K OTÁZKÁM NĚKTERÝCH ZÁKLADNÍCH LIDSKÝCH PRÁV A SVOBOD V SOUVISLOSTI S PRÁVNÍ OCHRANOU BIOMETRICKÝCH ÚDAJŮ

Vojen Güttler* – Ján Matejka**

Abstract: *Biometrické údaje představují zvláštní a vysoce privilegovanou kategorii citlivých osobních údajů. Jejich použití je tak silně limitováno zákonem, a to z celé řady důvodů. Typickým důvodem je zde možný konflikt mezi veřejným zájmem (či i zájmem jednotlivců) na práci s biometrickými údaji na straně jedné a základním právem, zejména na ochranu soukromého života, na straně druhé. Zde je možnou metodou řešení test proporcionality. 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; veřejnoprávním instrumentem k omezení rizik je zde však pouze rámcová úprava zákonem č. 101/2000 Sb., o ochraně osobních údajů. Jakkoliv kolem právní kvalifikace a samotného režimu biometrických údajů panují některé pochybnosti, je zřejmé, že řešení lze nalézt – co do interpretace – zejména v rovině ústavněprávní, případně na úrovni práva Evropské unie. Je nutno lépe využívat princip proporcionality, posílit záruky proti zneužití biometrických údajů, rozvíjet opatření preventivní a důsledněji analyzovat aktuální otázky veřejnoprávních titulů k nakládání s těmito údaji, jakož i souvisejících bezpečnostních, technologických a právních aspektů předmětné problematiky. Zůstává tak otázkou, zda nenastal čas na vypracování zásad právních pravidel užívání a ochrany biometrických údajů, včetně popularizace či katalogizace jejich potenciální zranitelnosti. Základem by měl být právní rámec souvisejících základních práv, v němž by mělo stát na prvním místě základní právo na lidskou důstojnost.*

Klíčová slova: *biometrické údaje, citlivé osobní údaje, soukromý život, důstojný život, princip proporcionality*

ÚVOD

Existuje jen velmi málo oblastí platné právní úpravy, jež mohou být navzdory své relativní novosti charakterizovány vysokou mírou dynamiky a relativní stability zároveň, a to současně s výrazným prvkem diskontinuity. Pokud se zamyslíme nad historií, podstatou a relativní dynamikou právní regulace ochrany osobních údajů člověka, patrně zjistíme, že si takovou charakteristiku v mnoha ohledech zaslouží. Uvedené pak logicky vede k potřebě podstatně upravit teoretická, případně i paradigmatická východiska, na kterých taková úprava spočívá; za tímto účelem musíme především pochopit samotnou podstatu a účel takové regulace, kde je nutno se do jisté míry vymanit z existujících právních, sociologických či ekonomických perspektiv a vysvětlit podstatu jejich dynamiky s tradičními konstrukty.[1]

S ohledem na výše uvedené lze považovat za nesporné, a to zcela ve shodě s jinými autory,[2] že žijeme v době převratných změn a vzniku nových paradigmat, která jsou

* JUDr. Vojen Güttler, Ústav státu a práva AV ČR, v. v. i. Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-269105 s názvem *Biometrické údaje a jejich zvláštní právní ochrana* (*Biometric Data and Their Specific Legal Protection*). E-mail: ilaw@ilaw.cas.cz.

** JUDr. Ján Matejka, Ph.D., Ústav státu a práva AV ČR, v. v. i. Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-269105 s názvem *Biometrické údaje a jejich zvláštní právní ochrana* (*Biometric Data and Their Specific Legal Protection*). E-mail: matejka@ilaw.cas.cz.

1 GIDDENS, Anthony. *Důsledky modernity*. Praha: SLON, 2003, s. 22.

podmíněna nejenom technologickou, ale také sociokulturní a socioekonomickou realitou. Úkolem práva, případně jeho aplikační praxe, je především dosáhnout stavu, kdy tradice a potřeba inovace mohou dlouhodobě koexistovat ve stabilní rovnováze. Za tímto účelem jsou obvykle přijímána určitá pravidla, včetně pravidel právních; proto se o právu hovoří jako o jednom ze společenských normativních systémů (jako je náboženství, morálka či ostatní zvyklosti).[3] Tato koncepce se tak logicky odráží i v právní vědě, jelikož zachycuje nejmodernější společenská východiska a další determinanty vývoje. Pokud se pokusíme stručně analyzovat vývoj této novodobé právní úpravy, zjistíme, že kromě obecných pilířů této úpravy, zmíněných v mezinárodních úmluvách (např. Úmluva č. 108 Rady Evropy), byla normativním základem české právní úpravy především směrnice č. 95/46/ES, která byla navzdory svým jasným cílům i relativně konkrétním normativním ustanovením do národních právních řádů jednotlivých členských států transponována v různé podobě, stejně se různil i výklad národních dozorových orgánů či soudů. U nás se tak stalo konkrétně zákonem č. 101/2000 Sb., o ochraně osobních údajů, který byl navzdory tomu, že zákonodárce převzal téměř doslovně znění směrnice, následně více než dvacetkrát novelizován.

Právě odlišnosti v národních úpravách členských států EU, jakož i rozdíly v jejich správní a soudní praxi, pak vedly k výrazné dichotomii v právním režimu mezi konkrétní národní úpravou a očekávanou úpravou v právu EU, respektive implementovanou úpravou v národních státech. V důsledku toho tak vznikaly komplikace[4] vyplývající z nepředvídatelnosti této odlišně harmonizované úpravy, přičemž sílilo volání po nové právní regulaci ve formě přímo aplikovatelného nařízení EU, jakož i po jasných principech a mechanismech spolupráce dozorových úřadů, které by měly vést k jednotnému či jednotnějšímu výkladu[5] této dynamické oblasti. Z důvodu zastaralosti současné úpravy, zejména pak s přihlédnutím k rozvoji technologií a dále komplikovanosti některých právních institutů této úpravy, které znesnadňují volný pohyb a zpracování informací, bylo přijato Nařízení Evropského parlamentu a Rady č. 2016/679, Obecné nařízení o ochraně osobních údajů (tzv. *General Data Protection Regulation*, zkráceně GDPR), které bylo publikováno dne 27. dubna 2016 a vstoupí v účinnost ke dni 25. května 2018. Spolu s ním byla přijata i tzv. trestněprávní směrnice týkající se zpracování osobních údajů při zajišťování veřejné či státní bezpečnosti[6] a směrnice o používání jmenné evidence cestujících leteckou dopravou (tzv. PNR).[7]

---

2 Srov. HURDÍK, Jan. *Institucionální pilíře soukromého práva v dynamice vývoje společnosti*. Praha: C. H. Beck, 2007, s. VI.

3 LAVICKÝ, Petr. Kritické poznámky ke koncepci návrhu občanského zákoníku. *Právní rozhledy*. 2007, č. 23, s. 849. Replika ELIÁŠ, Karel. Rekodifikace občanského práva v postmoderní době. *Právní rozhledy*. 2008, č. 1, s. 3.

4 V tomto ohledu je např. běžné, že v jednom z národních států lze totožné zpracování dat provádět bez souhlasu dotčených osob a bez nutnosti registrace zpracování u tamějšího dozorového úřadu, zatímco v jiném státě jsou dle tamního výkladu souhlas a registrace zcela nezbytné, navíc pod významnou sankcí za správní delikt.

5 K tomu srovnej čl. 60–67 obecného nařízení o ochraně osobních údajů.

6 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.

7 Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

Obecné nařízení o ochraně osobních údajů se tak nově uplatní přímo, a to ve všech členských státech Evropské unie. Má větší právní sílu než vnitrostátní předpis. Pokud by proto spolu byly v konfliktu, např. český zákon by uváděl, že zabezpečení osobních údajů v určitém sektoru může být nižší, než jak je tomu podle nařízení, přednostně bude aplikováno právě evropské nařízení. I tato skutečnost samozřejmě přináší otázku, jaký bude další osud českého zákona o ochraně osobních údajů, respektive jaký bude mít nařízení dopad do právního řádu jako takového, neboť určité aspekty některých zpracování dat v daném sektoru jsou upraveny v řadě dalších právních předpisů.[8]

Z pohledu aktuálně platného zákona o ochraně osobních údajů je tak nutno konstatovat, že podstatná část jeho ustanovení je novým nařízením překonána a nebude důvodu, aby je případný vnitrostátní zákon nadále obsahoval. Nařízení však obsahuje část týkající se postavení a kompetencí dozorového orgánu i některé procesní aspekty jeho postupu, které nejsou natolik konkrétní, aby mohly v plném rozsahu nahradit úpravu dozoru v zákoně o ochraně osobních údajů a ve vnitrostátních procesních předpisech.[9] Stejně tak nařízení na řadě míst členským státům ukládá nebo umožňuje, aby určitý aspekt upravily detailněji nebo upřesnily.[10] V tomto ohledu lze tedy očekávat patrně nejvýznamnější novelizace této oblasti regulace od jejího vzniku, a to ve smyslu postavení a faktické realizace některých kompetencí dozorového orgánu, případně sektorové úpravy zpracování osobních údajů tam, kde to s ohledem na obecné nařízení a na jiné vnitrostátní předpisy bude nezbytné (jak je tomu např. již dnes v ustanovení § 5 odst. 5 až 9 zákona č. 480/2004 Sb., o některých službách informační společnosti, upravujícím podmínky pro adresný marketing provozovaný prostřednictvím provozovatele poštovních služeb). Pro novou koncepci české právní úpravy tak bude zejména nutné identifikování případných problematických bodů, tzn. míst, kde je současná úprava v rozporu s nařízením, adaptace českých předpisů na nový právní režim, jakož i uvážlivá a rozumná koncepce nepopírající klíčové principy předvídatelnosti správního rozhodování, právní jistoty a proporcionality.

Takovéto koncepční a obecné úvahy jsou však doménou právní politiky, případně legislativy, výrazně přesahují jak limitovaný rozsah tohoto článku, tak i samotné možnosti obou jeho spoluautorů, kteří se zaměří zejména na ty aktuální aspekty právní úpravy, jež se týkají problematiky biometrických, případně genetických údajů; ty i předmětné nařízení zařazuje do tzv. zvláštní kategorie osobních údajů, pro jejichž zpracování platí přísnější režim. Z pohledu českého práva se však nejedná o nic nového, neboť zákon o ochraně osobních údajů již od roku 2007[11] genetické a biometrické údaje, respektive ty biometrické údaje, které umožňují přímou identifikaci či autentizaci člověka, za citlivé údaje považuje.

---

[8] Jako příklad lze uvést zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), který konkrétně reguluje zpracování údajů v rámci zdravotnické dokumentace, nebo zákon č. 262/2006 Sb., zákoník práce, který samostatným způsobem upravuje řadu zpracování osobních údajů zaměstnanců.

[9] Především zákon č. 500/2004 Sb., správní řád, a zákon č. 255/2012 Sb., o kontrole (kontrolní řád).

