Využití biometriky při sledování veřejného prostoru v České republice

Václav Mach
Jan Vobořil

Iuridicum Remedium, z. s.,
únor 2021

Kontrola pod kontrolou. S odvahou.

Projekt podpořila Nadace OSF v rámci programu Active Citizens Fund, jehož cílem je podpora občanské společnosti a posílení kapacit neziskových organizací. Program je financován z Fondů EHP a Norska.

Iceland Liechtenstein Norway **Active citizens** fund

Nadace **OSF**

VÝBOR DOBRÉ VŮLE Nadace Olgy Havlové

SKAUTSKÝ INSTITUT

Obsah

1. Úvod

Nejméně v patnácti státech Evropy se do května 2020 začaly využívat biometrické technologie automatizovaného rozpoznávání obličejů ve veřejných prostorech. Zavádění těchto plošných sledovacích systémů se nevyhnulo ani České republice. Dále je sledování pomocí rozpoznávání na základě biometrických údajů používáno také v Dánsku, Francii, Německu, Řecku, Maďarsku, Itálii, Nizozemsku, Polsku, Rumunsku, Srbsku, Slovinsku, Švédsku, Švýcarsku a Velké Británii.[1] Tyto automatizované systémy jsou často zaváděny netransparentním způsobem bez řádného posouzení jejich nezbytnosti a proporcionality, bez přiměřeného upozornění veřejnosti, a tedy i bez předchozí společenské debaty. Kamerové systémy s automatizovaným biometrickým rozpoznáváním obličeje ve veřejných prostorech mohou porušovat lidská práva – především právo na soukromí, informační sebeurčení a důstojnost; mohou mít negativní dopad na svobodu projevu a shromažďování; a omezovat ochotu obyvatel účastnit se veřejných, společenských nebo politických aktivit. Vzhledem k zásadnímu významu podoby pro osobní identitu jednotlivce a k jedinečnosti a neměnnosti tělesných charakteristik může budoucí rozvoj biometrických sledovacích systémů umožnit trvalý průnik do naší autonomie, svobody a soukromí v masovém měřítku. Trend zvyšování míry sledování obyvatel ve světě navíc ještě zesiluje v souvislosti s pandemií viru SARS-CoV-2.[2]

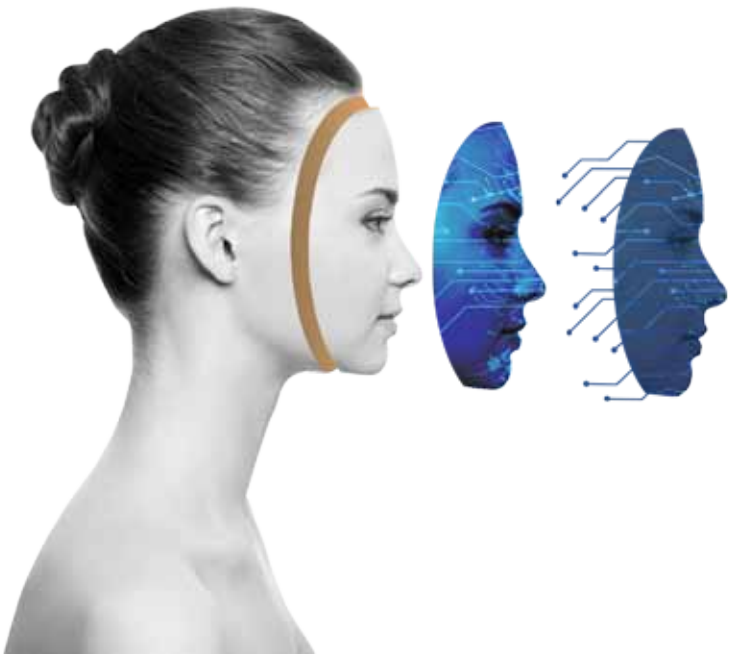
Biometrické údaje, které jsou v současnosti stále více využívané v automatickém zpracovávání, mohou být definovány jako informace o biologických vlastnostech, fyziologických charakteristikách, znacích jedince nebo opakovatelném jednání, kdy jsou tyto rysy nebo jednání pro daného jedince jedinečné a měřitelné, a to i tehdy, když použité vzorky zahrnují určitý stupeň pravděpodobnosti. Typickými příklady takových biometrických dat jsou otisky prstů, struktura obličeje, hlas, ale také geometrie rukou, vzorky žil nebo některé hluboce zakořeněné dovednosti nebo jiné charakteristiky chování (například ručně psaný podpis, stisknutí kláves, konkrétní způsob chůze nebo mluvy).[3]

Systémy zpracovávající biometrické údaje se rychle rozšiřují, a to především kvůli rostoucímu financování z veřejných rozpočtů a pokroku v algoritmech strojového učení. Důsledkem technologického pokroku je analýza fotografií, videa a dalších materiálů v masovém měřítku stále levnější a dostupnější. Sběr, zpracování a ukládání biometrických údajů není jen otázkou technologickou, ale především otázkou etickou, právní a společenskou, protože podle dat Evropské agentury pro lidská práva již dnes zhruba 83 % Evropanů a 84 % Čechů nesouhlasí s tím, aby úřady využívaly vyobrazení jejich obličeje.[4] V listopadu 2020 byla spuštěna celoevropská petiční akce **ReclaimYourFace**, která požaduje plné informace o využívání biometrických technologií a následně odmítnutí těchto technologií ve veřejném prostoru. Petice je registrována jako tzv. Evropská občanská iniciativa, která bude v souladu s evropskou legislativou požadovat v případě úspěšného naplnění předepsaného počtu podpisů konkrétní kroky po Evropské komisi.

Biometrické kamerové systémy však dosud v České republice nebyly předmětem systematického odborného zájmu ani hlubší veřejné diskuse. Jako v případě jiných technologií, začaly být fakticky používány, aniž by byly řešeny právní a etické důsledky. Společenské diskusi by měly být biometrické technologie podrobeny z hlediska možného zesílení existujících nerovností a diskriminace. Otázkou také je, zda je jejich rozvoj v souladu s koncepcí demokracie, svobody, rovnosti a sociální spravedlnosti.

Několik úřadů evropských států pro dohled nad ochranou osobních údajů již konstatovalo, že některé současné instalace systémů využívajících biometrické údaje jsou nezákonné[5] a podle našich zjištění ani nejrozsáhlejší systém provozovaný v České republice na Letišti Václava Havla Praha nesplňuje všechny zákonné podmínky. Vývoj a instalace těchto systémů jsou navíc dotovány z veřejných prostředků bez předchozího zhodnocení toho, zda mohou být využívané v souladu s právním řádem.

Tento dokument se pokouší o základní argumentaci dokládající neslučitelnost biometrických technologií ve veřejných prostorech s ochranou základních práv a svobod, právem na ochranu osobních údajů, demokracií a základními zásadami právního státu. Dále se pokouší poskytnout základní vhled na dosavadní rozšíření, využívání a aplikaci biometrických technologií ve veřejném prostoru v České republice.



2. Zavádění automatického monitoringu jako systému společenské kontroly

2.1 Plošné sledování

Technologie, které provádějí plošné sledování, ať už za účelem veřejné správy či vymáhání práva, nebo pro komerční účely, představují vážnou hrozbu pro soukromí i bezpečnost. Plošné sledování lze definovat jako sledování, které není prováděno cíleně ve vztahu ke konkrétní osobě a začíná bez předchozího důvodného podezření. Zásady ochrany soukromí a spravedlivého procesu vyžadují, aby u cíleného sledování (např. odposlechy telefonů dle trestního řádu) měl orgán provádějící sledování zákonné oprávnění a k tomu důvodné podezření na konkrétního jednotlivce. Plošné sledování je naopak opatřením s obecným dopadem na veřejnost, a probíhá bez předchozího důvodného podezření, často bez vědomosti sledovaných osob o nasazení nebo rozsahu sledování.

Původně byly před lety instalovány do veřejných prostor kamerové systémy s deklarovaným cílem prevence kriminality.[6] Podle výsledků studií četnosti kriminality nedošlo v místech instalace kamerových systémů k jejímu snížení, ač měl tento faktor vliv na strukturu kriminality. V současné době jsou některé nainstalované či nově instalované kamerové systémy doplňovány o biometrické zpracování obrazu za účelem identifikace na základě tváře, což zvyšuje intenzitu plošného sledování. Technologie rozpoznávání obličeje umožňuje automatickou identifikaci jednotlivce porovnáním dvou nebo více obličejů zachycených na digitálních snímcích. To probíhá na základě detekce a měření různých rysů obličeje, extrakce těchto hodnot ze zachycené fotografie a v dalším kroku jejich porovnáním s hodnotami v databázi, které jsou převzaté z jiné fotografie.[7]

Biometrické rozpoznávání obličeje kamerovými systémy představuje významné navýšení všudypřítomného sledování, jehož důsledkem je nárůst nerovnováhy moci mezi lidmi a státem (a soukromými společnostmi) a také potenciálu zneužívání. Biometrické systémy nasazené pro jeden konkrétní účel mohou být v tajnosti zneužívány k jiným účelům. Přestože lidé v některých případech poskytnou souhlas nebo alespoň mají povědomí o použití svých

biometrických údajů pro konkrétní účel, mají už zpravidla mizivé povědomí o dalším využití těchto údajů. Jakmile se objeví neplánovaná možnost využití nějaké technologie k řešení nově vzniklého problému, vlády a úřady často tuto technologii nasadí nad rámec původního cíle, pro který byla zavedena.

