EU) č. 383/2012 ze dne 4. května 2012, kterým se stanoví technické požadavky týkající se řídičských průkazů, které zahrnují paměťové médium (mikročip).

[27] Nařízení Komise (ES) č. 205/2009 ze dne 16. března 2009, kterým se schvalují změny menšího rozsahu ve specifikaci označení zapsaného do rejstříku chráněných označení původu a chráněných zeměpisných označení (*Riso Nano Vialone Veronese* (CHZO)).

[28] Nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy.

[29] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[30] Směrnice Evropského parlamentu a Rady 2006/126/ES ze dne 20. prosince 2006 o řídičských průkazech (přepřacované znění) (Text s významem pro EHP).

[31] 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.

[32] Usnesení předsednictva České národní rady ze dne 16. prosince 1992 č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

[33] Zákon č. 263/2016 Sb., atomový zákon, v platném znění.

[34] Zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů, v platném znění.

[35] Zákon č. 89/2012 Sb., občanský zákoník, v platném znění.

- [36] Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji a o změně některých zákonů, v platném znění.
- [37] Zákon č. 40/2009 Sb., trestní zákoník, v platném znění.
- [38] Zákon č. 273/2008 Sb., o Policii České republiky, v platném znění.
- [39] Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.
- [40] Zákon č. 493/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
- [41] Zákon č. 221/2003 Sb., o dočasné ochraně cizinců, v platném znění.
- [42] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.
- [43] Zákon č. 329/1999 Sb., o cestovních dokladech, v platném znění.
- [44] Zákon č. 326/1999 Sb. o pobytu cizinců na území České republiky a o změně některých zákonů.
- [45] Zákon č. 325/1999 Sb., o azylu, v platném znění.
- [46] Zákon č. 269/1994 Sb., o Rejstříku trestů, v platném znění.
- [47] Zákon č. 246/1992 Sb., na ochranu zvířat proti týrání, v platném znění.
- [48] Zákon č. 563/1991 Sb., o účetnictví, v platném znění.
- [49] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), v platném znění.
- [50] Vyhláška č. 400/2011 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech, v platném znění.
- [51] Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu.
- [52] Vyhláška č. 88/2011 Sb., o technických podmínkách a postupu při pořizování biometrických údajů a podpisu cizince pro účely vydání průkazu o povolení k pobytu, v platném znění.
- [53] Vyhláška č. 415/2006 Sb., kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu.
- [54] Důvodová zpráva k zákonu č. 263/2016 Sb., Atomový zákon.
- [55] Důvodová zpráva k zákonu č. 186/2016 Sb. o hazardních hrách.
- [56] Důvodová zpráva k zákonu č. 150/2016 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů, a zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
- [57] Důvodová zpráva k zákonu č. 304/2008 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a některé zákony.

[58] Důvodová zpráva k zákonu č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.

[59] Důvodová zpráva k zákonu č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

[60] Rozhodnutí Soudního Dvora EU ve věci C-434/16 Peter Nowak proti Data Protection Commissioner ze dne 20. 12. 2017.

[61] Rozsudek ESLP ze dne 2. září 2010, stíž. č. 35623/05 ve věci Uzun proti Německu.

[62] Nález Ústavního soudu ze dne 12. 10. 1994 č. Pl. 4/94 (Anonymní svědek).

6.3 DALŠÍ PRAMENY

[63] Article 29 – Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies. In: *Evropská komise* [online]. 27. 4. 2012 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> .

[64] Article 29 Data Protection Working Party. Opinion No. 1/2012 on the data protection reform proposals. *European Commission* [online]. 23. 3. 2012 [vid. 2017-12-08]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf> .

[65] Article 29 – Data Protection Working Party. Opinion 4/2007 on the concept of personal data. In: *Evropská komise* [online]. 20. 6. 2007 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> .

[66] Article 29 – Data Protection Working Party. Working document on biometrics. In: *Evropská komise* [online]. 1. 8. 2003 [cit. 2017-10-16]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf> .

[67] International standard ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics. Second edition 2017-02. In: *International Organization for Standardization* [online]. 2017 [cit. 2017-10-16]. Dostupné z: <<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>> .

[68] Metodický pokyn Ministerstva vnitra č.j. SC - 243/2006 ze dne 6. září 2006 k postupu obecních úřadů obcí s rozšířenou působností při zpracovávání žádostí a vydávání cestovních pasů se strojově čitelnými údaji a s nosičem dat s biometrickými údaji.

[69] Pracovní skupina podle článku 29. Vodítka k k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679. *Úřad na ochranu osobních údajů* [online]. 3. 10. 2017 [vid. 2017-12-08]. Dostupné z: <https://www.uouu.cz/assets/File.ashx?id_org=200144&id_dokumenty=30197> .

[70] Směrnice Ministerstva vnitra k zákonu č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, zákonu č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a zákonu č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), ve znění pozdějších předpisů.

[71] Sněmovní tisk č. 1059/0 ze dne 21. 3. 2017, vládní návrh zákona o platebním styku. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [cit. 2017-10-16]. Dostupné z: <<http://www.psp.cz/sqw/historie.sqw?o=7&t=1059>> .

[72] Sněmovní tisk č. 973/0 ze dne 29. 11. 2016, vládní návrh zákona, kterým se mění zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [cit. 2017-10-16]. Dostupné z: <<http://www.psp.cz/sqw/historie.sqw?t=973>> .

[73] Standards catalogue – ISO/IEC JTC 1/SC 37 – Biometrics. In: *International Organization for Standardization* [online]. 2017 [cit. 2017-10-16]. Dostupné z: <<https://www.iso.org/committee/313770/x/catalogue/>> .

Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).