[10] Např. čl. 37 odst. 4 obecného nařízení o ochraně osobních údajů členským státům umožňuje, aby povinnost jmenovat pověřence pro ochranu osobních údajů rozšířily i na další kategorie správců a zpracovatelů, než které jsou vymezeny v prvém odstavci tohoto článku.

[11] Definice citlivého údaje byla v českém právu takto rozšířena tzv. schengenskou novelou, tzn. zákonem č. 170/2007 Sb.

Oba spoluautoři však považují za vhodné uvést, že hlavním záměrem, respektive ambicí tohoto počinu je zde především provést analýzu povahy převážně ústavněprávní. Právě analýza tohoto typu předznamenává další rámec možného řešení konkrétních problémů v praxi.

1. BIOMETRIKA ČLOVĚKA, BIOMETRICKÝ ÚDAJ A BIOMETRICKÝ SYSTÉM A ZÁKLADNÍ VÝCHODISKA JEJICH OCHRANY

Pod pojmem biometrika lze s určitými výhradami rozumět techniku či systém, který umožňuje strojovou (elektronickou) identifikaci jednotlivce či umožňuje potvrdit totožnost daného uživatele. Biometrické systémy tak v podstatě představují poznávací systém, zajišťující identifikaci či verifikaci (autentizaci) určitých rysů (vlastností) člověka; ty jsou odvozeny přímo buď od fyziologických údajů, jako jsou např. otisky prstů, rysy tváře, duhovky, sítnice, geometrie ruky (prstu či dlaně), krevního řečiště, oční duhovky, obličeje, vůně těla apod., nebo od chování jednotlivce, kde hovoříme o tzv. behaviorálních údajích, jako je např. charakteristika hlasu, písma, podpisu, dynamika psaní na klávesnici aj. Klíčovým pojmem je zde tedy identifikace na základě biometrické charakteristiky lidského těla, včetně konkrétní či presumované charakteristiky jeho projevů (tzv. behaviorální charakteristika), kde osobu rozlišujeme buď podle toho, jak fyzicky vypadá, jak se sociálně chová, či jaké konkrétní role vykonává (profil). Jde tak o přístup k identifikaci osoby podle jejích fyzických, biologických, genetických či behaviorálních nebo jiných obdobných charakteristik, kde je nutno v závislosti na čase rozlišovat nepřeberné spektrum souvisejících markantů (tj. dílčích znaků či významných příznaků a specifických vlastností těchto charakteristik). Za účelem takové identifikace můžeme využívat nejrůznější metody, postupy i algoritmy, včetně souvisejících prvků katalogizace a indexace, které zjednodušeně můžeme nazývat biometrickými systémy.

V tomto ohledu slouží biometrické systémy dvěma hlavním účelům: na jedné straně k identifikaci, na druhé straně k verifikaci (autentizaci) osoby.[12] Pojem biometrický údaj lze chápat jako svého druhu základní stavební jednotku biometrického systému. Legální definici biometrických údajů české právo jako takové neobsahuje. Lze ji nalézt až v novém obecném nařízení na ochranu osobních údajů. V čl. 4 odst. 14 jsou biometrické údaje definovány jako „*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*“. Ani směrnice 95/46/ES pojem biometrického údaje nezná. Jako výkladové pravidlo se v tomto směru používala definice formulovaná Pracovní skupinou pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů dle čl. 29 směrnice 95/46/ES. Podle této definice jsou biometrickými údaji „*biologické vlastnosti, fyziologické charakteristiky, živoucí rysy nebo opakovatelné akce, pokud jsou tyto vlastnosti a/nebo funkce*

[12] Verifikace nesměřuje přímo k identitě osoby, pouze určuje, zda se dvě data týkají téže osoby. Jestliže identifikační funkce vyžaduje srovnání jednoho vůči mnoha („*one to many*“), verifikační funkce vyžaduje srovnání „*one to one*“. K tomu více viz např. EVROPSKÁ KOMISE. *Working document on biometrics* [online]. 20. 6. 2007, Article 29 WP, č. 80. [2016-09-26]. Dostupné z: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf>.

jednak jedinečné pro danou osobu, tak i měřitelné, a to i v případě, že schémata používaná v praxi pro jejich technické měření zahrnují určitou míru pravděpodobnosti".[13]

Biometrické údaje jsou unikátní a zpravidla představují fyziologickou (fyzickou či behaviorální) charakteristiku, jíž se jednotlivé osoby od sebe rozlišují. Klíčovým faktorem je zde zejména možnost identifikace osoby s extrémně vysokou mírou její spolehlivosti podle jejích fyzických, biologických nebo genetických charakteristik.

Samozřejmě osobu lze identifikovat i na základě celé řady jiných (standardních), byť mnohdy i obdobných kritérií, např. podle toho, jak tato osoba fyzicky vypadá, jak se sociálně chová, v jaké je interakci se svým okolím, jaké má jméno, jak ji nazývají ostatní (příjmením, jménem, přezdívkou) v rodinném nebo pracovním prostředí (kde zastává určitou funkci, vykonává konkrétní roli) a mezi přáteli. Osobu zároveň můžeme identifikovat podle toho, co má, zná nebo dělá apod. Z hlediska medicínského a kriminalistického je osoba identifikovatelná i pomocí určitých prodělaných nemocí, zranění a lékařských zásahů a jejich následků (stav chrupu, různé zlomeniny, lékařské zásahy zanechávající typické a neodstranitelné stopy – implantát kostí, kloubů, cév, voperování elektronických prvků jako např. kardiostimulátorů, dalších technických, elektronických přístrojů na zlepšení nebo nahrazení původních biologických funkcí, pooperační jizvy apod.).[14]

S ohledem na identifikační (verifikační) potenciál těchto údajů lze tak považovat – zpravidla – biometrické údaje za osobní údaje ve smyslu platné právní úpravy; to s tím, že tyto údaje mohou představovat zvláštní kategorii citlivých osobních údajů podléhajících zvláštnímu (privilegovanému) zákonnému režimu.[15]

Zatímco osobním údajem tak může být ve smyslu ustanovení § 4 písm. a) zákona o ochraně osobních údajů prakticky jakákoliv informace identifikující konkrétní osobu, ať již stojí relativně samostatně (např. jméno a příjmení), či nikoliv (např. pseudonym používaný fyzickou osobou pro komunikaci v diskusních fórech na internetu, *cookies*[16] atd.), pokud se týká určeného nebo určitelného subjektu údajů, za citlivý osobní údaj lze považovat pouze takový údaj, který buď splňuje konvenční definiční kritéria,[17] nebo jde o takový biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Je tedy zřejmé, že ne každý osobní údaj je současně údajem biometrickým. To plyne ze samé podstaty biometrických údajů a z povahy věci vůbec. Lze ovšem připustit, že někdy může být v konkrétním případě obtížné hranici mezi biometrickým údajem a osobním údajem vůbec najít. Lze však dovozovat, že biometrické údaje jsou začasté

[13] Viz EVROPSKÁ KOMISE. Opinion 4/2007 on the concept of personal data. Article 29 Data Protection Working Party, s. 8 [online]. 20. 6. 2007 [2016-09-26]. Dostupné z: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

[14] K tomu více viz RAK, Roman – MATYÁŠ, Vašek – ŘÍHA, Zdeněk. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Praha: Grada, 2008.

[15] Nutno však rozlišovat biometrické údaje a systémy, jejichž účelem je toliko verifikace uživatele (např. ověření osoby jako toliko člena určité skupiny) a systémy, jejichž účelem je právě a jen identifikace člověka dle jeho fyziologické či behaviorální charakteristiky.

[16] V tomto ohledu je zcela zásadní samotný kontext v podobě existujících informací, které jsou o uživateli dále sbírány a sledovány, včetně míry jejich průběžné anonymizace a zvolené formy užití (viz např. behaviorální reklama apod.). K tomu srovnej ČUHELOVÁ, Mária. Cookies jako osobní údaj? Neumím si představit, jak to bude v praxi fungovat. *Právní rádce.* 2012, č. 12, s. 68.

[17] Tj. jde o 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 sexuálním životě subjektu údajů a genetický údaj subjektu údajů [viz § 4 odst. 2 písm. b) věta první].

i údaji citlivými, byť to neplatí u všech (srovnej citovaný § 4 písm. b zákona o ochraně osobních údajů *in fine*).[18] V této souvislosti je vhodné dodat, že např. biometrické údaje invalidních lidí mohou mít vztah k jejich stavu zdravotnímu. Korelace může být např. mezi papilárami a nemocí, jako je leukémie či hrudní karcinom; obdobně rekognice tváře může prozrazovat rasový či etnický původ.

Problematika rozdílu mezi překrývajícími se množinami osobních údajů a citlivých osobních údajů je však otázkou povýtce definiční; klíčový je však samotný právní režim, tj. způsob, rozsah a limity nakládání s těmito kategoriemi údajů ve vazbě na jejich zákonnost a na ústavní principy a zásady. V tomto ohledu je nutno zmínit zejména dva principy.

V prvé řadě je to princip proporcionality (úměrnosti), jenž platí zejména při zkoumání vztahu mezi biometrickými údaji a základními právy jednotlivce, která jsou použitím biometrických údajů dotčena (jde o „balanční" princip, o „vyvažování" a zkoumání významu užití biometrického údaje ve vztahu k dotčenému základnímu právu v konkrétní věci). Zde je třeba akcentovat tzv. test proporcionality tak, jak jej používá např. Ústavní soud České republiky (srovnej nález ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94, dále Pl. ÚS 15/96, Pl. ÚS 16/98 aj.). Tím se budeme blíže zabývat v části týkající se vztahu práva na soukromý život k ostatním souvisejícím základním právům vůbec.

Dále je třeba zdůraznit princip transparentnosti, který rovněž tvoří podstatný prvek práce s biometrickými údaji. Sběr a použití biometrických údajů musí být jasný, průhledný a musí být dán jejich obhajitelný důvod. To se týká i bezpečného uchovávání biometrických údajů a jeho časového limitu; samo užití biometrických údajů má být přípustné jen tehdy, jestliže by jiná, méně rušivá metoda stejný výsledek přinést nemohla. To vše je třeba podrobovat potřebné a náležité kontrole.

V obecné rovině je však na místě znovu konstatovat, že biometrické osobní údaje začasté představují zvlášť citlivé osobní údaje (§ 4 písm. b zákona o ochraně osobních údajů), kde by měl existovat jen mimořádně závažný veřejný zájem na tom, aby byla ochrana takového osobního biometrického údaje prolomena. V tomto směru lze odkázat i na ust. § 9 zákona o ochraně osobních údajů, který stanoví podmínky, na jejichž splnění je zpracování citlivých údajů vázáno.