Plošné sledování obecně tvoří překážku ve výkonu občanských a politických práv. Dopady sledovacích systémů posílených biometrickým rozpoznáváním mohou mít velmi zásadní dopad na svobodu projevu a shromažďování, protože plošné sledování znamená faktickou ztrátu anonymity na veřejných prostranstvích. Všudypřítomnost plošného sledování je způsobilé omezovat účast občanů na společenském, veřejném a politickém životě a má dopad na možnost žít svobodně bez nutnosti přizpůsobovat své chování kvůli obavám z dopadů neustálého sledování. Německý ústavní soud ve svém nálezu z roku 1983 ve věci sčítání lidu uvedl:

Osoba, která si klade otázku, zda je neobvyklé chování pokaždé zaznamenáno a poté vždy ukládáno, používáno nebo rozšiřováno, se pokusí, aby mu nebyla tímto způsobem věnována pozornost. Osoba, která například předpokládá, že účast na schůzi nebo občanské iniciativě je oficiálně zaznamenána a může pro ni představovat riziko, se může rozhodnout neuplatňovat příslušná základní práva ([zaručeno v] článcích 8 a 9 Ústavy). To by omezilo nejen možnosti osobního rozvoje jednotlivce, ale také společenské dobro, protože sebeurčení je základním předpokladem svobodné a demokratické společnosti založené na schopnostech a soudržnosti občanů.[8]

Sledovací systémy prakticky vytváří situaci, kdy mocní sledují a bezmocní jsou sledováni. To umožňuje vládnoucí skupině posilovat svou moc nad ostatními sociálními skupinami, jako jsou sociálně vyloučení nebo opoziční političtí aktivisté. Vyvolává to etické otázky týkající se sociální spravedlnosti, ale také základních práv. Kromě toho existence monitorovací infrastruktury a její používání v každodenním životě může vést k mylné víře, že neustálé sledování, monitorování a analýza osobních dat jsou normální. Demokratické společnosti by přitom neměly dovolit normalizaci činností, které jsou vlastní autoritářským režimům.

2.2 Prohlubování nerovností

Biometrické a automatizované profilovací systémy jsou v podstatě technologie, které mají lidi automatizovaně třídit do různých kategorií. Jejich účelem je posoudit a ustanovit riziko u sledovaných osob a ve výsledku s nimi na základě toho zacházet odlišně. Tato kategorizace v podstatě diskriminuje skupiny obyvatel na základě jejich „rizikovosti“, a může vést k prohlubování nerovnosti, protože tyto skupiny budou podřízeny také vyššímu sledování biometrickými technologiemi.[9] Diskriminaci ještě zhoršuje skutečnost, že vstupní údaje, které se používají k trénování biometrických systémů rozpoznávání nebo umělé inteligence, nejsou neutrální, ale odrážejí a kódují předsudky či strukturální diskriminaci ve společnosti.

Zkreslení a chybovost v důsledku diskriminačního nastavení může vést k falešným identifikacím sledovaných skupin a může zhoršit dopady jejich nadměrné kontroly. Biometrická identifikace je založena na pravděpodobnosti a existuje určitá míra chybné shody (falešně pozitivní shoda) a chybné neshody (falešně negativní shoda). Míra chybovosti je ovlivněna celou řadou faktorů včetně vstupních údajů, podmínek snímání a algoritmu. Například se zjistilo, že rozpoznávací biometrické systémy může zmást podobnost sourozenců nebo příbuzných.[10] Také se prokázalo, že technologie k rozpoznávání tváře mají vyšší chybovost u Afričanů nebo Asiatů.[11] V konečném důsledku to může prohlubovat diskriminaci těchto skupin. Konkrétním příkladem negativního dopadu falešné pozitivity biometrického systému s umělou inteligencí na konkrétní osobu došlo například v lednu 2020 v americkém Detroitu, kde došlo k zatčení Afroameričana Roberta Williamse, který měl údajně 15 měsíců předtím ukrást hodinky. Důkazy pocházející z technologie na rozpoznávání obličejů se však později ukázaly jako chybné. Kvůli chybě biometrické technologie tak musel nedobrovolně absolvovat několikahodinovou proceduru včetně odběru DNA a otisků prstů.[12]

2.3 Bezpečnostní rizika

V systémech zpracovávajících biometrické údaje může dojít k porušení zabezpečení. Získání samotných biometrických údajů určité osoby by mohl v případě jejich falešné autentizace umožnit průnik do systému, kde jsou tyto biometrické údaje užívány jako přístupové. K takovému odcizení dat by mohlo dojít podobně jako v případě používání stejného hesla u dvou odlišných systémů. Na rozdíl od systémů založených na klasickém heslu, jednou kompromitovaná biometrická informace nemůže být změněna nebo zrušena. Pokud byla dříve biometrická informace uložena v několika databázích, zvyšuje to pravděpodobnost úniku biometrických údajů, k čemuž již dochází. [13] [14]

Biometrické rozpoznávání má uplatnění také v soukromém sektoru, kde je obecně nižší úroveň kontroly a ochrany než u veřejných institucí. Biometrické technologie se používají v reklamě nebo marketingu k profilování zákazníků a předvídání jejich preferencí vůči produktům založené na jejich mimice. Pomocí analýzy výrazů v obličeji se profilují uchazeči o zaměstnání během pohovorů. Sociální média, jako je Facebook, zavádějí biometrické technologie k zlepšení jejich systému označování osob na fotografiích.

Zavádění biometrických identifikačních a sledovacích systémů ve veřejně přístupných prostorech mnohdy dochází bez řádné odpovědnosti státu, bez náležitého veřejného dohledu a v rozporu s právní ochranou soukromí, jejímž cílem je bránit lidi před zneužitím státní moci.[15] Navíc nad technologiemi používanými veřejnými orgány získávají příliš velkou moc soukromí aktéři, zejména vývojáři a správci příslušných technologií, přičemž mají za své jednání směrem k veřejnosti jen malou nebo žádnou odpovědnost. Zapojení soukromých aktérů ve vývoji systémů plošného biometrického sledování jim může poskytnout příliš velkou moc nejen nad lidmi, ale také velký vliv na státy.[16]

2.4 Propojování údajů a globální dystopie

Kombinovaný dopad rozpoznávání obličejů na veřejných prostranstvích a slučování různých biometrických databází představuje růst rizik pro bezpečnost, soukromí a další základní práva. Ohrožení svobody občanů by ještě narostlo, pokud by data získaná systémem plošného sledování veřejného prostoru byla dále analyzována a používána k vytváření profilů jednotlivců. Možnosti této funkce se budou postupem času zvyšovat, protože stále více různých dat (sociální sítě, data veřejných orgánů, různé databáze) bude možné propojit se záznamy z veřejných prostor. Vývoj podobných funkcí slibuje také česká společnost Cogniware, která hodlá vyvíjet algoritmy propojující sledovací systémy s daty ze sociálních sítí.[17] Ovšem také metadata nebo anonymizované údaje lze v kombinaci s dalšími možnými zdroji, jež mají k dispozici veřejné a soukromé subjekty, použít k získání citlivých informací. Rozrůstající se sledovací sítě vytvářejí trvalé záznamy o našich životech, interakcích a chování bez možnosti to reálně ovlivnit.

Pokud by bylo plošné sledování spolu s biometrickým zpracováním dat na veřejných prostranstvích normalizováno v běžném životě, mohlo by být mnohem snadněji zavedeno bodování a kategorizování obyvatel.[18] Protože jsou neustále zaváděny inovace s velkými daty a umělou inteligencí, existuje riziko, že jednou dojde ke kombinaci obrovského množství údajů z různých evidencí veřejné správy, veřejně přístupných rejstříků a dalších zdrojů včetně sociálních sítí, které mají k dispozici komerční subjekty. Propojování databází by mohlo být spojeno se zaznamenáváním fyzického výskytu jedinců na ulicích, přičemž by to umožňovalo monitorovat jejich interakce a pohyb způsobem, jenž by vytvářel podrobné a důvěrné obrazy jejich životů. To by při extrémním zneužití mohlo vést k systémům sociálního skórování a manipulaci s chováním veřejnosti. V tomto ohledu je často zmiňovaný systém sociálního kreditu v Čínské lidové republice. Jedná se o postupně budovaný státní systém hodnocení obyvatel na základě různých aspektů jejich ekonomického a společenského chování, na jehož základě

se bude jednotlivým občanům poskytovat různá úroveň přístupu k veřejným službám, ale například i k různým slevovým akcím ze strany soukromého sektoru.[19] Systém nebezpečně propojující pestré spektrum informací o jednotlivcích z mnoha veřejných i soukromých zdrojů se nachází v testovací fázi a jeho ostré spuštění se plánuje v blízké době.

Používání biometrických algoritmů k hodnocení chování, motivací nebo vlastností lidí mnohdy postrádá vědecký základ. Funkce biometrických systémů na „rozpoznávání emocí" nebo „předpovídání chování" se pokouší identifikovat emoce a záměry sledovaných osob. Podstatně tím ohrožují lidskou důstojnost a autonomii. Analýza studií zkoumajících emoce dospěla k závěru, že neexistuje vědecký důkaz pro tvrzení technologických společností, že mohou spolehlivě detekovat emoce prostřednictvím analýzy videa.[20] Tyto formy předpovědí ignorují souhlas detekovaných osob ke zpracování jejich biometrických údajů, zbavují je práva na řádný proces, vysvětlení a nápravy, pokud tím utrpí újmu. Může tím docházet k porušování základních práv a narušuje to důvěru lidí v provozovatele takovýchto biometrických technologií.[21]

3. Právní regulace

Využívání biometrických systémů ve veřejných prostorech není v českých a evropských právních předpisech podrobně a jasně upraveno, přestože významně zasahuje do základních práv občanů. Biometrické technologie jsou v České republice zaváděny bez dostatečného zhodnocení jejich možných dopadů, a to přestože mají tyto technologie potenciál k plošnému a hlubokému zásahu do základních práv. Následující část se pokusí zhodnotit současnou právní úpravu, pokud jde o evropskou i vnitrostátní rovinu.

3.1 Ochrana základních práv

Plošné sledování je z hlediska ochrany základních práv regulováno nástroji na vnitrostátní, evropské a mezinárodní úrovni. Základní práva na soukromí a ochranu osobních údajů jsou zakotvena v čl. 7 a 8 Listiny základních práv Evropské unie, čl. 8 Úmluvy o ochraně lidských práv a základních svobod a čl. 7 odst. 1 a 10 odst. 2 a 3 Listiny základních práv a svobod České republiky.

Kromě práv na soukromí a ochranu osobních údajů zasahuje plošné sledování také do dalších základních práv, která jsou uvedenými předpisy chráněna. Patří mezi ně právo na důstojnost, svobodu projevu a svobodu shromažďování a sdružování. Listina základních práv Evropské unie stanoví právo na důstojnost v čl. 1, právo na svobodu projevu v čl. 11 a právo na svobodu shromažďování a sdružování v čl. 12. Úmluva o ochraně lidských práv a základních svobod chrání důstojnost v Preambuli (s odkazem na Všeobecnou deklaraci lidských práv), svobodu projevu v čl. 10 a svobodu shromažďovací a sdružovací v čl. 11. Odpovídajícími ustanoveními Listiny základních práv a svobod České republiky jsou pak: čl. 10 odst. 1 (důstojnost), čl. 17 (svoboda projevu) a čl. 19 a 20 (svoboda shromažďování a sdružování).