V souvislosti s rozvojem nových technologií a jejich možností je třeba připomenout, že problematika biometrických údajů a s tím souvisejících systémů představuje vysoce dynamické průmyslové odvětví, jehož komerční potencialitu a současné či budoucí analytické možnosti neradno podceňovat. Ačkoliv jsou zde jakékoliv predikce mimořádně problematické, zahraniční literatura[19] považuje tzv. druhou generaci biometriky, respektive systémů umožňujících osobnostní identifikaci (tzv. profilování) na bázi dynamiky chování osoby za právně i fakticky vysoce problematickou. Cílem takto navržených systému totiž není toliko identifikace osoby, cílem je „čtení její mysli" a predikce budoucího chování jednotlivce. Druhá generace biometrických údajů je zaměřena na kategorizaci jednotlivců, kde neoprávněná či nespravedlivá selekce může vyústit v diskriminaci; stigmatizace dopadne na jednotlivcovu budoucnost. Je zde tedy otázka, co vše umožní

[18] Tato nejasnost je zachována i v novém obecném nařízení na ochranu osobních údajů, které v čl. 9 stanoví podmínky pro zpracování zvláštních kategorií osobních údajů, které odpovídají českému pojetí citlivých osobních údajů. Bez dalšího tak nemohou být zpracovávány biometrické údaje za účelem jedinečné identifikace fyzické osoby.

[19] CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics.* 2. díl. London: Springer-Verlag, 2013, s. 405–406.

technický pokrok v době příští.[20] Domyšleno do všech možných důsledků, naznačené cíle druhé generace biometriky by popřely samu podstatu svobody jednotlivce a vytvořily by nebezpečnou prioritní roli nejen státu a jeho mocenských orgánů vůči jednotlivcům, nýbrž i významných mimostátních skupin (ekonomických i jiných), jimž by jednotlivec konkurovat nemohl.

2. PRÁVO NA SOUKROMÍ A JEHO VZTAH K OSTATNÍM ZÁKLADNÍM PRÁVŮM SE ZŘETELEM K PRÁVNÍM PROBLÉMŮM BIOMETRICKÝCH SYSTÉMŮ

Úvodem je na místě zdůraznit, že nosným pilířem jakékoliv úvahy tohoto typu je přesvědčení obou autorů tohoto textu o nezadatelnosti, nezcizitelnosti a nezrušitelnosti základních práv jako relativně složitých a jemných kulturních výtvorů vyspělých lidských společností, které bez nadsázky tvoří jediný společný základ právně politického myšlení v současném světě. Konstrukce tohoto článku tak do jisté míry stojí především na náležité ochraně základních (lidských) práv a svobod, zejména základního práva na lidskou důstojnost, byť nelze opomíjet ani dostatečnou právní ochranu biometrických údajů na podústavní úrovni (viz níže). Hlavní metodou zkoumání vztahu mezi biometrickými údaji a základními právy či svobodami jednotlivce – jak již bylo uvedeno výše – je především princip proporcionality a jeho uvážlivé a adekvátní používání.

Pokusíme-li se analyzovat vztah práva na soukromí a ostatních základních práv, musíme vyjít z obecného práva na ochranu soukromého života, neboť – jak je v evropském prostoru zřejmé – to především je sběrem, zpracováním a uchováváním biometrických údajů nutně dotčeno. Toto základní právo na soukromý život upravují v České republice zejména následující předpisy:

- Listina základních práv a svobod v čl. 7
- Úmluva o ochraně lidských práv a základních svobod v čl. 8
- Zákon o ochraně osobních údajů
- Nový občanský zákoník, zejména v § 81 odst. 2 a § 86
- Listina základních práv Evropské unie v čl. 7 (výhradně pokud je uplatňováno právo Unie)

Sběr, zpracovávání a uchovávání biometrických údajů zasahující do základního práva na soukromý život jsou těmito předpisy silně limitovány. Evropské soudy (i Ústavní soud ČR) provádějí třístupňový test, posuzující, zda restrikce týkající se práva na soukromý život jsou ospravedlnitelné. Jde o následující otázky:

a) zda je zásah v souladu se zákonem; zákon má mít určitou kvalitu, má být dostupný, přesný a s předvídatelnými následky; to platí i s ohledem na závažnost a míru zásahu do základního práva (srovnej nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011),
b) zda zásah sledoval legitimní cíl (např. ochranu veřejné bezpečnosti, života, zdraví, majetku třetích osob),
c) zda byl zásah v demokratické společnosti nezbytný (tj. zda existovala naléhavá společenská potřeba takového zásahu).

[20] K tomu viz např. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013.

Tento poslední požadavek vyžaduje provedení analýzy pomocí testu proporcionality. Ta spočívá v následujících kritériích:

a) kritérium vhodnosti zásahu k dosažení daného cíle,
b) kritérium potřebnosti zásahu v porovnání s jinými opatřeními (méně omezujícími) umožňujícími dosažení daného cíle,
c) 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 (blíže srovnej pod bodem 4 níže).

Základní právo na soukromý život zahrnuje mimo jiné právo na informační sebeurčení; jednotlivec má v zásadě sám právo rozhodnout, které údaje z vlastního soukromého života zpřístupní jiným subjektům. Tu lze odkázat např. na nálezy Ústavního soudu sp. zn. IV. ÚS 23/05 ze dne 17. 7. 2007, I. ÚS 705/06 ze dne 1. 12. 2008 a na rozhodnutí Spolkového ústavního soudu Německa BVerfg GE 65, 1. Tam německý ústavní soud vycházel mj. z judikatury Evropského soudu pro lidská práva, zejména ve věci *Malone v. Spojené království* (rozsudek z 2. 8. 1984, č. 8691/79), který z čl. 8 Úmluvy o ochraně lidských práv a základních svobod právo na informační sebeurčení dovodil.

K zásadnímu významu ochrany základního práva na soukromý život judikoval i Nejvyšší správní soud v rozsudku ze dne 28. 6. 2013 sp. zn. 5 As 1/2011 – 156. Uvedl mj. následující: „*Aby mohla být dána přednost ochraně jiného základního práva nebo svobody před ochranou soukromí, musí se jednat o takovou situaci, kdy jinak si rovná základní práva a svobody jsou v konfliktu, a na základě důkladného zvažování, zda v té které konkrétní situaci je zájem chráněný jiným základním právem a svobodou natolik závažný a natolik ohrožen, že lze svolit k zásahu do soukromí a tedy částečně či úplně omezit základní lidské právo na soukromí nebo soukromý a rodinný život a tedy i lidskou důstojnost.*“[21]

V obecné rovině lze konstatovat, že základní právo na soukromý život (srovnej zejména čl. 7 Listiny základních práv a svobod, čl. 8 Úmluvy o ochraně lidských práv a základních svobod) má dopad natolik široký, že se mnohdy překrývá i s dalšími základními právy upravenými jinými články Listiny, Úmluvy a mezinárodních paktů. Podle uznávané literatury „*ve většině situací Soud* [rozuměj Evropský soud pro lidská práva] *poté věc zkoumá pod specifičtějším článkem, a nikoli čl. 8* [rozuměj Úmluvy], *který je v tomto ohledu obecný*“.[22] Souvislost dále uvedených základních práv, pokud jsou dotčena sběrem, zpracováváním a uchováváním osobních údajů (včetně biometrických údajů), je pak nasnadě.

Která základní práva se tedy nejčastěji překrývají či mohou překrývat se základním právem na soukromý život? Patří sem zejména:

a) Základní právo na lidskou důstojnost,[23] osobní čest a dobrou pověst (jež lze zařadit i do základního práva na soukromý život v širším smyslu).

---

[21] V uvedené věci šlo o připuštění kamerového systému k ochraně bezpečnosti osob a majetku vlastníka objektu a hotelových hostů, o kontrolu vstupů do objektu a o prevenci proti vandalismu.

[22] Srov. KMEC, Jiří – KOSAŘ, David – KRATOCHVÍL, Jan – BOBEK, Michal. *Evropská úmluva o lidských právech. Komentář*. Praha: C. H. Beck, 2012, s. 866.

[23] Viz CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics*. 2. díl. London: Springer-Verlag, 2013, s. 393: Zpráva Rady Evropy označuje integritu těla za aspekt lidské důstojnosti; „*the use of your body*“ jako identifikačního nástroje může porušit to, co je nazýváno naším informačním soukromím. Publikace však dovozuje, že biometrika je „v plenkách“ a existují jen malé znalosti o jejich možných stinných stránkách (*draw-backs*); může být tedy nastartován vývoj s nepředvídatelnými následky.

Sama „lidská důstojnost“ může být totiž sběrem, zpracováváním a uchováváním biometrických údajů dotčena, např. důkladnými osobními prohlídkami a kontrolami, zejména na letištích; to se bude týkat i jiných, dále uvedených základních práv. Ponecháváme stranou, že zdaleka ne každá taková kontrola je nepřijatelným porušením daného základního práva (čl. 7 Listiny, čl. 8 Úmluvy), neboť začasté převáží zájem veřejný či ochrana práv a svobod třetích osob. Pokud jde o ochranu dobré pověsti, tu řadí pod pojem soukromý život i Evropský soud pro lidská práva (srovnej *Pfeifer v. Rakousko*, rozsudek z 15. 11. 2007, č. 12556/03). Kontroly na letištích státními orgány či srovnatelné kontroly jiné jsou mnohdy spojeny s odběrem biometrických údajů např. formou otisků prstů nebo i jinými, invazivnějšími formami (srovnej Evropský soud pro lidská práva, *S. a Marper v. Spojené království*, rozsudek ze 4. 12. 2008, č. 30562/04).[24]

b) Základní právo na ochranu osobních údajů.

Rovněž toto základní právo se nepochybně dotýká soukromého života jednotlivce. Pokud jde o biometrické údaje, tu dochází k jejich sběru či zpracovávání např. již při vydávání osobních průkazů, cestovních dokladů a při jejich kontrole (otisky prstů, fotografie aj.). Uchovávání osobních údajů pak řadí pod ochranu soukromého života i Evropský soud pro lidská práva (srovnej *Amanna v. Švýcarsko*, rozsudek z 16. 2. 2000, č. 27798/95).

c) Základní právo na osobní svobodu (např. při zadržení podezřelého).

Toto základní právo může být ve srovnatelných případech rovněž dotčeno. Může jít např. o krátkodobé zadržení za účelem kontroly totožnosti cestujícího, či i o dlouhodobé zadržení imigrantů úřady daného státu. Kontrola i pomocí biometrických údajů, zvláště u zemí ohrožených přílivem imigrantů, je nasnadě. Jako příklad lze uvést zastavení cestujícího na státní hranici v rámci schengenského prostoru bez uvedení důvodů. Tu však nelze nevidět současný stav, kdy se státy octly uprostřed nového fenoménu a snaží se čelit imigrační vlně i prostředky, jež by byly ještě před krátkou dobou stěží myslitelné. Volání po prolomení schengenského systému či po jeho nové úpravě je nyní v Evropě dosti hlasité.

d) Základní právo na svobodu pohybu.

e) Základní právo na nedotknutelnost obydlí (svoboda domovní).

I toto právo nepochybně souvisí se základním právem na soukromý život a zpravidla se dotýká i ochrany biometrických údajů konkrétního jednotlivce; např. sběr otisků prstů je při domovní prohlídce běžným jevem. V této souvislosti je opět namístě poukázat na rozhodnutí Evropského soudu pro lidská práva ve věci *S. a Marper v. Spojené království*,[25] kde se hovoří o nebezpečí stigmatizace (zejména u mladistvých) v souvislosti s odběrem DNA; uchovávání DNA bez časového limitu může, důsledně vzato, presumpci neviny ovlivnit. Podobný důsledek mohl mít návrh francouzské vlády v roce 2004, aby byly registrovány biometrické údaje těch cizinců, kterým bylo odmítnuto vydání víza; tento případ se však může jevit jako sporný.

[24] Srov. KMEC, Jiří – KOSAŘ, David – KRATOCHVÍL, Jan – BOBEK, Michal. *Evropská úmluva o lidských právech. Komentář*. Praha: C. H. Beck, 2012, s. 871, 884.
[25] Ibidem, s. 916.

f) Základní právo na ochranu listovního tajemství, jiných písemností, záznamů a jiných zpráv.

Zde jde v podstatě o komunikační provoz, kam patří i tzv. e-maily apod. (tím se zabýval např. Evropský soud pro lidská práva ve věci *Coplad v. Spojené království*, rozsudek z 3. 4. 2007, č. 62617/00, či Ústavní soud České republiky ve věci sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 32). Specifické je pořizování zvukového záznamu hlasu; i tu jde nepochybně o biometrický údaj (srovnej Evropský soud pro lidská práva, *P. G. a J. H. v. Spojené království*, rozsudek z 25. 9. 2001, č. 44787/98).

g) Základní právo na svobodu myšlení, svědomí a náboženského vyznání.

Toto právo výrazně vystupuje do popředí právě v poslední době v Evropě, zejména v souvislosti s přílivem imigrantů (mnohdy ilegálních) z muslimských zemí. Ostatně takových osob žilo v některých evropských státech značné množství ještě před imigrační vlnou poslední doby (Spojené království, Francie, Německo). Státy se více či méně brání, poukazují jak na veřejný zájem, tak i na nutnost ochrany práv a svobod třetích osob, zejména vlastních obyvatel. V této souvislosti je namístě zmínit i problémy týkající se tzv. zahalených muslimek, ať již užívají burku, nikáb, čádor, šajlu či hidžáb; burka a nikáb v podstatě znemožňují optickou identifikaci osoby, která má zahalenou postavu i tvář. Tu se nabízí otázka, jak potom řešit nutný sběr (zpracování) biometrických údajů formou automatického rozpoznávání charakteristických rysů (markantů) tváře (tzv. *facial recognition*), ať již pro účely veřejné (kontrola osobních dokladů a zjištění totožnosti), či pro účely soukromé (např. vstup do budovy firmy). V současné době je to zřejmě otázka právní úpravy toho kterého státu.

h) V širším slova smyslu patří do této skupiny i základní právo na zákaz diskriminace.

S ochranou biometrických údajů – jsou-li součástí práva na ochranu osobních údajů a s ochranou základního práva na soukromý život – souvisí jako možný antipod ústavní právo na svobodu projevu a právo na informace (čl. 17 Listiny základních práv a svobod). Tu lze odkázat např. na zákon č. 106/1999 Sb., o svobodném přístupu k informacím; ten stanoví v § 2 odst. 3 (včetně poznámky pod čarou), že zákon se nevztahuje na poskytování osobních údajů a informací podle zvláštního právního předpisu (např. zák. č. 101/2000 Sb., o ochraně osobních údajů). V ustanovení § 8 písm. a téhož zákona ve znění zákona č. 61/2006 Sb. se pak praví, že povinný subjekt poskytne informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje jen v souladu s právními předpisy upravujícími jejich ochranu, tedy mj. v souladu se zákonem o ochraně osobních údajů. Vzdor tomu je však třeba i nadále dovozovat, že základní právo na soukromý život a základní právo na informace nestojí striktně proti sobě, ale vedle sebe. I zde je nutné vycházet z okolností konkrétního případu a v rámci testu proporcionality poměřovat, zda ochrana toho kterého základního práva v daném případě převáží (srovnej nález Ústavního soudu publikovaný pod č. 405/2002 Sb.).

Možné omezení základních práv cestou sběru, zpracovávání a uchovávání biometrických údajů vyžaduje existenci odpovídajících bezpečnostních záruk, které zajišťují, že osobní údaje (zde biometrické údaje) jsou efektivně chráněny před nesprávným použitím a zneužitím. Jde mj. o to, aby byly biometrické údaje využívány ve formě dovolující identifikaci subjektu k účelu, pro který jsou uchovávány, a po dobu ne delší, než takový účel skutečně vyžaduje.

Právní záruky vyžadují, aby národní právo zabránilo takovému užití osobních údajů, které by mohlo být nekonzistentní s garancemi danými čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Národní právo musí zajistit, aby sběr a uchovávání osobních údajů byly relevantní, a nikoli excesivní ve vztahu k účelu, pro který jsou uchovávány, a to ve formě, která dovoluje identifikaci subjektu osobních údajů po dobu ne delší, než vyžaduje účel, pro který jsou osobní údaje uchovávány. Uvedené postuláty vyslovil Evropský soud pro lidská práva v již zmíněné kauze *S. a Marper v. Spojené království*; tu lze však odkázat i na případy další, řešené Evropským soudem pro lidská práva; jde např. o kauzy *Leander v. Švédsko*, rozsudek ze dne 26. 3. 1987, č. 9248181, *Turek v. Slovensko*, rozsudek ze dne 14. 2. 2006, č. 57986/00, či *Gardel v. Francie*, rozsudek ze dne 17. 12. 2009, č. App.16428/05.

Společné prvky (rysy) záruk označuje významná oxfordská studie[26] takto:

a) Specifikace účelu: údaje musí být shromážděny pro specifikovaný, explicitní a legitimní účel.
b) Kvalita údajů: shromážděné údaje by měly být relevantní a nutné k dosažení legitimních účelů, pro které se shromažďují.
c) Sběr údajů: údaje by měly být poskytovány se souhlasem nebo s vědomím subjektů údajů.
d) Upozornění: subjekty údajů by měly být informovány o účelech, pro které se údaje shromažďují, o úřadu povolujícím shromažďování údajů, o tom, zda je zveřejnění povinné či dobrovolné a o konsekvencích jejich neposkytnutí.
e) Limitace užití: údaje by měly být užívány pro původně specifikované účely nebo pro účely, jež jsou s původními účely kompatibilní. Restrikce platí i pro transfer údajů mezi státními orgány a mezi státem a soukromými organizacemi nebo jednotlivci.
f) Bezpečnost: měla by být nastolena odpovídající bezpečnostní opatření, zajišťující bezpečnost, integritu a důvěrnost osobních údajů.
g) Přístup: subjekty údajů by měly mít právo na přístup ke svým osobním údajům obsaženým v databázích.
h) Korekce: subjekty údajů by měly mít právo na aktualizaci a opravu těchto údajů.
i) Nezávislý úřad ochrany údajů: všechny jurisdikce v této studii zajišťují pro nezávislý úřad ochrany údajů právo monitorovat konformitu se zárukami soukromí údajů a právo vyšetřovat stížnosti a jednat o nich.

Oxfordská studie[27] k problematice aktuálních výzev biometrických systémů odkazuje na tři právní věci. Nejdříve rozebírá již citovaný případ *S. a Marper* (Evropský soud pro lidská práva), dále se zabývá případem *Nahon v. Knesset*, řešeným Nejvyšším soudem státu Izrael; Nejvyšší soud sice stížnost pro předčasnost odmítl, leč soudci věc kritizovali a zvažovali, zda je skutečně nezbytné uchovávat biometrické údaje celé izraelské populace v jedné centralizované databázi; šlo o otisky prstů a o komputerizované údaje rysů tváře. Třetí případ posuzovala Ústavní rada Francie; šlo rovněž o otisky prstů a rysy tváře

[26] Viz ERDOS, David et al. *Biometric Identification and Privacy*. Oxford: Oxford Pro Bono Publico, February 2013, která v souhrnné části pod názvem *Safeguards for the Protection of Biometric Data* rozlišuje právní záruky, společné rysy (prvky) záruk (tzn. u více států) a „*challenges to biometric identification schemes*". Dostupné z: <http://www3.law.ox.ac.uk/denning-archive/news/events_files/2013.2_-_Indian_Biometrics_and_Privacy.pdf>.

[27] A to konkrétně v části nazvané *Challenges to biometric identification schemes*.

jako součásti národní databáze sloužící k prevenci krádeže identity; podle názoru Ústavní rady zde však šlo o zásah, který neproporcionálně omezoval právo subjektu na soukromý život.

Biometrické údaje, jejich sběr, zpracovávání a uchovávání sice omezují základní právo na soukromý život (popřípadě i jiná základní práva), na druhé straně však k ochraně jiných základních práv – zvláště ve vztahu k třetím osobám – slouží či mohou sloužit. Sem patří především:

a) základní právo na život,
b) základní právo vlastnit majetek a
c) další základní práva výše uvedená, která jsou u dotčené osoby na jedné straně omezena, leč na druhé straně – jak již bylo uvedeno – jsou (mohou být) tatáž práva ve vztahu k třetím osobám chráněna (např. základní právo na soukromý život, na lidskou důstojnost a další výše uvedená základní práva).

Pokud jde o biometrické údaje sloužící k ochraně základních práv třetích osob, nelze nevidět, že tu může být v některých případech dotčen i zájem veřejný. Veřejný zájem je však pojem širší, neboť zahrnuje zejména ochranu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochranu zdraví a morálky aj. (srovnej např. čl. 8 odst. 2 Úmluvy o ochraně lidských práv a základních svobod). To nejsou základní práva (stát základní práva nemá), leč jde o hodnoty, jež je třeba v rámci testu proporcionality reflektovat a zvažovat, zda převažuje zájem na ochraně určitého základního práva konkrétní osoby (např. práva na soukromý život) nad atributy, jež veřejný zájem – oproti němu – naplňují. Vždy je ovšem třeba vycházet z okolností konkrétního případu, obecný návod tu neexistuje.[28]

3. RIZIKA NAKLÁDÁNÍ S BIOMETRICKÝMI ÚDAJI A JEJICH KVALIFIKACE

Některá (dále uváděná) rizika mohou mít povahu nejen právní, ale i technickou či sociální; někdy je to *promiscue*, nesnadno rozdělitelné.