Jakýkoli zásah do uvedených základních práv – včetně využívání biometrických technologií v kamerových systémech – podléhá splnění určitých hodnotících kritérií, která se promítají do tzv. testu proporcionality. Předně musí být zásah do základních práv stanoven zákonem, může být aplikován, pouze pokud je vhodný (naplňuje legitimní cíl v podobě veřejného zájmu nebo ochrany práv a svobod druhých) a nezbytný (legitimního cíle nelze dosáhnout vhodnějším způsobem) a nakonec takový zásah musí být proporcionální. Evropský inspektor ochrany údajů[22] stanoví k prokázání nezbytnosti a proporcionality přísné pokyny,[23] přičemž dosavadní využívání biometrických technologií splnění těchto právních kritérií zatím neprokázala.

Soukromý život je dle Evropského soudu pro lidská práva „široký pojem, který není poddajný vyčerpávající definici".[24] Obecně chrání možnosti jednotlivce žít svůj život bez nepřiměřených zásahů a omezení. V základech tohoto práva je koncept svobody, ve smyslu „být nechán na pokoji", tedy koncept existence soukromé zóny, do které by neměl nikdo neoprávněně vstupovat nebo zasahovat.[25] Evropský soud pro lidská práva také vyjádřil, že extenzivní interpretace pojmu soukromý život je ve shodě s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat,[26] jejímž cílem je ***„zaručit na území každé smluvní strany každé fyzické osobě (...) respektování jejích práv a základních svobod, a zejména jejího práva na soukromý život, v souvislosti s automatizovaným zpracováním údajů osobního charakteru, které se jí týkají (čl. 1), přičemž ty jsou definovány jako jakékoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (čl. 2)".*** Evropský soud pro lidská práva také rozhodl, že tajné sledování za účelem odhalování nebo prevence trestné činnosti a sdílení kamerových záznamů spadá do oblasti působnosti čl. 8 Úmluv o ochraně lidských práv a základních svobod, který chrání právo na soukromý a rodinný život.[28]

Ochrana osobních údajů je v českém ústavním právu označována jako právo na informační sebeurčení, podle kterého má každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.[29] Jak konstatoval Ústavní soud ČR: ***„Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti z jeho osobního soukromí zpřístupněny jiným subjektům."***[30]

Odmítnutí plošného sledování v souvislosti s ochranou soukromí a ochranou osobních údajů je v judikatuře často odůvodněno tím, že sledování probíhá bez dostatečně zdůvodněného podezření vůči sledovaným osobám. V tomto ohledu je znám případ S. a Marper proti Velké Británii, ve kterém Evropský soud pro lidská práva shledal, že „plošné a nerozlišující" uchovávání biometrických údajů je „nepřiměřeným zásahem" do práva na soukromí.[31]

V případu Digital Rights Ireland zkoumal Soudní dvůr Evropské unie slučitelnost směrnice o uchovávání údajů 2006/24/ES s čl. 7 a 8 Listiny základních práv Evropské unie. Zvláště zdůraznil, že směrnice: ***„Pokrývá obecně všechny osoby a všechny prostředky elektronické komunikace (...), aniž by došlo k jakékoli diferenciaci, omezení nebo výjimce s ohledem na cíl boje proti závažné trestné činnosti."***[32] Soud v případu poznamenal, že napadená opatření ***„pravděpodobně vyvolala v myslích dotčených osob pocit, že jejich soukromý život je předmětem neustálého sledování".*** V tomto rozhodnutí pak tuto směrnici o tzv. data retention, tedy o plošném uchovávání metadat o elektronické komunikaci zrušil. V navazujících rozsudcích ve věcech Tele2/Watson, Privacy International a La Quadrature du Net and Others pak opakovaně odmítl plošné a nerozlišující sledování elektronických komunikací.[33]

Problematické je především plošné sledování občanů, kteří nejsou podezříváni z protiprávních činů nebo ohrožení veřejného pořádku. Jak uvedl Soudní dvůr Evropské unie: ***„Právní úprava, která veřejným orgánům umožňuje globální přístup k obsahu elektronických komunikací, musí být považována za zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny..."***[34]

Základní práva Evropské unie jsou založena na důstojnosti člověka podle čl. 1 Listiny základních práv Evropské unie, který stanoví: ***„Lidská důstojnost je nedotknutelná. Musí být respektována a chráněna.“*** Další nástroje v oblasti lidských práv jsou podobně centrálně založeny na všeobecné a nezcizitelné lidské důstojnosti. To vedlo k tomu, že důstojnost je někdy považována za „mateřské právo“.[35] V pojetí Ústavního soudu ČR představuje právo na lidskou důstojnost v čl. 10 odst. 1 Listiny základních práv a svobod subjektivní právo jednotlivce a je chápáno ve významu přirozené hodnoty člověka, která mimo jiné vylučuje jednat s jednotlivcem jako s objektem.[36]

Jakékoli zpracovávání biometrických údajů je ze své podstaty právně problematické již kvůli nezbytnosti splnění požadavků, jako jsou nezbytnost, proporcionalita a zákonnost. Jakmile však dochází k necílenému (plošnému) zpracování biometrických údajů získaných na veřejných prostranstvích, lze ho z hlediska ochrany lidských práv ospravedlnit jen velmi těžko.

3.2 Právní úprava Evropské unie

V právu Evropské unie jsou dva základní právní předpisy, které se týkají ochrany osobních údajů a přímo se dotýkají využívání biometrických údajů. Jedná se především o Obecné nařízení o ochraně údajů (známé pod zkratkou GDPR),[37] které stanoví obecné zásady ochrany osobních údajů. Druhým právním aktem je Směrnice o ochraně údajů v oblasti prosazování práva,[38] která uvedené nařízení doplňuje, pokud jde o ochranu osobních údajů v oblasti prevence, vyšetřování, odhalování či stíhání trestných činů. Podle GDPR a Směrnice o ochraně údajů v oblasti prosazování práva je definována tzv. zvláštní kategorie údajů, což jsou osobní údaje obzvláště citlivé mající zvýšenou ochranu. Mezi tyto zvláště citlivé údaje patří také zpracování biometrických údajů, jako jsou tváře nebo otisky prstů, pokud jsou použity za účelem jedinečné identifikace fyzické osoby, ale také informace jako rasa, etnická příslušnost, pohlaví, sexuální orientace, náboženství nebo zdravotní stav. GDPR výslovně definuje biometrické údaje v čl. 4 odst. 14 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“.***

GDPR stanovuje přímo aplikovatelná pravidla pro zpracování osobních údajů v členských státech Evropské unie. Nařízení se vztahuje na všechna zpracování osobních údajů k jiným účelům než pro účely vymáhání práva bezpečnostními sbory. Podle čl. 9 odst. 1 je zpracování biometrických údajů a dalších údajů zvláštní kategorie (rasový či etnický původ, politické názory, náboženské vyznání, filozofické přesvědčení, členství v odborech, genetické a další údaje) krom výjimek uvedených v čl. 9 odst. 2 zakázáno z důvodu citlivosti těchto údajů. Jednou z výjimek z tohoto pravidla je udělení souhlasu dle čl. 9 odst. 2 písm. a) GDPR ve spojení s čl. 7 nařízení. Omezení možnosti založit zpracování osobních údajů na platném souhlasu může demonstrovat příklad, kdy švédská Datainspektionen[39] udělila v roce 2019 první pokutu za nedodržování GDPR. Škola ve

Skellefteå na severu Švédska využívala ve zkušebním provozu technologii na rozpoznávání obličeje ke sledování docházky 22 žáků po dobu tří týdnů. Škola tím porušila několik ustanovení GDPR. Neobstál argument školy, že byl proces prováděn se souhlasem, protože taková dohoda dle Datainspektionen postrádá platný právní základ kvůli nerovnováze sil mezi subjektem a správcem údajů.[40] Podobně realizace plošného sledování na veřejných prostranstvích v zásadě vylučuje schopnost lidí udělit skutečný, informovaný a svobodný souhlas.

GDPR dále stanoví, že při využívání osobních údajů, musí být splněny určité zásady uvedené v čl. 5 nařízení, kam patří například nutnost zákonnosti zpracování osobních údajů. Mezi další zásady podle čl. 5 GDPR patří požadavek minimalizace využívaných údajů, který ukládá, aby shromažďované údaje byly omezeny jen na to, co je nezbytné pro jasně definované a výslovně stanovené legitimní cíle; požadavek omezení účelu; požadavek na kvalitu údajů zakazující použití nedostatečně přesných osobních údajů; požadavek transparentnosti a další zásady. Článek 22 GDPR dále zakazuje plně automatizovaná rozhodnutí založená na využívání osobních údajů včetně biometrických.

Směrnice o ochraně údajů v oblasti prosazování práva stanoví pravidla pro zpracování osobních údajů příslušnými orgány. Nejčastěji, ale nikoli výlučně, se jedná o orgány činné v trestním řízení, které se zaměřují na oblast prevence, odhalování nebo stíhání trestných činů. Směrnice o ochraně údajů v oblasti prosazování práva byla přijata současně s GDPR jako součást jednoho souborného balíčku a jedná se o vzájemně se doplňující nástroje založené na stejných principech.[41]

Směrnice o ochraně údajů v oblasti prosazování práva v čl. 4 odst. 1 písm. a) uvádí, že také pro účely vymáhání práva musí být údaje ***„zpracovávány zákonným a korektním způsobem“.*** Směrnice v čl. 6 ukládá také povinnost rozdílného zacházení s osobními údaji odsouzených nebo podezřelých z trestných činů (v takovém případě musí mít orgán závažné důvody se domnívat, že konkrétní osoba spáchala nebo se chystá spáchat trestný čin) a osobními údaji osob, které nejsou odsouzené nebo podezřelé z trestné činnosti. Rozlišení různých kategorií osob je důležité, aby došlo k odlišení legitimního a zákonného zpracování údajů u důvodně podezřelých osob a nelegitimním necíleným zpracováváním osobních údajů kterékoliv osoby. Právě do druhé kategorie zpracování můžeme zařadit necílené biometrické zpracování údajů osob pohybujících se ve veřejných prostorech.

Stejně jako v případě zpracování osobních údajů dle GDPR musí zpracování údajů pro účely vymáhání práva splňovat přísná kritéria. Podle čl. 8 odst. 1 Směrnice o ochraně údajů v oblasti prosazování práva musí zpracování osobních údajů splňovat podmínku nezbytnosti. Podle WP 29[42] to znamená, že bezpečnostní orgány musí pro zpracování těchto údajů předkládat odůvodnění,[43] a také musí být toto zpracování výslovně umožněno právem Evropské unie nebo členského státu. Dle čl. 10 se pak odlišují zvláštní kategorie osobních údajů, kam patří biometrické údaje. Na rozdíl od GDPR není dle směrnice souhlas právním důvodem zpracování.

Některé aplikace biometrického zpracování spadají jednoznačně do působnosti GDPR (např. správa školského systému nebo vstup zaměstnanců na pracoviště) a jiná pod Směrnici o ochraně údajů v oblasti prosazování práva (soudnictví, policejní právo a pořádkové činnosti). Přesto existují situace, ve kterých dochází k překryvu a není jednoznačné, jakou právní úpravu použít. Nejasný může být například policejní monitoring fanoušků při fotbalovém

utkání k identifikaci známých výtržníků, přičemž jsou zabírány všechny osoby v davu. Tyto problémy může ještě komplikovat rostoucí role soukromých aktérů v oblasti vymáhání práva, například outsourcingem nebo poskytováním komplikovaných technologií, o kterých nemá policie dostatečné technické znalosti. Ve smyslu ochrany biometrických nebo jiných citlivých údajů a odstraňování mezer v zákoně, stále panuje potřeba lepšího prosazování a jasnějšího výkladu GDPR, Směrnice o ochraně údajů v oblasti prosazování práva a jejich vzájemných vztahů. Přesto zásadní otázky biometrického zpracování používané k plošnému sledování zůstávají stejné, ať se použije GDPR, nebo Směrnice o ochraně údajů v oblasti prosazování práva, respektive její národní implementace.

Vzhledem k faktu, že se v případě biometrického zpracování a umělé inteligence jedná o rychle se rozvíjející oblast, lze v ní také očekávat vývoj evropské legislativy. Evropská komise vydala v únoru 2020 Bílou knihu o umělé inteligenci,[44] která stanoví možnosti politiky pro širokou škálu aplikací umělé inteligence.[45] Ohledně rozpoznávání obličeje a biometrického zpracování bylo v knize s ohledem na jejich rizika navrženo, aby byly automaticky považovány za „vysoce rizikové“. Dokument však již adekvátně neposuzoval dopady těchto „vysoce rizikových“ aplikací na základní práva.[46]

3.3 Právní úprava v České republice

Česká právní úprava týkající se ochrany osobních údajů v souvislosti s využíváním biometrických údajů vychází z právní úpravy Evropské unie. Důležité jsou v tomto ohledu zákon č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 89/2012 Sb., občanský zákoník, a zákony upravující pravomoci bezpečnostních sborů a zpravodajských služeb a to zejména zákon č. 273/2008 Sb., o Policii ČR, zákon č. 153/1994 Sb., o zpravodajských službách České republiky, a zákon č. 300/2013 Sb., o Vojenské policii. GDPR je v členských státech Evropské unie přímo vykonatelný právní akt, takže je součástí českého právního řádu dnem nabytí jeho účinnosti 25. května 2018. Směrnice o ochraně údajů v oblasti prosazování práva je v českém právním systému prováděna především zákonem o zpracování osobních údajů, který je pak doplněn dalšími zákony.

V oblasti ochrany osobních údajů v soukromoprávních vztazích dochází k souběhu ochranné regulace dle GDPR a ochrany osobnosti zakotvené v občanském zákoníku,[47] což se uplatní také při zpracování biometrických údajů.[48] Přes přednostní regulaci GDPR mají osobnostní práva zakotvená v občanském zákoníku vliv na rozsah autonomie vůle.[49] Primárně je chráněno ***„svobodné rozhodnutí člověka žít podle svého“***. Hlavním nástrojem je svolení dotčené osoby. Toto svolení nezakládá smluvní vztah mezi osobou, která udělila svolení, a osobou, které bylo svolení uděleno, protože osobnostní práva nemohou být předmětem závazků. Svolení k použití osobních údajů může být tedy kdykoliv odvoláno.[50]

Dne 24. dubna 2019 nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, někdy nazývaný jako „adaptační zákon“ k GDPR. Zákon o zpracování osobních údajů využívá pro zpracování osobních údajů ve vybraných případech některá oprávnění ke stanovení odchylné úpravy od GDPR.[51]

Z hlediska pracovního práva a užívání biometrických údajů stanovuje česká právní úprava na základě GDPR jednu povinnost. Zpracování biometrických údajů podléhá dle čl. 9 odst. 2 GDPR několika výjim-

kám, kdy musí osoby zpracování svých údajů strpět. Jednou z výjimek je zpracování biometrických údajů ***„pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu“***. Zatím u nás existuje jedna taková výjimka, která výslovně stanoví povinnost biometrické identifikace pro zaměstnance, a tou je vstup do jaderných zařízení.[52] Ve sféře pracovního práva je jinak zaměstnanec chráněn § 316 odst. 2 zákona č. 262/2006 Sb, zákoníku práce, který stanoví, že zaměstnavatel nesmí bez závažného důvodu narušovat soukromí zaměstnance tím, že by ho podroboval otevřenému nebo skrytému sledování.

Směrnice o ochraně údajů v oblasti prosazování práva byla do českého právního řádu provedena zákonem o zpracování osobních údajů. Hlavy III a IV první části zákona jsou věnovány zpracování a ochraně osobních údajů orgány veřejné moci za plnění úkolů v trestněprávní oblasti, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti a zpracování a ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky. Uvedené hlavy však z hlediska zvláštní kategorie údajů, kam patří také biometrické údaje, nestanoví nad rámec směrnice podstatné odlišnosti. Zásadní je v tomto další legislativa. Společně se zákonem o zpracování osobních údajů nabyl účinnosti také zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů a který zapracovává změny, vyvolané přijetím zákona o zpracování osobních údajů, do vybraných dalších právních předpisů. Tyto změny se týkají zejména zpracování osobních údajů v souvislosti s výkonem veřejné moci. Podstatné jsou s ohledem na biometrické údaje změny zákona č. 273/2008 Sb., o Policii ČR a zákona č. 300/2013 Sb., o Vojenské policii. Dále pak v září 2019 nabyla účinnosti změna zákona č. 153/1994 Sb., o zpravodajských službách České republiky, která do využívání biometrických údajů zásadně zasáhla.[53]

V případě pravomocí Vojenské policie se jedná o oprávnění zpracovávat biometrické údaje. Podle nového § 11a odst. 3 Vojenská policie může při plnění úkolů v zahraničních misí pořizovat a dále zpracovávat biometrické údaje také u osob, které nejsou podezřelé nebo obviněné ze spáchání trestného činu. V zákoně pak není blíže specifikováno, o které osoby by se mohlo jednat, ale v této souvislosti je potřeba připomenout, že má Vojenská policie dle § 12 oprávnění požadovat informace z agendových informačních systémů, jako jsou informační systém evidence občanských průkazů, informační systém evidence cestovních dokladů, informační systém evidence obyvatel a dalších způsobem umožňujícím dálkový a nepřetržitý přístup. Jak extenzivně a v jakých případech Vojenská policie své oprávnění využívá, není jasné, ale podmínka „plnění úkolů v zahraničních misí“ pravděpodobnost zneužití k plošnému sledování podstatně snižují, nicméně je v tomto ustanovení prolamována zásada rozlišování mezi různými kategoriemi subjektů údajů v čl. 6 Směrnice o ochraně údajů v oblasti prosazování práva.

Podstatně problematičtější je nové oprávnění Policie ČR a zpravodajských služeb, které bylo zavedeno do zákona o Policii ČR (§ 66a odst. 1 a 2) a zákona o zpravodajských službách (§ 11c) teprve v roce 2019. V případě zákona o zpravodajských službách se změna týká všech tří zpravodajských služeb, kterými jsou Bezpečnostní informační služba, Vojenské zpravodajství a Úřad pro zahraniční styky a informace. Zpravodajské služby a policie tak

mohou získávat a zpracovávat digitální fotografie a identifikátory lidí vedených v informačních systémech, konkrétně v informačním systému evidence občanských průkazů, informačním systému evidence cestovních dokladů, informačním systému evidence diplomatických a služebních pasů, registru řidičů, centrálním registru řidičů nebo informačním systému cizinců. Ačkoli není v zákoně jednoznačně definován účel zpracování digitálních fotografií, tak důvodové zprávy jsou v tomto celkem jednoznačné. V důvodové zprávě k novele zákona o policii ČR se uvádí: ***„…Navrhovaná změna přináší policii možnost softwarového vyhledávání a rozpoznávaní obličejů, která v případě potřeby dokáže významným způsobem zkrátit čas k odhalení pachatele, případně zabránit dalším hrozícím útokům…“*** Digitální fotografie ze státních registrů tak budou využívány k identifikaci osob metodami rozpoznávání obličeje celkem čtyřmi státními orgány, které pracují zcela nebo z velké části v utajení. Spolu s fotografiemi budou uchovávány také agendové identifikátory, které umožňují policii a zpravodajským službám propojovat fotografie s dalšími osobními údaji v daných registrech. Tyto orgány pak budou pracovat s anonymizovanou databází všech občanů, jejichž tváře budou porovnávány se zájmovými fotografiemi. Bude tak docházet k masivnímu využívání biometrických údajů o všech osobách bez ohledu na jakékoli podezření. Dle výše citované důvodové zprávy bude ke ztotožnění osoby docházet až v případě nalezení shody s anonymními fotografiemi v referenční databázi. To ovšem nic nemění na rozsahu zpracování biometrických údajů občanů.