V prvé řadě je třeba znovu zdůraznit, že biometrické údaje jsou velmi zranitelné již svojí specifickou povahou, neboť jsou unikátní, trvalé a univerzální. Proto je třeba zajistit takovou kontrolu dat, která umožní identifikovat eventuální rizika, a přijmout taková bezpečnostní opatření, jež budou vycházet mj. z testu proporcionality. Ten cílí k nalezení odpovídající úrovně bezpečnostních údajů, umožňujících zhodnocení rizik vztahujících se k zpracování specifického druhu dat a k zavedení specifických opatření korespondujících stupňům zranitelnosti těchto dat. Tu však vyvstává (mj.) problém, neboť česká legislativa sama postrádá konzistentní přístup k biometrickým údajům; jinými slovy, v otázce zpracování biometrických údajů existuje v České republice právní nejistota, čili ne zcela jasný právní stav. Z toho vyplývá sociální potřeba revize komplikovaného a rigidního přístupu k biometrickým údajům, jež jsou začasté údaji citlivými.

Riziko sběru, zpracovávání a uchovávání biometrických údajů v podstatě znamená možnost zneužití biometrických údajů. To se týká zejména základního práva na soukromý

[28] Jako příklad lze uvést masívní kontroly cestujících a jejich i osobní prohlídky na řadě letišť; tu jde začasté o sběr a zpracování jejich biometrických údajů a o zásah do jejich soukromého života a do dalších výše uvedených základních práv (např. do práva na lidskou důstojnost).

život, což je zpravidla riziko nejzávažnější; zneužití biometrických údajů se však může týkat i jiných základních práv, která jsou uvedena v předcházejícím textu. V rámci toho bývají jako klasické příklady uváděny krádež identity, vydírání, ničení osobní reputace či útok na lidskou důstojnost; to může vést jak k újmám osobní povahy, tak i ke škodám charakteru finančního. Nicméně jako zásadní problém se jeví, někdy opticky, někdy skutečně, konflikt mezi níže uvedenými základními právy (zejména právem na soukromý život) na straně jedné a základními právy třetích osob nebo i se zájmem veřejným na straně druhé.[29]

Při úvaze o rizicích spojených s biometrickými údaji obecně – ve snaze minimalizovat jejich dopad – se nelze vyhnout ani existujícím zákonným instrumentům, které k danému cíli směřují. Sem patří zejména zákon o ochraně osobních údajů č. 101/2000 Sb., neboť biometrické údaje jsou zpravidla za osobní údaje považovány. Tu lze odkázat na ustanovení § 13 odst. 1 citovaného zákona, podle něhož správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Podle § 13 odst. 3 uvedeného zákona v rámci opatření podle odst. 1 správce nebo zpracovatel posuzuje rizika týkající se:

a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Uvedené povinnosti tedy předpokládají, že správce musí vytvořit potřebné záruky v oblasti personální, technické (např. zabezpečení místa zpracování biometrických údajů) a – v užším smyslu – v oblasti použití výpočetní techniky vůbec. Systém totiž může být napaden hackery nebo užit neoprávněnými osobami a pro jiné účely, než pro které byl určen. Je tedy zřejmé, že posouzení rizik souvisejících se zpracováním osobních údajů je otázkou vyhodnocení konkrétní situace daným správcem či zpracovatelem, zejména pak zvolených či stanovených prostředků a způsobu zpracování osobních údajů, druhu a rozsahu těchto údajů, ale také třeba specifik, lokality či budovy, v níž ke zpracování dochází.[30]

Způsobů, jak zpracovávat biometrické údaje, je celá řada, avšak naprostá většina z nich s sebou nese nutnost ukládání citlivých osobních údajů, tj. zejména těch, které lidé běžně a zcela záměrně nesdílejí se svým okolím (typicky otisk prstu, obraz sítnice či duhovky oka apod.).[31] To vede k reálným rizikům zneužití takových dat proti jejich původcům (biometrická falzifikace pro neoprávněný přístup, výroba falza důkazů pro soudy, přístup

[29] K tomu srov. bod. 2 *in fine*.
[30] Srov. KUČEROVÁ, Alena – NOVÁKOVÁ, Ludmila – FOLDOVÁ, Vanda – NONNEMANN, František – POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů. Komentář.* Praha: C. H. Beck, 2012, s. 229.
[31] K tomu více viz např. ŠČUREK, R. *Biometrické metody identifikace osob v bezpečnostní praxi.* (Studijní opora pro kombinovanou formu studia). Ostrava: VŠB, 2008.

k choulostivým zdravotním údajům). Proto některé systémy neukládají do databáze obrazové předlohy jednotlivých uživatelů, ale pouze naměřené vzdálenosti jejich obličejových markantů (typicky jde o charakteristické části obličeje – koutky úst, konce očí apod.). Při případném napadení systému tak útočník (typicky hacker) nezískává přístup k fotografiím, ale pouze k maticím číselných dat. I takovéto údaje však nutno považovat za biometrické údaje ve smyslu jejich zákonného režimu (jde o citlivé osobní údaje). V tomto ohledu je nutno odmítnout takové názory odborné literatury,[32] že tato data nepodléhají zákonné regulaci vyplývající ze specifického režimu citlivých osobních údajů.

Rizika zneužití biometrických údajů mohou být eliminována v případech označených jako tzv. zákonná licence. O tom hovoří ust. § 88 a § 89 nového občanského zákoníku, jež podrobněji normují případy, kdy svolení, např. k zásahu do soukromého života, není třeba. Tu však nelze přehlédnout výjimku ze zákonné licence, kterou stanoví ust. § 90 nového občanského zákoníku. Tam se praví, že zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka. Citované ustanovení je tak třeba aplikovat velmi opatrně a vždy náležitě zvažovat okolnosti konkrétního případu.

K některým zvláštním případům práce s biometrickými údaji lze uvést jen následující poznámky:

– otisky prstů patří mezi velmi specifické biometrické údaje, neboť jsou snadno přenositelné a jejich falzifikaci nelze zcela vyloučit; jde např. o přenos otisku prstu ze skla a vytvoření podobného otisku na uchovávané médium do vosku.
– existence tzv. černých listin osob působících potíže – *trouble makers* (např. v obchodech, restauracích) je problematická, neboť se obvykle nejeví proporcionální registrovat všechny zákazníky za účelem eliminace jen některých z nich (např. zpracovávání markantů detailu tváře či otisku prstu za účelem možného vyloučení určitého zákazníka z další kontraktace apod.)
– zcela specifické je riziko užití biometrických údajů vedoucí k možné diskriminaci, jestliže vylučuje ty osoby, které nemohou užívat biometrický systém např. pro své duševní či fyzické vady.

Obtížně katalogizovatelná jsou rizika u tzv. druhé generace biometrických údajů, které tak představují úvahu spíše *pro futuro*. Směřuje totiž k identifikaci osoby na bázi jejího chování. Cílem může být snaha „číst lidskou mysl". To však může vést – jak již bylo uvedeno – až ke stigmatizaci, kategorizaci osob, k deindividualizaci, a tím i k jejich diskriminaci (jako příklad lze uvést, že kategorizace osob může zapříčinit, že lidé mohou být individuálně zastaveni na ulici či prohlíženi při kontrole u hraničního přechodu jen proto, že spadají pod určitý „kategorizovaný" profil). Tu je však třeba zdůraznit, že etické požadavky týkající se těchto rizik musí být respektovány – a to nejen u biometrických údajů druhé generace – od samého počátku práce s biometrickými údaji vůbec.

Je tedy zřejmé, že existuje „*značná tenze mezi zpracováváním biometrických údajů druhé generace a principem individuální účasti jednotlivce na takovém procesu*"[33];

[32] Viz např. VALER, T. Biometrie obličeje pro autentizaci osob. *Data Security Management*. 2014, roč. XVIII, č. 2, s. 19.
[33] Srov. CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics*. 2. díl. London: Springer-Verlag, 2013, s. 406, 407.

je nesnadné minimalizovat obecné riziko, že systém může být využit jinými osobami a pro jiné než předvídané účely bez tradiční možnosti individuální participace.

Hodnocení rizik plynoucích ze zákonem daných povinností (např. hraniční kontroly) – celkově i jednotlivě – je značně nesnadné. V prvé řadě je třeba uvést, že systémy a práce s nimi nejsou ještě výrazně rozvinuty; to může ovlivnit i zkoumání proporcionality mezi prací s biometrickými údaji na straně jedné a zásahem do základního práva na soukromý život či do jiného základního práva na straně druhé. Biometrické údaje v podstatě jen reprezentují jistou míru pravděpodobnosti, výsledky práce s nimi tedy absolutizovat nelze. Jak již bylo uvedeno, biometrické údaje jsou jedinečné, s trvalou platností, a tedy velmi zranitelné. K tomu přispívá i právní nejistota v oblasti práce s biometrickými údaji, neboť právní pravidla zde dostatečně jasná nejsou.

Hodnotíme-li rizika spojená s biometrickými údaji bližším pohledem a zvažujeme-li potřebné záruky, je namístě poukázat např. i na rezoluci 27. Mezinárodní konference o ochraně dat a soukromí, konané v roce 2005.[34] Konference plédovala mj. pro striktní rozlišení mezi biometrickými údaji sbíranými a uchovávanými pro účely veřejné (např. hraniční kontroly) na bázi zákonné povinnosti a pro účely smluvní na bázi konsenzu; míra a závažnost rizika z hlediska veřejného zájmu se tu jeví být zřejmá.

Nabízí se i další aspekt, umožňující hodnocení rizika toho kterého biometrického údaje, jenž má být použit. Jde o volbu mezi biometrickými údaji, jež zanechávají stopy (např. vzorky DNA, otisky prstů), a biometrickými údaji, které to nečiní (např. duhovka). Tam je riziko zásahu do soukromého života v zásadě menší. Vždy je ovšem věcí konkrétního případu, který biometrický údaj lze vůbec reálně použít jako adekvátní. Zcela specifický biometrický údaj je pak lidský obličej (respektive přesněji samotná geometrie obličeje); ten má povahu veřejné informace a v jeho nahodilém či příležitostném rozpoznání tedy patrně nespočívá žádné riziko vyvolávající možné zneužití osobních identifikátorů proti konkrétní osobě. Zcela jiná je však situace, kdy je takové rozpoznávání realizováno automatizovaně, sofistikovanou technologií, za účelem další indexace a katalogizace údajů o člověku s tím, že potencialita celkových výsledných efektů takto zpracovávaných údajů není a s ohledem na současný vývoj ani nemůže být v době tohoto zpracování známa.[35]

Zvláštní opatrnost je přirozeně třeba mít u těch biometrických údajů, jež jsou již svojí povahou výrazně invazivní a rušivé, protože přinášejí informace např. o zdravotním stavu či o rasovém nebo etnickém původu jednotlivce. Ostatně, to jsou data, jež považuje za citlivý osobní údaj i zákon o ochraně osobních údajů v ust. § 4 písm. b).

---

[34] Ibidem, s. 399.

[35] Příkladem pokročilého zařízení pro snímání geometrie obličeje je např. technologie označovaná jako *Broadway 3D* ruské společnosti Artec. Dle tvrzení výrobce je to první zařízení schopné identifikovat osobu srovnatelnou rychlostí, jakou se lidé poznávají mezi sebou (cca jedna sekunda). Zařízení je složeno ze dvou částí – čtečky (kamery) a výpočetní jednotky. Čtečka při výskytu procházející osoby v záběru kamery v rychlých intervalech promítá na obličej přesně definovaný vzor. U procházející osoby pak snímá body promítaného vzoru a výpočetní jednotka pak vyhodnocuje jejich změnu polohy v závislosti na čase, což ve výsledku vede k identifikaci. Speciální algoritmus výrobce dovede vyhodnotit absenci jemné mimiky v obličeji a na základě toho provést identifikaci. Na trhu existuje také řada softwarových nástrojů, které umožňují využít pro 3D autentizaci běžné kamery. K tomu více VALER, T. Biometrie obličeje pro autentizaci osob. *Data Security Management*. 2014, roč. XVIII, č. 2, s. 18.

4. MOŽNÁ ŘEŠENÍ V ÚSTAVNĚPRÁVNÍ ROVINĚ

Řešení věci z ústavněprávního pohledu nevyžaduje – po našem soudu – změnu Ústavy České republiky. Existující problémy, popřípadě rizika, lze překlenout, byť mnohdy obtížně, na bázi platné Ústavy a ústavního pořádku vůbec. Ústavní pořádek tvoří – kromě Ústavy – Listina základních práv a svobod a další zákony, uvedené v čl. 112 odst. 1 Ústavy. Ústavu je však třeba vykládat jako celek, takže s dikcí čl. 112 odst. 1 nevystačíme.[36] Ústavní soud ČR již řadu let akcentuje ústavní význam mezinárodních závazků, zejména vyhlášených a ratifikovaných mezinárodních smluv ve smyslu čl. 10 Ústavy. Tu se lze opřít zejména o čl. 1 odst. 2 Ústavy, podle něhož Česká republika dodržuje závazky, které pro ni vyplývají z mezinárodního práva; takové závazky mají tedy současně povahu ústavněprávní. Tu lze – na příklad – poukázat na povinnosti založené Úmluvou o ochraně lidských práv a základních svobod, Mezinárodním paktem o občanských a politických právech a Mezinárodním paktem o hospodářských, sociálních a kulturních právech; to jsou právě smlouvy podle čl. 10 Ústavy.

Při řešení existujících problémů a rizik můžeme, zjednodušeně řečeno, vycházet zejména z Listiny základních práv a svobod a z mezinárodních dokumentů o ochraně lidských práv a základních svobod. V podstatě půjde, jak již bylo uvedeno výše, o posouzení vztahu mezi shromažďováním, zpracováváním a uchováváním biometrických údajů na straně jedné a ochranou základního práva na soukromý život a souvisejících základních práv na straně druhé. Tu se ustáleně pracuje s testem proporcionality. Ten spočívá – jak již bylo stručněji vyjádřeno – v následujících fázích – kritériích.

Prvním je kritérium vhodnosti, tj. odpověď na otázku, zda institut omezující určité základní právo umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva). Druhým kritériem poměřování základních práv a svobod je kritérium potřebnosti spočívající v porovnávání legislativního prostředku omezujícího základní právo, respektive svobodu s jinými opatřeními umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod. Třetím kritériem je porovnání závažnosti obou v kolizi stojících základních práv. Tato základní práva jsou *prima facie* rovnocenná.

Porovnávání závažnosti v kolizi stojících základních práv (po splnění podmínky vhodnosti a potřebnosti) spočívá ve zvažování empirických, systémových, kontextových i hodnotových argumentů. Empirickým argumentem lze chápat faktickou závažnost jevu, jenž je spojen s ochranou určitého základního práva. Systémový argument znamená zvažování smyslu a zařazení dotčeného základního práva či svobody v systému základních práv a svobod. Kontextovým argumentem lze rozumět další negativní dopady omezení jednoho základního práva v důsledku upřednostnění práva jiného. Hodnotový argument představuje zvažování pozitiv v kolizi stojících základních práv vzhledem k akceptované hierarchii hodnot (srovnej nález pléna Ústavního soudu ze dne 12. 10. 1994 sp. zn. Pl. ÚS 4/94).

Vraťme se k problémům řešení stávající právní situace (rizik) na poli zvláštní právní ochrany biometrických údajů. Je nesnadné. Jde především – obecně i v tom kterém konkrétním případě – o možný či skutečný konflikt mezi veřejným zájmem, popřípadě mezi základními právy jednotlivců na ochranu života, zdraví, bezpečnosti a majetku pomocí

[36] Tento názor však není v České republice přijímán obecně.

sběru, zpracovávání a uchovávání biometrických údajů na straně jedné a na ochranu základních práv na osobní svobodu, lidskou důstojnost a soukromý život subjektů údajů (zkoumaných osob) na straně druhé. Tu proti sobě stojí v kolizi dvě skupiny ústavně zakotvených hodnot. Uznávanou metodou řešení takového konfliktu je již zmíněná zásada proporcionality a test proporcionality, o nichž se blíže zmiňujeme na jiném místě tohoto textu.[37]

Při úvaze o existující právní situaci se nelze vyhnout ani právním předpisům Rady Evropy a Evropské unie (srovnej též Úvod), které podrobně upravují ochranu osobních údajů jednotlivých osob, byť se u výše citované Úmluvy č. 108 jedná o ochranu se zřetelem na automatizované zpracování osobních dat. U Úmluvy č. 108 je významné, že takové zpracování tzv. citlivých osobních údajů (prozrazujících rasový původ, politické názory, náboženské nebo jiné přesvědčení, jakož i osobní údaje týkající se zdraví nebo pohlavního života) je vázáno na to, že vnitrostátní právní řád stanoví vhodné záruky (č. 6 citované Úmluvy). Jsou však takové „vhodné záruky" v právním řádu České republiky skutečně a efektivně zakotveny? To je velká otázka.

Při zkoumání současného právního stavu je namístě se zabývat i aspekty běžného (podústavního) práva, byť je přirozeně třeba interpretovat běžné právo pomocí ústavních principů, ne naopak. Jde mj. o již výše citovaný zákon o ochraně osobních údajů.[38] Nicméně i v zákoně o ochraně osobních údajů lze nalézt normy povahy ústavněprávní. Totéž se týká i nového občanského zákoníku a v neposlední řadě též relativně nikoli staré literatury odborné.

Zákon o ochraně osobních údajů zakotvuje i ústavněprávní pravidla chování zejména v ust. § 5 odst. 3 a v ust. § 10.

V ust. § 5 odst. 3 se praví, že provádí-li správce zpracování osobních údajů na základě zvláštního předpisu, je povinen dbát na ochranu soukromého a osobního života subjektu údajů [srovnej též § 5 odst. 2 písm. e) citovaného zák.]. Jde o obecný princip, který vychází již z ust. § 1 zákona a prostupuje celou právní úpravou ochrany osobních údajů.

V souvisejícím ustanovení § 10 citovaného zákona se stanoví, že při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů. Zde zákonodárce zdůrazňuje zvláště lidskou důstojnost, k jejíž ochraně – přímo či nepřímo – směřují téměř všechny ostatní ústavněprávní garance. Komentářová literatura pak uvádí, že každý, kdo zpracovává osobní údaje, by měl, alespoň na základní úrovni, provést test proporcionality, čili posoudit, nakolik je jím prováděné zpracování pro dosažení stanoveného účelu nezbytné, zda je jeho rozsah, množina zpracovávaných údajů, doba jejich uchování atd. účelu adekvátní a zda by jej nebylo možné dosáhnout i méně invazivním způsobem zpracování osobních údajů.[39]

---

[37] Zde lze odkázat i na českou ústavněprávní judikaturu, zejména na rozhodnutí Ústavního soudu sp. zn. Pl. ÚS 4/94, Pl. ÚS 15/96, Pl. ÚS 16/98 a Pl. ÚS 40/08.

[38] Podle Parlamentního institutu Parlamentu ČR je každý biometrický údaj i osobním údajem, pokud je možné jej identifikovat s jeho nositelem a jako takový jej uchovat. Viz PARLAMENTNÍ INSTITUT. *Odpověď na dotazy: Právní úprava biometriky*. Červenec 2014.

[39] Princip proporcionality je tak rozhodujícím faktorem právního přezkumu biometrických systémů podle *Data Protection Authorities* (DPA) v členských státech Evropské unie. Autor (tam Paul de Hert) však upozorňuje, že

Nový občanský zákoník (zákon č. 89/2012 Sb.) se oproti dřívější právní úpravě relativně rozsáhle věnuje ochraně osobnosti člověka. Pro účely tohoto textu je třeba jmenovat obzvláště ustanovení § 81 nového občanského zákoníku. Ten stanoví v odst. 1, že chráněná je osobnost člověka, včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého. V odst. 2 daného ustanovení se pak praví, že ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.

Ústavněprávní – leč i podústavní – aspekty související se zvláštní právní ochranou biometrických údajů nacházíme i v odborné literatuře,[40] jež ukazuje, že ani *case law*, ani existující právní rámec (*framework*) nedávají jasnou odpověď na otázky, které jsou s užíváním biometrických údajů spojeny. Tam uváděný autor (de Hert) se dále zabývá argumentem lidské důstojnosti a zdůrazňuje, že v průběhu „*sběru a zpracování tělesných rysů*" by měla být lidská důstojnost plně respektována. Jiný autor (tam Niels Christian Juul) vychází zejména z doporučení dánského úřadu na ochranu dat; uvádí, že „*privacy impact assessment*" (PIA, nebo také posouzení vlivu na ochranu osobních údajů) zajišťuje rozumnou rovnováhu mezi účelem systému, možnou úrovní identifikace, úschovou osobních dat a rizikem jejich zneužití a krádeže. Biometrické systémy budou užívány tak, aby bylo dosaženo větší úrovně soukromí a aby uživatelé měli zajištěnou možnost svá vlastní data kontrolovat.

Jak již bylo uvedeno výše, je namístě reflektovat i některé souvislosti vyplývající z právní úpravy podústavní. V zákoně o ochraně osobních údajů lze poukázat – a to pouze například – na následující ustanovení.

Ustanovení § 4 písm. b) zákona rozšiřuje – oproti znění předchozímu – definici pojmu „citlivý údaj"; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Komentář k zákonu o ochraně osobních údajů pak správně uvádí, že legální definice pojmu „biometrické údaje" neexistuje.[41] Současně platí, že ne každý biometrický údaj je nutně údajem citlivým. V novém znění definice pojmu „citlivý údaj" se jako podmínka pro zařazení určitého biometrického údaje do kategorie citlivých dat objevuje jednak obecně srozumitelný pojem identifikace (zjištění totožnosti osoby), jednak i méně častý termín autentizace (ověření proklamované identity subjektu, např. jako zaměstnance), který uvedenou definici doplňuje tak, aby byly podchyceny pokud možno všechny případy využití biometriky jako jediného prostředku k určování nebo ověřování identity osob.[42]

Ustanovení § 4 písm. n) citovaného zákona stanoví, že pro účely tohoto zákona se rozumí souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. V souvisejícím ust. § 5 odst. 4 se pak praví, že subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Lze tedy dovozovat, že souhlas subjektu údajů s jejich zpraco-

je nejisté, jak má být princip proporcionality v biometrice aplikován. K tomu více viz CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics*. 2. díl. London: Springer-Verlag, 2013, s. 385.