Využívání těchto pravomocí by mohlo vypadat tak, že záběry z bezpečnostních kamer, k nimž se na základě svých oprávnění může policie a zpravodajské služby dostat, bude možné pomocí softwaru na rozpoznávání obličejů analyzovat a porovnávat s fotografiemi ze základních registrů. Jednoduše je takto možné vysledovat pohyb konkrétního člověka ve veřejném prostoru nebo identifikovat osoby, které se na záznamu objeví, a zároveň je jeho fotografie v informačních systémech. Tyto pravomoci může policie a zpravodajské služby využívat různě intenzivně. Zákony v tomto ohledu nekladou prakticky žádná omezení. Přitom oprávněné orgány mají obecně tendenci vykládat své pravomoci co nejšířeji.[54]

Vzhledem k velmi neurčité formulaci znění obou novel, které hovoří pouze o možnosti zpracovávat digitální fotografie a identifikátory umožňující propojení do příslušných registrů státní správy, bez toho, aby bylo v textu zákona vymezeno o fotografie jakých osob může jít, jakým způsobem mají být využívány, a že by tato pravomoc měla sloužit k provádění biometrické identifikace, je otázkou, jestli lze takovou právní úpravu považovat za dostatečný právní základ pro využití biometrické identifikace při sledování veřejných prostor.

Nedostatky právní úpravy lze přirovnat k fungování kriminalistické databáze DNA, která se opírá o oprávnění policie odebírat genetické vzorky určitého okruhu osob a blíže nedefinuje, co se s těmito vzorky může dělat, a neupravuje ani fungování samotné kriminalistické databáze genetických profilů. Celé fungování kriminalistické databáze je pak upraveno interními pokyny policejního prezidenta, které nejsou veřejně dostupné. Tato praxe je dlouhodobě kritizována řadou subjektů a v současné době čeká na projednání před Ústavním soudem návrh na zrušení oprávnění policie genetické vzorky pro účely budoucí identifikace odebírat.[55]

4. Aplikační praxe v České republice

Rozsah využívání veřejných kamerových systémů, které automatizovaně zpracovávají osobní údaje, je do značné míry neprozkoumanou oblastí. Vzhledem k tomu, že jsou v některých případech využívány ve veřejných prostorech bez toho, aniž by byla veřejnost informována o jejich nasazení, bylo by náročné získat komplexní obraz jejich využití. Navíc se jedná o rychle se rozvíjející oblast a související informace rychle zastarávají. Níže uvedené příklady využívání technologií automatizovaného zpracovávání osobních údajů – zejména biometrických – ve veřejném prostoru v České republice nejsou tudíž komplexní analýzou, ale pouze upozorňují na některé způsoby jejich nasazení a vývoje. Ještě méně je známo o využívání biometrických systémů v soukromém sektoru, kterému se uvedené příklady nevěnují. Přesto je nutné upozornit, že dle Úřadu pro ochranu osobních údajů docházelo v posledních letech k nárůstu používání biometrických zařízení soukromými subjekty. V některých takových případech pak správce nezvažoval dostatečně požadavky na ochranu osobních údajů nebo je řešil pouze formálně. Například se jedná o používání biometrického dynamického podpisu v bankách a pojišťovnách, při doručování zboží či uzavírání zakázek velkými prodejci.[56] Podobnou aplikací využívání biometrických údajů v soukromoprávní sféře je nakonec opuštěný záměr městské části Prahy 1 dotovat zavedení biometrických zámků v rámci boje proti negativním dopadům krátkodobých pronájmů bytů.[57]

4.1 Kamerový systém s automatickou detekcí na Letišti Václava Havla Praha

Nejrozsáhlejší veřejně známý kamerový systém s automatickou detekcí biometrických údajů v České republice je provozován Policií ČR na Letišti Václava Havla v Praze. Systém biometrické detekce obličejů byl vybudovaný na základě usnesení vlády České republiky č. 47/2015, o zvýšení bezpečnosti na mezinárodním letišti Václava Havla v Praze, ze dne 19. 1. 2015. Prvních sto kamer bylo napojeno na software s automatickou detekcí obličejů na základě biometrických údajů a uvedeno do testovacího provozu v tranzitním prostoru letiště 15. 6. 2018. Na základě testovacího provozu bylo vyhodnoceno, že na pokrytí tranzitního prostoru stačí 100 namísto původně plánovaných 145 kamer. V březnu 2019 bylo rozhodnuto o rozmístění dalších 45 kamer ve veřejném prostoru letiště na místa s vysokou koncentrací osob, především kolem informačních tabulí, kde se cestující a jejich doprovod na delší dobu zastavují.[58] Ministerstvo vnitra dále plánuje zavedení podobných systémů na dalších mezinárodních letištích v České republice (Brno, Ostrava, Pardubice a Karlovy Vary).[59] Instalace biometrických kamerových systémů s detekcí obličeje měla být na zbývajících letištích dle plánu Ministerstva vnitra ČR realizována do konce roku 2020.[60]

Dodavatelé kamerového systému na Letiště Václava Havla Praha se ve smlouvě o realizaci uvedeného projektu zavázali, že systém bude uzpůsoben ***„pro hledání shod zachycených obličejů se zájmovými osobami jednotlivých klientů a pro vyhodnocování uložených záznamů z detekce obličejů s vyhledáváním ex post vložených fotografií osob“.*** [61] Celý kamerový systém s biometrickým zpracováním je pak propojen s dalšími bezpečnostními systémy a databázemi provozu letiště. Celková cena zavedení projektu integrace bezpečnostního systému s biometrickou detekcí obličejů v kamerových systémech byla na základě smluv a jejich dodatků do září 2020 více než 90 milionů korun.[62]

Detailní podmínky provozu kamerového systému s automatizovaným zpracováváním biometrických údajů na letišti nebyly zveřejněny. Ministerstvo vnit-

ra, které se na zavádění funkcí kamerového systému podílelo, uvedlo na svém webu a v tiskových zprávách pouze kusé informace. Provozovatel a gestor systému Ředitelství služby cizinecké policie pak považuje interní předpisy policie za informace, které je potřeba ze strategických důvodů tajit.[63] Také smlouva mezi Ministerstvem vnitra ČR s dodavateli zabezpečovacího systému obsahuje klauzule o mlčenlivosti, podle které jsou okolnosti a údaje získané v souvislosti s plněním zakázky považovány za důvěrné, a to včetně „specifikace předmětu plnění" v příloze smlouvy.[64] Kamerový systém na Letišti Václava Havla Praha z tohoto důvodu postrádá možnost detailnější kontroly ze strany veřejnosti.

Z informací poskytnutých Policií ČR není jednoznačné, jak a kým jsou biometrická data z kamerového systému aktivně využívána. Biometrická data získaná z kamerového systému Letiště Václava Havla Praha jsou Policií ČR porovnávána s informačním systémem Pátrání po osobách (PATROS), v němž jsou zpracovávány údaje o hledaných a pohřešovaných osobách. Kromě Policie ČR mají k záznamům z kamerového systému přístup také Celní správa České republiky a zpravodajské služby (Bezpečnostní informační služba a Vojenské zpravodajství), přičemž Policie ČR může údaje předávat ještě národnímu členovi Eurojustu,[65] Národnímu bezpečnostnímu úřadu, Národnímu úřadu pro kybernetickou a informační bezpečnost, Vojenské policii, Ministerstvu vnitra ČR, Vězeňské službě České republiky a dalším orgánům veřejné správy.[66] V jaké míře kamerový systém s biometrickým rozpoznáním obličeje jmenované státní orgány skutečně využívají, nebylo Policií ČR sděleno.

Údaj o chybovosti biometrického rozpoznávání ze záznamu kamer není znám. Od spuštění systému rozpoznávání obličejů na letišti dne 15. 6. 2018 až do 19. 8. 2020 došlo k celkem 189 shodám s osobami vedenými v zájmových databázích. Ovšem dle sdělení Policejního prezidia není nijak evidováno, kolik shod bylo takzvaně falešně pozitivních, což jsou shody, při kterých dojde k záměně náhodné osoby procházející po letišti s osobou v zájmové databázi.[67]

Podle našich zjištění je provoz kamerového systému s biometrickým rozpoznáním obličeje na Letišti Václava Havla Praha provozován bez řádného splnění všech zákonných povinností. Policie ČR si pro provozování systému nezpracovala obligatorní posouzení vlivu na ochranu osobních údajů dle Směrnice o ochraně údajů v oblasti prosazování práva. Policie to obhajuje tvrzením, že v době spuštění sledovacího systému do zkušebního provozu nebyla směrnice do národní legislativy transformována a postačovala prý ohlašovací povinnost Úřadu pro ochranu osobních údajů.[68]

Povinnost zpracovat tzv. posouzení vlivu na ochranu osobních údajů je stanovena v čl. 27 Směrnice o ochraně údajů v oblasti prosazování práva. Posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů musí správce údajů provést, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob.[69] Používání kamerových systémů k biometrickému rozpoznávání obličeje na veřejných prostranstvích tyto podmínky naplňuje a posouzení vlivu na ochranu osobních údajů bude podléhat vždy. Uvedené ustanovení směrnice je provedeno § 37 zákona č. 110/2019 Sb., o zpracování osobních údajů. Posouzení musí obsahovat alespoň obecný popis zamýšlených operací zpracování, posouzení rizik z hlediska práv a svobod subjektů údajů, plánovaná opatření k řešení těchto rizik, záruky, bezpečnostní opatření a mechanis-

my k zajištění ochrany osobních údajů a k doložení souladu s touto směrnicí, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Zákon o zpracování osobních údajů vešel v účinnost dne 24. 4. 2019, což je více než 14 měsíců poté, kdy byl spuštěn kamerový systém s biometrickou detekcí na Letišti Václava Havla Praha. Směrnice Evropského parlamentu a Rady většinou nemají přímý účinek ve vnitrostátním právu členských států, jako je to u nařízení. Nicméně v čl. 63 odst. 1 Směrnice o ochraně údajů v oblasti prosazování práva, který stanový podmínky provedení ve vnitrostátním právu, ukládá povinnost členských států přijmout, zveřejnit a uvést v platnost právní předpisy nezbytné pro dosažení souladu se směrnicí do 6. 5. 2018. Evropský soudní dvůr ve své judikatuře stanovil, že směrnice má přímý účinek, jsou-li její ustanovení bezpodmínečná, dostatečně jasná a přesná a pokud členský stát Evropské unie neprovedl směrnici ve stanovené lhůtě.[70] Přestože bylo později Evropským soudním dvorem určeno, že tento účinek je jenom vertikální vzestupný, v tomto případě je i tento požadavek splněn, protože směrnice ukládá povinnost členskému státu chránit citlivé osobní údaje jeho občanů.

Směrnice o ochraně údajů v oblasti prosazování práva také v čl. 57 ukládá členským státům povinnost stanovit sankce za porušení předpisů přijatých na základě této směrnice a přijmout veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující. Zákon o zpracování osobních údajů provádí toto ustanovení v Hlavě VI Přestupky, kde je v § 63 odst. 1 písm. k) zákona o zpracování osobních údajů stanoveno, že právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s § 37 zákona o zpracování osobních údajů neprovede posouzení vlivu na ochranu osobních údajů. Podle § 63 odst. 3. zákona o zpracování osobních údajů lze za tento přestupek uložit pokutu do 10 000 000 Kč.

Přestože byla Směrnice o ochraně údajů v oblasti prosazování práva přijata již 27. 4. 2016 a stanovovala členským státům povinnost provést ji do dvou let (6. 5. 2018), nebylo posouzení vlivu na ochranu osobních údajů pro kamerový systém s biometrickým rozpoznáváním obličeje na letišti Václava Havla Praha zpracováno od spuštění kamerového systému dne 15. 6. 2018 minimálně do 24. 8. 2020. Demonstruje to absenci vynucování evropské legislativy na ochranu osobních údajů při zavádění biometrického zpracovávání údajů bezpečnostními orgány.

Kromě výše uvedeného je třeba zdůraznit, že v čase docházelo ke změnám kamerového systému včetně navyšování počtu kamer a sledování dosud nesledovaných prostor, a to pravděpodobně minimálně u rozšíření o dalších 45 kamer v roce 2019 také již v době po účinnosti zákona o zpracování osobních údajů.

4.2 Biometrická identifikace nežádoucích osob na fotbalových stadionech

Podle vyjádření Úřadu pro ochranu osobních údajů mu byl v rámci konzultační činnosti sportovním klubem pořádající fotbalové zápasy předložen návrh na využití technologie rozpoznávání obličejů při vstupech na stadion. Navrhovaný systém měl mezi vstupujícími návštěvníky identifikovat osoby, které narušily průběh předchozích zápasů a byly po určitou dobu vyloučeny z návštěvy fotbalových utkání. Snadná identifikace měla pomoci zamezit nekontrolovanému vstupu těchto nežádoucích osob na fotbalové stadiony.

V reakci na to v srpnu 2019 vydal Úřad pro ochranu osobních údajů stanovisko, podle kterého ***„nelze najít dostatečný právní důvod ke zpracování biometrických osobních údajů návštěvníků fotbalového utkání technologií face recognition vlastníkem sportovního zařízení v postavení správce osobních údajů“.*** [71] V odůvodnění pak uvedl, že zpracování biometrických údajů by dle GDPR v tomto případě vyžadovalo výslovné zákonné zmocnění, které musí být přiměřené sledovanému cíli. Stávající zákon č. 115/2001 Sb., o podpoře sportu, který pouze obecně upravuje opatření k zajištění pořádku v průběhu sportovního podniku a vydání návštěvního řádu, pak nelze považovat za dostatečné zmocnění pro zpracování biometrických údajů. Úřad pro ochranu osobních údajů doporučil vyčkat novely zákona o podpoře sportu připravované ministerstvem vnitra, jejíž příprava má zahrnovat i posouzení vlivu na ochranu osobních údajů podle článku 35 odst. 2 písm. b) GDPR. Problém diváckého násilí biometrickou identifikací návštěvníků fotbalového utkání je v některých zemích (např. v Dánsku) řešeno právě na základě zákona zmocňujícího k biometrickému zpracování z důvodu zájmu fotbalovému klubu, pokud poskytne vhodné a konkrétní záruky ochrany osobních údajů požadované GDPR.[72]

Následně se Úřad pro ochranu osobních údajů v březnu 2020 vyjádřil k navrhované novele zákona o podpoře sportu, která by uvedené zákonné zmocnění obsahovala. Návrh zákona úřad nepodpořil z několika důvodů. Předně návrh zákona neodpoví-

dal požadavkům kladeným v GDPR na přípravu takového právního předpisu, který by měl v odůvodnění obsahovat posouzení vlivu na ochranu osobních údajů.[73] Posouzení vlivu na ochranu osobních údajů je povinnou součástí přípravy takového právního předpisu. V návrhu legislativních změn dále nebyla dostatečně zdůvodněna nezbytnost zpracování biometrických údajů ve srovnání s jinými možnostmi eliminace rizik násilí na stadionech.[74]

4.3 Biometrické rozpoznávání obličeje v kamerovém systému hlavního města Prahy

Ze strany Policie ČR je snaha zavést biometrické rozpoznávání obličeje také v městském kamerovém systému hlavního města Praha.[75] Na základě žádosti Policie ČR o aktivaci funkcionality rozpoznávání tváří na šesti lokalitách městského kamerového systému v Praze se Magistrát hlavního města Prahy obrátil v listopadu 2019 na Úřad pro ochranu osobních údajů se žádostí o konzultaci.[76] Z důvodu nutnosti zpracování posouzení vlivu na ochranu osobních údajů dle § 37 zákona o zpracování osobních údajů byl další postup ze strany Magistrátu hlavního města Prahy přenechán Policii ČR, která by byla současně zpracovatelem biometrických údajů získaných z kamerového systému.[77] Další kroky, které Policie ČR ve spolupráci s Úřadem pro ochranu osobních údajů činí, nejsou Magistrátu hlavního města Prahy známy, ani je samotná policie nezveřejnila.

V této souvislosti je třeba upozornit i na sporný aspekt využívání biometrické identifikace ze strany obecní či městské policie, která nedisponuje obdobným oprávněním ke zpracování digitálních fotografií jako Policie ČR, a která je přitom například v případě Prahy uváděna jako společný správce kamerového systému spolu s Policií ČR. Názory na možnost využívání kamer s biometrickou identifikací ze strany Městské policie se rozchází, klíčový Úřad pro ochranu osobních údajů spíše tuto možnost vylučuje.[78]

4.4 Financování technologického vývoje biometrických systémů z veřejných rozpočtů

Vývoj biometrického rozpoznávání obličeje a následné zpracování umělou inteligencí je financováno z veřejných rozpočtů České republiky. Financují se tímto způsobem projekty vyvíjející aplikace, jejichž nasazení v České republice a celé Evropské unii by nesplňovalo zákonné požadavky stanovené v GDPR a Směrnici o ochraně údajů v oblasti prosazování práva. Skrze Technologickou agenturu České republiky a další instituce jsou přerozdělovány veřejné prostředky v řádech desítek milionů korun na řadu projektů výzkumu a vývoje biometrického zpracování a umělé inteligence zpracovávající osobní údaje.

Může se jednat o projekty pro vývoj aplikací, které jsou původně určené pro použití v České republice, ale jejichž použití se následně ukáže jako neslučitelné s právní ochranou osobních dat. Příkladem může být projekt na vývoj automatizovaného panoramatického dohledového systému pro ochranu osob a majetku na sportovních stadionech, jehož realizace byla pro období let 2017 až 2020 podpořena ze státního rozpočtu Ministerstvem vnitra ČR částkou více než 16 milionů Kč. V hlavních cílech projektu bylo uvedeno: ***„Tyto metody umožní detekci a rozpoznání osob podle obličejů nebo oblečení v případě maskování, jejich sledování v davu a vyhledávání jejich pozice v obsáhlých záznamech.“*** [79] Právě uvedený projekt měl vyvíjet funkci rozpoznání dle obličeje osob na fotbalovém stadionu, což by dle stanoviska Úřadu pro ochranu osobních údajů bylo v rozporu s platnou legislativou na ochranu osobních údajů[80] (viz kapitola 4.2). Popsaný příklad, kdy je nejprve financován projekt v řádech milionů korun a následně je zjištěno, že užití jeho výsledků není právně aprobováno, by mohlo vést k postupné erozi a rozvolňování současné právní regulace, protože může docházet ke snahám výsledky vývoje nějakým způsobem uplatnit v praxi.

Dalším negativním efektem financování projektů biometrického zpracovávání a umělé inteligence ze státního rozpočtu je nepřímá podpora vlád nedemokratických režimů, kde nejsou funkční mechanismy ochrany lidských práv a kde je systém kontroly

zneužíván k potírání politické opozice. Může to být další krok, který následuje, pokud je nemožné využít výsledky aplikovaného výzkumu biometrického zpracování a umělé inteligence přímo v České republice nebo ve státech Evropské unie. Napovídá tomu další příklad, kdy proudí státní finanční podpora na ***„výzkum a vývoj nových modulů umělé inteligence pro sledování a detekci anomálií a predikci chování osob“.***[81] V dubnu 2020 na projekt vývoje popsaného softwaru pod názvem Cogniware Insights 2.0 dostala společnost Cogniware, s.r.o. státní dotaci ve výši více než 16,5 milionu korun.[82] Výsledky vývoje mají být zaměřeny ***„na vyšetřování a pokročilou analýzu podezřelých objektů, aktivit a vztahů s využitím prvků umělé inteligence a statistických analýz, která patří do oblasti známé jako analýza Big Data. Řešení bude obsahovat detekci anomálií, modulu pro klasifikaci objektů do skupin dle příbuznosti, predikci chování, rozpoznávání osob a objektů z obrazu a bude doporučovat vhodné postupy a prioritizace.“***[83] Cogniware Insights 2.0 by tak prakticky propojoval data získaná z kamerových systémů včetně biometrických dat s osobními daty získanými z jiných zdrojů, jako například sociální sítě. Analýzou dat by pak měl systém na základě algoritmu strojového učení vyhodnotit, jaký postup zvolit v případě zjištění podezřelého chování monitorované osoby.

Podle vyjádření samotné společnosti Cogniware, s.r.o. dodávají systémy využívající popsané technologie silovým složkám zemí Středního východu, zejména do Spojených arabských emirátů, Saúdské Arábie, Jordánska nebo Bahrajnu. Společnost to odůvodňuje právě tím, že ***„tyto státy mají volnější pravidla, co se ochrany osobních údajů týče“.***[84] V uvedených státech vládnou nedemokratické autoritářské režimy a hrozí v nich zneužití sledovacího systému k potlačování politické plurality a k potlačování lidských práv. Dle vyjádření společnosti, lze u vyvíjeného sledovacího systému různě upravit funkce, aby se přizpůsobil právní úpravě v jednotlivých zemích. Ačkoli cílem společnosti je dodávat v budoucnu tyto systémy také Policii ČR,[85] faktem je, že z českého státního rozpočtu se financuje vývoj sledovacího systému, který není plně kompatibilní s evropským právem a systémem ochrany osobních údajů, případně bude muset pro potřeby České republiky doznat dalších úprav.