40 CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics*. 2. díl. London: Springer-Verlag, 2013, s. 385, bod 15.5.3., s. 393, bod 15.7.4., s. 423, bod 16.3.1, 2.

41 Dnes však nutno s pojmem biometrický údaj zacházet ve smyslu jeho režimu dle GDPR (viz výše).

42 Srov. pozn. č. 32, s. 60, 61.

váním je zásadně základním právním titulem uvedeného postupu (podrobnější vymezení pojmu „zpracování osobních údajů" upravuje citovaný zákon ust. § 4 písm. e). Na druhé straně však nelze nevidět, že ust. § 5 odst. 2 zákona zakotvuje pod písm. a)–g) řadu výjimek, které správci umožňují, aby zpracovával osobní údaje i bez souhlasu subjektu údajů. Pokud však jde o citlivé osobní údaje, tu je třeba se dovolat – jak již bylo uvedeno – ust. § 9 zákona o ochraně osobních údajů (*lex specialis*).

Ustanovení § 21 zákona o ochraně osobních údajů konečně upravuje ochranu práv subjektu údajů, jestliže má subjekt za to, že zpracování jeho osobních údajů je v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem. Subjekt údajů může požadovat nápravu od správce (nebo zpracovatele); pokud vznikla v důsledku zpracování osobních údajů subjektu údajů jiná než majetková újma, postupuje se při uplatňování jeho nároku podle zvláštního zákona (nyní nový občanský zákoník ust. § 2956 a § 2957).

Ve výše uvedené odborné literatuře[43] stojí za pozornost mj. následující názory:

– V prvé řadě je třeba zaměřit se na regulátory a operátory (správce či zpracovatele) biometrických údajů; to jsou ve většině případů operátoři, kteří uvádějí systém do chodu. Regulátor je osoba, která potvrzuje účel dat, kategorizaci dat a jejich užití; jasné definice jeho role a odpovědnosti a zajištění vhodné supervize od kompetentních úřadů na ochranu dat jsou tedy nutné.[44]
– Významná je i otázka souhlasu subjektu údajů, pokud nejde o sběr biometrických údajů právně povinných. Teorii konsenzu je třeba více propracovat; subjekt musí znát účel sběru biometrických údajů a identitu kontrolora. Za zmínku stojí i případy, kdy souhlas nemohl být dán dobrovolně, zejména tam, kde byla jasná neshoda mezi subjektem biometrických údajů a kontrolorem.
– Obecně platí, že biometrické údaje by měly být používány jen tehdy, jestliže by jiný, méně rušivý způsob, nepřinesl efekt stejný (pozn.: tento požadavek lze vidět i v souvislosti s již vícekrát zmíněným testem proporcionality).
– Národní úřady na ochranu dat musí být angažovány v právních řízeních proti operátorům, pokud ti nerespektují předpisy na ochranu biometrických údajů; úřady tedy mají vyslechnout stížnosti jednotlivců tvrdících, že byly porušeny jejich svobody a práva ve vztahu k zpracování biometrických údajů.
– Je třeba rozlišovat mezi biometrickými technologiemi podle toho, zda zanechávají stopy, či nikoli a jasně vyjádřit preferenci těch druhých (např. obraz duhovky nebo sítnice).[45]
– Lidská práva logicky vyžadují, aby je vlády chránily i tím, že vytvoří adekvátní zákonný rámec, předvídatelný a přijatelný.
– Subjekt biometrických údajů – ještě předtím, než je zahrnut do systému biometrického řešení – je informován o účelu a rozsahu své registrace; uživatel tedy může vidět a kontrolovat, zda je registrovaná informace správná a korektní.[46]

[43] CAMPISI, Patrizio (ed.). *Security and Privacy in Biometrics*. 2. díl. London: Springer-Verlag, 2013, s. 375, 376.
[44] Ibidem, s. 375, 381, 403.
[45] Ibidem, s. 403.
[46] Ibidem, s. 1, s. 416.

Podle literatury bezpečnost biometrických údajů vyžaduje kladnou odpověď na následující otázky:

„*1. Představuje reálná přidaná hodnota biometrických systémů (‚the added biometry') konečné řešení více či méně spolehlivé a důvěryhodné?*

2. Jsou biometrické údaje zpracovávány a uchovávány bezpečně?

3. Jsou shromažďované biometrické údaje chráněny proti zneužití pro dodatečné účely (‚function creep')?

4. Předchází biometrické řešení nespravedlivé diskriminaci skupin nebo jednotlivců?"[47]

Jestliže uvažujeme o řešení stávající situace na poli zvláštní právní ochrany biometrických údajů, je namístě stručně reprodukovat některé kruciální otázky týkající se zákonných aspektů jejich zpracovávání. Sem patří zejména následující:

a) Právní nejistota co do zpracovávání biometrických údajů.

České právní prostředí je formováno jak legislativou Evropské unie, tak i domácím právem. Pokud jde o Evropskou unii, je třeba poukázat zejména na *General Data Protection Regulation*, jež však všechny problémy neodstranila; jde např. o nejistotu co do přesných hranic, ve kterých lze uvažovat o biometrických údajích, o nejistotu co do speciálních měřítek ve vztahu k zpracovávání biometrických údajů jako zvláštní kategorie aj.[48]

b) Neznámý sociální dopad v České republice.

Toto téma úzce souvisí s otázkou rizik, sběru, zpracovávání a uchovávání biometrických údajů, jíž se podrobněji zabýváme zejména v bodu 3 tohoto textu.

c) Neefektivnost běžné (současné) legislativy.

Stávající legislativa postrádá náležitou a kompletní jasnost; ani dopad a rizika spojená se zpracováváním biometrických údajů zcela jasná nejsou. Není zřejmé, do jakého stupně zajišťuje běžná legislativa potřebnou úroveň ochrany; je ovšem diskusní, jaká úroveň ochrany je žádoucí a jaké zájmy by mohly být reflektovány, aby byly právně respektovány a zajištěny (flexibilně a reaktivně) potřeby a rozhodnutí subjektů biometrických údajů.

d) Problémy s biometrickou autentizací.

Vzhledem ke svým specifikům jsou biometrické údaje zranitelné, neboť – jak již bylo uvedeno – jsou unikátní, trvalé a univerzální. Užívání biometrických údajů, např. jako obecných hesel, vytváří riziko jejich kompromitování bez možnosti takové heslo změnit. Který nástroj biometrické identifikace a forma zpracování však znamenají nejmenší riziko? Existují efektivní metody zmírňující rizika spojená s biometrickou autentizací? Je nutné aplikovat test proporcionality pro specifické kategorie biometrických údajů různými způsoby? To vše přitom vyčerpávající souhrn problémů ještě nepředstavuje.[49]

---

[47] Ibidem, s. 1, s. 416.

[48] Je však pochopitelně otázkou, zda lze takové přesné hranice *a priori* vůbec stanovit. Odpověď na tuto otázku se odvíjí od stále se zdokonalujících metod datové analýzy a samozřejmě od okolností případného konkrétního případu.

[49] Existují specifická technologická řešení (PET – *Privacy Enhancing Technologies*), která umožňují například odběr vzorku biometrického údaje (např. bazálního stěru) a následné zpracování pouze jeho části a vymazání původního údaje. Jde tak o biometrický údaj, který ztrácí část své vypovídací hodnoty. Otázkou je, zda a do jaké míry pak zůstává biometrickým údajem.

ZÁVĚR

S ohledem na shora uvedené je třeba konstatovat, že obdobně jako u ostatních dynamicky se rozvíjejících oblastí práva[50] samotné technologické změny, jakož i náchylnost k právním a jiným rizikům nakládání s biometrickými údaji, nezasahují do obsahu dosavadních právních vztahů a jejich existujících struktur natolik významně, že by mohlo dojít k narušení samotné podstaty fungování těchto tradičních právních konstrukcí. Je však zjevné, že tyto změny generují normativně značně obtížně řešitelné právní problémy v celé řadě oblastí a institutů týkajících se ochrany soukromí; jejich řešení lze hledat v dosavadních ústavněprávních zásadách a na ně navazujících interpretačních metodách.

V tomto ohledu se sluší připomenout, že oba spoluautoři tohoto textu jsou si vědomi toho, že jednotlivé části jejich textu se nezřídka dotýkají jak oblasti práva soukromého, tak i práva veřejného. Taková situace může někdy vyvolávat dojem směšování obou sfér. Tu však nelze nevidět, že sama relevantní ústavněprávní judikatura formou nálezu pléna Ústavního soudu ČR vyslovila, že právní řád v ČR je sice založen na dualismu veřejného a soukromého práva, leč v současné době není soukromé a veřejné právo odděleno „čínskou zdí"; dochází tedy k častějšímu a užšímu prolínání, kombinaci i vzájemnému intenzivnímu ovlivňování prvků soukromoprávních a veřejnoprávních.[51] S takovou situací je třeba počítat i v době budoucí.

Normativním základem řešení by tak mělo být především lepší využívání a posilování principu proporcionality; to včetně náležitého poměřování 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. Zvláštní právní ochrana biometrických údajů a oproti tomu ochrana zejména základního práva na soukromý život (a na související základní práva) jsou zpravidla spojité nádoby; stěží je lze zkoumat nezávisle na sobě.

Právě využití principu proporcionality by mělo vycházet ze zásady, 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. To lze označit jako test rozumnosti a vhodnosti svého druhu; ten by měl vycházet ze čtyř kritérií, která souvisejí či navazují na ústavní test proporcionality (srovnej výše). Podle těchto kritérií před zahájením shromažďování či zpracovávání biometrických údajů by mělo být zkoumáno a potvrzeno, že shromažďování, spravování a zpracování biometrických údajů jednotlivců je skutečně nezbytné k dosažení vymezeného cíle nebo potřeby, že je nejefektivnějším způsobem, jak dosáhnout daný cíl nebo potřebu, že ztráta soukromí spojená s konkrétní metodou zpracování konkrétního biometrického údaje je proporcionální (že je tedy zajištěna určitá úměrnost zásahu do soukromí ve srovnání s přínosem, který takové zpracování biometrických údajů přináší) a že neexistuje jiný vhodný způsob, jak dosáhnout stanoveného cíle, který by byl menším zásahem do soukromí dotčených jednotlivců.[52]

---

[50] K tomu více viz např. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013, s. 187.

[51] K tomu srov. nález ze dne 10. 1. 2001 sp. zn. Pl. ÚS 33/2000.