Přitom používání sledovacích systémů umělé inteligence pro odhalování trestné činnosti lze u nás očekávat v následujících letech. Budoucí nasazení systémů umělé inteligence v činnosti českých orgánů v trestním řízení je zmiňováno také Nejvyšším státním zastupitelstvím, které ho považuje za nejvýznamnější technologický trend. Nejvyšší státní zastupitelství ve zprávě týkající se kybernetické kriminality uvádí: ***„Především tzv. prediktivní vyhledávání trestné činnosti, případně dovozování trestní odpovědnosti za ´připravovanou trestnou činnost´ za pomoci jednoduché umělé inteligence, je dnes v některých zemích světa již realitou.“***[86]

Zásadním nedostatkem je, že technologický vývoj v této oblasti dalece předbíhá společenskou debatu o právních a etických důsledcích technologií využívajících biometrické zpracování a umělou inteligenci.

4.5 Nákupy mobilních inspekčních biometrických systémů Policií České republiky

Celkový rozsah a konkrétní způsob využívání kamer s biometrickým rozpoznáváním obličeje Policií ČR není ve své komplexnosti veřejně znám a lze ho pouze domýšlet z některých neúplných informací. Přestože na žádost o informace, zda a kde jsou Policií ČR využívány kamerové systémy s funkcí rozpoznávání obličeje, bylo Policejním prezidiem oznámeno pouze Letiště Václava Havla Praha,[87] z registru smluv vyplývá, že došlo k nákupům biometrických technologií již před pořízením biometrického systému na pražském letišti. Se společností AUROTON COMPUTER, spol. s r.o., která je mimo jiné spoludodavatelem systému rozpoznávání obličeje na Letišti Václava Havla Praha, uzavřelo Ministerstvo vnitra ČR několik smluv na dodávky vybudování komplexního informačního systému pro inspekci a kontrolu osob a dokladů pomocí biometrických prvků pro potřeby Policie ČR.[88]

Záměrem uvedené dodávky biometrické technologie zřejmě není plošné biometrické sledování ve veřejných prostorech, ale kontrola totožnosti konkrétních osob vybudováním komplexního informačního systému pro kontrolu osob a dokladů pomocí biometrických prvků. To spočívá v dodání technologie a softwaru, které by umožňovaly mobilní kontrolu identity osob oproti databázím za využití biometrických prvků, jako jsou otisky prstů a rozpoznání tváře, a prověření na výskyt ve sledovaných datových fondech Policie ČR a ostatních bezpečnostních složek, členských států Evropské unie a mezinárodních organizací.[89] Konkrétní popis funkcionalit dodané technologie byl z registru smluv odstraněn a je pokryt klauzulemi mlčenlivosti stran, tudíž možnosti zneužití dodaného systému jiným způsobem než jsou zákony aprobované nelze zcela vyloučit. Uživatelská praxe těchto technologií je především na jednotlivých Krajských ředitelstvích Policie ČR, do kterých dodávka technologických zařízení směřovala.

V tomto směru je zajímavá také webová prezentace dodavatele, kde je na úvodní stránce uvedeno: ***„Naše společnost dlouhodobě poskytuje služby***

v oblasti biometrické kontroly osob. Nově jsme schopni vám dodat systémy na rozpoznávání obličejů včetně nadstavbového systému umožňující založení vlastní databáze žádoucích a nežádoucích osob umožňující například automatický vstup do areálů či naopak vyhlášení alarmu při objevení se osoby nežádoucí." [90] Mezi zákazníky různých produktů společnosti je celá řada ministerstev, státních orgánů a soukromých osob, z čehož ovšem nelze jednoznačně dovodit, kdo technologie biometrického zpracování obličeje skutečně užívá. Přesto lze na základě komerční nabídky technologií očekávat, že užívání biometrických systémů identifikace bude již dnes rozšířeno také mimo bezpečnostní složky státu.

5. Navrhované kroky k regulaci v rámci České republiky

Používání technologie pro necílené zpracování biometrických údajů ve veřejných prostorech, ať už donucovacími orgány, dalšími veřejnými orgány nebo soukromými subjekty, přináší značné problémy v oblasti základních práv a svobod jednotlivce. Analýza základních práv ukazuje, že biometrické zpracování ve veřejných prostorech způsobem plošného sledování je jen obtížně slučitelné se základními právy. Dostává se do rozporu zejména s právem na soukromí, právem na informační sebeurčení a důstojností. Zásah to těchto práv může být v rozporu se zásadami nezbytnosti a proporcionality.

V České republice lze uplatnit čtyři mezinárodní právní nástroje, které vylučují plošné biometrické sledování. V nejširším smyslu to jsou Evropská úmluva o lidských právech a Listina základních práv Evropské unie, konkrétněji pak GDPR a její sesterský nástroj – Směrnice o ochraně údajů v oblasti prosazování práva. České zákony pak poskytují bližší úpravu v zákoně o zpracování osobních údajů a občanském zákoníku. V praxi však nejsou všechny instrumenty evropského a českého práva plně vymáhány. Má to za následek skutečnost, že došlo k zavedení necíleného biometrického zpracování biometrických údajů občanů pohybujících se na Letišti Václava Havla Praha bez řádného zákonného posouzení vlivu na ochranu osobních údajů a jsou postupně vyvíjeny a plánovány další aplikace. Tento stav je neslučitelný s českými a evropskými právními předpisy. Současně postupně dochází k legislativním změnám, které dávají některým bezpečnostním sborům stále širší a nekonkrétní oprávnění k využívání biometrických fotografií, jež je interpretováno jako oprávnění k nasazení plošného biometrického sledování. V této souvislosti se jedná o změny zákona o Policii České republiky, zákona o Vojenské policii a zákona o zpravodajských službách České republiky.

Biometrické zpracování umožňující plošné sledování je v zásadním rozporu s podstatou lidské důstojnosti, demokratické společnosti, základních práv a svobod, ochrany osobních údajů, procesních práv

a právního státu. Rizika pro zvyšování mocenské nerovnováhy, diskriminace, rasismu, nerovností a autoritářské společenské kontroly skrze plošné biometrické sledování jsou příliš vysoká oproti jakýmkoliv možným „výhodám", které by použití těchto technologií mohlo představovat. Z toho důvodu lze na úrovni České republiky navrhnout následující kroky:

1. Zastavit veškerá biometrická zpracování určená k plošnému sledování ve veřejných prostorech, a to včetně již zavedených, tak plánovaných projektů. Touto cestou šlo například město San Francisco, když se v květnu 2019 stalo prvním městem ve Spojených státech, které zakázalo používání technologie rozpoznávání obličeje veřejným institucím. Jedním z důvodů byla neodůvodněnost zásahu do soukromí. Zákaz se týká činností prováděných samosprávou, jako jsou dopravní instituce nebo lokální bezpečnostní složky, ale nevztahuje se na činnosti federálních úřadů.[91]

2. Ve spolupráci s Úřadem pro ochranu osobních údajů zveřejnit všechny stávající a plánované systémy využívající biometrickou identifikaci včetně jejich funkcí a rozmístění. Agentura Evropské unie pro základní práva tvrdí, že „jsou v současné době v členských státech EU k dispozici pouze omezené informace o možném použití nebo testech využívaných technologií pro rozpoznávání podle obličeje".[92] To potvrzuje i naše snaha získat potřebné informace od zodpovědných státních orgánů v České republice. Je potřeba informovat širokou veřejnost o všech biometrických aplikacích, které zpracovávají citlivé osobní údaje občanů. Závazek poskytovat informace musí být z aktérů vyvíjejících a zavádějících biometrické technologie vymožen.

3. Zastavit zavádění právních předpisů, které umožňují biometrické zpracování k plošnému sledování ve veřejných prostorech. Jasné a předvídatelné zákony by měly umožňovat pouze cílené zpracovávání biometrických údajů, které je přiměřené daným problémům a kontextu, a měly by poskytovat účinné prostředky proti zneužití. Úřad pro ochranu osobních údajů může hrát roli tím, že bude v legislativním procesu radit a požadovat konkrétní opatření.

4. Přezkoumat a vyhodnotí všechny právní předpisy týkající se biometrického plošného sledování ve veřejných prostorech z hlediska základních práv.

5. Zastavit financování výzkumu biometrických technologií z veřejných rozpočtů a zajistit, že bude podporován pouze vývoj takových aplikací, které jsou v souladu s lidskými právy na mezinárodní úrovni.

6. Poznámky

1) European Digital Rights. Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States. Str. 7 [Online]. 2020. [cit. 2020-08-09]. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

2) Lin L., Hou Z. Combat COVID-19 with artificial intelligence and big data. Journal of Travel Medicine, Vol. 27, Issue 5, (July 2020), https://doi.org/10.1093/jtm/taaa080

3) Úřad pro ochranu osobních údajů. Výroční zpráva ÚOOÚ za rok 2019. [Online]. 2020. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019, str. 63. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocni%2Dzprava%2Dza%2Drok%2D2019

4) European Union Agency for Fundamental Rights. 2020. [Online]. Informace uveřejněná na sociálních sítích agentury. [cit. 2020-09-16]. Dostupné z: https://twitter.com/EURightsAgency/status/1234804039449239553

5) Smith A. Sweden Gets First GDPR Fine After Facial Recognition Used in School. [Online]. 2019. [cit. 2020-08-09]. Dostupné z: https://www.pcmag.com/news/sweden-gets-first-gdpr-fine-after-facial-recognition-used-in-school

6) Gill M., Spriggs A. Vyhodnocení účinku kamerových systémů. 2007. Český překlad: Institut pro kriminologii a sociální prevenci, Praha, str. 109. ISBN 978-80-7338-061-8.