Je však třeba posílit i záruky proti zneužití biometrických údajů. Tu se lze opřít mj. o judikaturu Evropského soudu pro lidská práva. Ve věci *Gardel v. Francie*, rozsudek ze 17. 12. 2009, App. 16428/05[53] soud judikoval, že bezpečnostní záruky mají zajišťovat, aby byly biometrické údaje (ve vztahu k účelu, pro který jsou uchovávány) relevantní, a nikoli excesivní, po dobu ne delší, než vyžaduje daný účel, a aby byly přijaty i další adekvátní záruky proti jejich zneužití. Uvedené požadavky pak vystupují do popředí zejména u osob mladistvých. Judikatura Evropského soudu pro lidská práva v již citované věci *S. a Marper v. Spojené království* (pokud šlo o uchovávání DNA a otisků prstů) dovodila, že musí existovat časové omezení, neboť jinak mladistvým hrozí jednak stigmatizace, jednak pocit stigmatizace.

Proti zneužití biometrických údajů by měla směřovat i opatření povahy preventivní. Sem patří zejména:

1) zesílení odpovědnosti správců, zpracovatelů (tj. včetně operátorů, případně i providerů) za eventuální způsobenou škodu a posílení jejich kontroly příslušným nezávislým orgánem;
2) periodický audit biometrických systémů, jejich certifikace a monitoring nezávislým tělesem. Takovým tělesem je v České republice Úřad na ochranu osobních údajů (§ 28 a násl. zákona o ochraně osobních údajů);
3) informativní souhlas subjektu údajů se zpracováním osobních údajů (i biometrických údajů); nutné výjimky stanoví zákonné normy daného státu.[54]

Dále je třeba zesílit ochranu zvláštních skupin osob před diskriminací. Kromě klasických případů diskriminace uvedených v čl. 3 odst. 1 Listiny základních práv a svobod (pohlaví, rasa atd.) sem patří i eventuální diskriminace z takových důvodů, jako jsou např. mentální slabost subjektu, fyzický handicap apod.

Rovněž je třeba posílit a náležitě kontrolovat dodržování povinnosti mlčenlivosti ve vztahu k biometrickým údajům. Obecně lze vyjít z ust. § 15 zákona o ochraně osobních údajů, avšak určitým, byť o poznání vzdálenějším, vodítkem může být i eventuální ingerence státních zastupitelství. Z výkladového stanoviska Nejvyššího státního zastupitelství SL 740/2000, poř. č. 15/2001 ze dne 19. 9. 2001 k postupu státních zastupitelství podle zákona č. 101/2000 Sb. plyne, že povinnost mlčenlivosti je upravena v celé řadě zvláštních zákonů; orgány činné v trestním řízení a státní zastupitelství, pokud působí v netrestní oblasti, jsou povinny o skutečnostech, které jsou předmětem povinné mlčenlivosti, samy mlčenlivost zachovávat a učinit jiná nezbytná opatření proti jejich neoprávněnému zveřejnění (např. v souvislosti s nahlížením do spisu podle procesních předpisů).

Zcela specifická a v posledních letech i frekventovaná je otázka biometrických údajů v souvislosti s náboženskou vírou (skutečnou či zneužitou). Jako příklad lze uvést již zmíněné muslimské šátky (či i zahalení postavy) u některých žen. I zde je třeba najít přijatel-

---

52 Srov. např. PARLAMENTNÍ INSTITUT. *Odpověď na dotaz: Právní úprava biometriky*. Červenec 2014, s. 6, 7 – Kanada. *Personal Information Protection and Electronic Documents Act*. S. C. 2000, s. 5.

53 RAINEY, Bernadette – WICKS, Elizabeth – OVEY, Clare. *The European Convention on Human Rights*. Sixth Edition. Oxford: Oxford University Press, s. 378.

54 Viz např. ustanovení § 5 odst. 2 zákona o ochraně osobních údajů, případně ustanovení § 9 téhož zákona, pokud jde o údaje citlivé apod.

nou proporci mezi základním právem svobodně projevovat své náboženství nebo víru (čl. 16 odst. 1 Listiny, čl. 18 odst. 1 Mezinárodního paktu o občanských a politických právech, čl. 8 odst. 1, čl. 9 odst. 1 Úmluvy o ochraně lidských práv a základních svobod) a veřejným zájmem na ochraně veřejné bezpečnosti, pořádku, zdraví, morálky nebo základních práv a svobod jiných (srovnej např. čl. 18 odst. 3 citovaného Paktu). Tu lze jako příklad uvést možnost identifikovat nositele šátku (či celé zahalené postavy), mj. v zájmu ochrany všech proti eventuálním teroristickým útokům.

Podnětem k úvaze zde může být i rozsudek Evropského soudu pro lidská práva ve věci *S.A.S. proti Francii* z 1. 7. 2014, v němž velký senát v poměru 15 : 2 dovodil, že francouzský zákon zakazující zahalování tváře na veřejných místech není v rozporu s Úmluvou o ochraně lidských práv a základních svobod; zájem na podřízení se „*minimálním požadavkům života ve společnosti*" a zásadě „*vzájemného soužití*" tedy podle Soudu převážil nad osobními právy podle čl. 8, 9 Úmluvy.[55] Lze tak mít za to, že tato otázka ještě není a zřejmě dlouho nebude zcela uzavřena. Je však třeba vycházet z okolností konkrétního případu? Či je možné učinit obecný závěr jako Evropský soud pro lidská práva ve sporu s *S.A.S. proti Francii*? Zde se lze spíše přiklonit k první variantě.[56]

Výrazněji a adresněji judikoval Evropský soud pro lidská práva ve věci stížnosti *Ebrahimian proti Francii* z 26. 11. 2015 Nr. 64846/11.[57] Šlo o muslimku (pracující jako sociální pracovnice v psychiatrickém oddělení nemocnice), jíž nebyla prodloužena pracovní smlouva, neboť se zdráhala – přes upozornění personálního vedoucího – odložit obličejovou roušku, což dalo podnět ke stížnostem více pacientů (tedy uživatelů veřejné služby). Soud rozhodl v poměru 6 : 1, že k porušení čl. 9 odst. 1, 2 Úmluvy o ochraně lidských práv a základních svobod nedošlo, neboť daný zásah do práva stěžovatelky na projev náboženského přesvědčení byl zákonem předvídatelný, úměrný a v demokratické společnosti byl nezbytný. Evropský soud pro lidská práva se odvolal zejména na neutralitu a nestrannost veřejných služeb a na princip laického státu ve Francii.

Lze mít důvodně za to, že relativně nová etapa zkoumání dané problematiky se začala časově i věcně odvíjet od útoku na tzv. newyorská dvojčata dne 11. 9. 2001. Později následovaly (a ještě následují) další krizové události, které do značné míry ovládly a stále více ovládají veřejné mínění nejen v zemích euroatlantické civilizace, leč i v zemích kultury islámské. Sem patří, časově bráno, zejména vznik a rozšíření vlivu agresívního tzv. islámského státu na Středním východě a na to navazující (a zčásti s tím i související) masová vlna uprchlíků z uvedené oblasti a ze severní Afriky, která zaplavuje Evropu, jež je, jak se zdá, do značné míry bezradná. Proti sobě, zjednodušeně řečeno, stojí snaha o zajištění ochrany lidských práv uprchlíků – byť nyní převládá tendence odlišovat uprchlíky ekonomické od ostatních – a oproti tomu snaha o zajištění ochrany domácího evropského obyvatelstva, zejména před náporem jiné kultury, vycházející z cizích morálních pravidel, z nichž mnohá jsou v demokratickém právním státu nepřijatelná. I zde platí princip proporcionality, byť tomu odpovídající test bude velmi obtížný. Omyl v tom by mohl být tristní; šířící se xenofobie, bezradnost států, výrazné posilování role

[55] K tomu srov. *Přehled rozsudků Evropského soudu pro lidská práva*. 2015, č. 2, s. 111–123.

[56] K této problematice blíže AGHA, Petr. Muslimské šátky v evropském veřejném prostoru. *Právník*. 2015, č. 10, s. 785–800.

[57] K tomu srovnej obsáhlý komentář v ÖIM-Newsletter. *Menschenrechte*. 2015, č. 6, s. 525–528.

represivních složek státní moci, dominový efekt atd. Který fenomén může mít potom větší ohlas u frustrovaných, vystrašených lidí? Všeobjímající křesťanská láska k bližnímu nebo Karel Martel nebo něco třetího?

Nyní se nabízí otázka, zda lze reálně uvažovat o zpracování zásad právních pravidel užívání a ochrany biometrických údajů, popřípadě i kodexu, po jehož zpracování před více než deseti lety (tj. ještě v „biometrickém pravěku") volala Rada Evropy.[58] Obecně lze říci, že alfou a omegou jakékoliv právní úpravy, jakož i její interpretace, by měl být adekvátní a propracovaný právní rámec lidských práv; mezi nimi pak na vedoucím místě stojí ochrana základního práva na lidskou důstojnost, tedy práva, k jehož naplnění prakticky téměř všechna ostatní lidská práva přímo či nepřímo směřují.

[58] Rada však i zde nakonec usoudila, že mnoho aspektů biometriky není dosud plně známo; proto nepřijala konečné závěry a ponechala je otevřené dalšímu zkoumání. K tomu více viz Úmluva o ochraně osob se zřetelem na automatizované zpracovávání osobních dat, konkrétně pak *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*. ETS 8, Štrasburk 28. 1. 1981. Dostupné z: <https://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf>.

Examination of Some Fundamental Human Rights and Freedoms with Regard to Legal Protection of Biometric Data

Vojen Güttler – Ján Matejka

Abstract: *Biometric data refers to a specific and highly privileged category of sensitive personal data. Its use is strongly limited by law for a number of reasons. Typical reason is a possible conflict between public or individual interests in processing biometric data on one hand and fundamental rights, especially the right to private life, on the other hand. A possible method for solving the problem is the test of proportionality. Compared to other personal data, biometric data possesses specific risks as it represents the only category of personal data that (with exceptions) cannot be changed during the lifetime of an individual. This data is, thus, vulnerable and exploitable in many ways; moreover, such exploitation can often happen in an irreversible manner. In the domain of public law, the only instrument for limitation of risks is represented by the Act No. 101/2000 of the Collection of Laws, on the protection of personal data. Although there are some ambiguities about legal qualification and the very legal regime of biometric data, it is obvious that a solution can be found – in respect of interpretation – especially on the levels of constitutional law and the law of the European Union. It is necessary to make a better use of the principle of proportionality, to strengthen safeguards against the misuse of biometric data, to develop preventive measures and to further analyze the current issues regarding public law titles for processing this data, as well as related security, technological and legal aspects of the issues involved. The question which remains is whether a time has come to prepare a set of principles and legal rules for processing and protection of biometric data, including the popularization and cataloguing of their potential vulnerability. The basis should refer to the legal framework of the relevant fundamental rights, while the right to human dignity should stand on the first place.*

Key words: *biometric data, sensitive personal data, private life, dignified life, principle of proportionality*