7) European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. [Online]. Str. 2, 2019. ISBN 978-92-9474-839-3, doi: 10.2811/231789 [cit. 2020-09-18]. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

8) Nález německého ústavního soudu ze dne 15. prosince 1983. 1 BvR 209/83, bod 146, Dostupné z: https://www.bverfg.de/e/rs19831215_1bvr020983.html

9) European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. [Online]. Str. 8, 2019. ISBN 978-92-9474-839-3, doi:10.2811/231789 [cit. 2020-09-18]. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

10) The iPhone X's Face ID thinks these two brothers are the same person. [Online]. 2017. MSPoweruser [cit. 2020-09-18]. Dostupné z: https://mspoweruser.com/iphone-xs-face-id-thinks-two-brothers-person

11) Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test. Part 3: Demographic Effects. [Online]. Str. 2, 2019. National Institute of Standards and Technology. U.S. Department of Commerce. [cit. 2020-08-09]. Dostupné z: https://doi.org/10.6028/NIST.IR.8280

12) Václavíková J. "Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře. [Online]. 2020. [cit. 2020-08-09]. Dostupné z: https://zpravy.aktualne.cz/zahranici/pocitac-se-spletl-policie-zatkla-spatneho-muze-kvuli-technol/r~b3cdeb14c1cb11ea8972ac1f6b220ee8/

13) Doffman Z. New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report. [Online]. 2019. [cit. 2020-09-18]. Dostupné z: https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/

14) Ungerleider N. The Dark Side Of Biometrics: 9 Million Israelis' Hacked Info Hits The Web. [Online]. 2011. [cit. 2020-08-09]. Dostupné z: https://www.fastcompany.com/1790444/dark-side-biometrics-9-million-israelis-hacked-info-hits-web

15) Schwartz J. Facial recognition challenged by French administrative court. [Online]. 2020. [cit. 2020-09-18]. Dostupné z: https://www.engage.hoganlovells.com/knowledgeservices/news/facial-recognition-challenged-by-french-administrative-court

16) European Digital Rights. Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States. [Online]. Str. 14, 2020. [cit. 2020-08-09]. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

17) Cogniware. Umělá inteligence z Česka pomáhá chytat zločince po celém světě. Tisková zpráva společnosti Cogniware ze dne 3. září 2020.

18) Dixon P., Gellman R. [Online]. The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future. 2014. World Privacy Forum. [cit. 2020-09-18]. Dostupné z: www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf

19) Botsman R. Big data meets Big Brother as China moves to rate its citizens. [Online]. 2017. [cit. 2020-10-07]. Dostupné z: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

20) Barrett L.F., Adolphs R., Marsella S., Martinez A.M., Pollak S.D. Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements. Str. 57, 2019. Psychological Science in the Public Interest, Vol 20, Issue 1, https://doi.org/10.1177%2F1529100619832930

21) European Digital Rights. Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States. [Online]. Str. 16, 2020. [cit. 2020-08-09]. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

22) Evropský inspektor ochrany údajů je nezávislý dozorový úřad, jehož hlavním cílem je zajistit, aby orgány a instituce EU respektovaly právo na soukromí a ochranu údajů při zpracování osobních údajů.

23) European Data Protection Supervisor. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. [Online]. 2019. [cit. 2020-09-18]. Dostupné z: https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

24) Rozsudek Evropského soudu pro lidská práva S. a Marper proti Spojenému království (2008), paragraf 66.

25) Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 294, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

26) Úmluva je pod Radou Evropy, v České republice v publikovaná jako Smlouva č. 115/2001 Sb. m. s.

27) Rozhodnutí Evropského soudu pro lidská práva ve věci Amann proti Švýcarsku (2000), bod 65.

28) Rozhodnutí Evropského soudu pro lidská práva ve věci Peck proti Spojenému království (2003), bod 133.

29) Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 290, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

30) Nález pléna Ústavního soudu České republiky. Pl. ÚS 24/10, bod 29.

31) Rozhodnutí Evropského soudu pro lidská práva ve věci S. a Marper proti Spojenému království (2008), paragraf 125.

32) Rozhodnutí Soudního dvora EU ve spojených věcech C-293/12 a C-594-12 Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a dalším (2014) ECR I-238, bod 57.

33) Jde o tři Rozhodnutí soudního dvora Evropské unie ve spojených věcech C 203/15 a C 698/15 ze dne 21. 12. 2016, ve věci C 623/17 z 6. 10. 2020 a ve spojených věcech C-511/18, C-512/18 a C-520/18 rovněž z 6. 10. 2020.

34) Rozhodnutí Soudního dvora EU ve věci C-362/14, Schrems v Data Protection Commissioner (2015), ECLI:EU:C:2015:650, bod 94.

35) Barak A. Human Dignity: The Constitutional Value and the Constitutional Right. 2015. Human Rights Law Review, Vol. 16, Issue 1, str. 176. https://doi.org/10.1093/hrlr/ngv042

36) Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 286, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

37) 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)

38) 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.

39) Jedná se o švédský úřad pro ochranu osobních údajů obdobný českému Úřadu pro ochranu osobních údajů.

40) Smith A. Sweden Gets First GDPR Fine After Facial Recognition Used in School. [Online]. 2019. [cit. 2020-08-09]. Dostupné z: https://www.pcmag.com/news/sweden-gets-first-gdpr-fine-after-facial-recognition-used-in-school

41) Pattynová J., Suchánková L., Černý J., Růžička M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. Str. 540, 2019. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-396-4.

42) Pracovní skupina 29 byla ustanovena článkem 29 směrnice 95/46/EC a zanikla a nabytím účinností GDPR. Jednalo se o nezávislý evropský poradní orgán na ochranu osobních údajů. Byla složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie. Účinností GDPR od 25. května 2018 se změnila v Evropský sbor pro ochranu osobních údajů (EPDB). Jeho úkolem je především zajišťování jednotného uplatňování ochrany dat a za tím účelem monitorovat míru ochrany dat a vydávatpokyny, doporučení a osvědčené postupy.

43) Evropská komise. Stanovisko k některým klíčovým otázkám směrnice o prosazování práva (EU 2016/680). 2017. Stanovisko pracovní skupiny pro ochranu údajů zřízené podle článku 29 přijaté dne 29. listopadu 2017.

44) Bílá kniha je obecně autoritativní zpráva nebo průvodce, který informuje o určitém problému a představuje filozofii Evropské unii v dané věci. Má pomoci porozumět problematice, vyřešit určité otázky nebo učinit rozhodnutí.

45) European Commission. White Paper: On Artificial Intelligence – A European approach to excellence and trust. 2020. Dostupné z: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

46) European Digital Rights. Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States. [Online]. Str. 18, 2020. [cit. 2020-08-09]. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

47) Oblast osobnostních práv je upravena v paragrafech 81 až 90 občanského zákoníku.

48) Krausová A., Matejka J., Ivančo A., Fialová E., Žolnerčíková V., Ščerba T. Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR. Výzkum potenciálu rozvoje umělé inteligence v České republice. Úřad vlády České republiky, str. 32, 2018.

49) Zásada autonomie vůle je v soukromém právu vyjádřena v § 3 odst. 1 občanského zákoníku. Ta se promítá do oblasti zpracování osobních údajů, kdy si fyzická osoba může zvolit, kterému správci udělí souhlas se zpracováním osobních údajů, a ke kterým konkrétním účelům zpracování.

50) Krausová A. Zásada autonomie v ochraně soukromí: Možnosti a limity v rozhodování o vlastních biometrických údajích. Článek byl publikován v časopise Právní rozhledy č. 6, str. 11, 2018.

51) Úřad pro ochranu osobních údajů. Změna v hodnocení úrovně právní ochrany biometrických údajů. [Online]. Stanovisko Úřadu pro ochranu osobních údajů ze dne 8. června 2017. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/zmena-v-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850

52) § 11 a § 13 vyhlášky č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu.

53) Dvořáková V., Černá Z. Průlom do soukromí. České zpravodajské služby chtějí vlastní databázi rozpoznávání obličejů. [Online]. Článek na Seznamzpravy.cz ze dne 23. července 2019. [cit. 2020-09-20]. Dostupné na: https://www.seznamzpravy.cz/clanek/prulom-do-soukromi-ceske-zpravodajske-sluzby-chteji-vlastni-databazi-rozpoznavani-obliceju-76242?seq-no=4&dop-ab-variant=&source=clanky-home

54) Malecký R. Velký bratr 2019: Pražská energetika, BIS, Avast. Pozitivní cenu má pražská koalice za odmítnutí sledovacího systému. [Online]. Článek na Hlídacím psu ze dne 4. března 2020. [cit. 2020-09-20]. Dostupné na: https://hlidacipes.org/velky-bratr-2019-prazska-energetika-bis-avast-pozitivni-cenu-ma-prazska-koalice-za-odmitnuti-sledovaciho-systemu/

55) Návrh byl podán JUDr. Ing. Vierou Horčicovou, soudkyní Městského soudu v Praze a věc je vedena pod sp. zn. Pl. ÚS 7/18.

56) Úřad pro ochranu osobních údajů. Výroční zpráva ÚOOÚ za rok 2019. [Online]. 2020. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019, str. 62. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocni%2Dzprava%2Dza%2Drok%2D2019

57) Heller J. Bez otisku prstu vstup zakázán. Radnice zaplatí Pražanům nové zámky proti Airbnb. [Online]. Článek na Aktuálně ze dne 6. března 2020. [cit. 2020-10-09]. Dostupné na: https://zpravy.aktualne.cz/regiony/praha/hosty-airbnb-maji-zastavit-zamky-na-otisk-prstu/r~295100105f8e11eab115ac1f6b220ee8/

58) Ministerstvo vnitra České republiky. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů. Tisková zpráva ze dne 4. března 2019. [cit. 2020-09-18]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx

59) Česká televize. Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti. [Online]. 2019. [cit. 2020-09-15]. Dostupné z: https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologii-na-rozpoznavani

60) Ministerstvo vnitra České republiky. Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích. Tisková zpráva ze dne 18. února 2018. [cit. 2020-08-09]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx

61) Smlouva o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. uzavřená dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-108/ČJ-2015-990656.

62) Dodatel č. 6 ke smlouvě o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-197/ČJ-2015-990656.

63) Rozhodnutí o částečném odmítnutí žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů vydané dne 20. srpna 2020 Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-6/ČJ-2020-990810. V současné době (prosinec 2020) po zrušení tohoto rozhodnutí ze strany Ministerstva vnitra je očekáváno nové rozhodnutí
ve věci.

64) Smlouva o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. uzavřená dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-108/ČJ-2015-990656.

65) Eurojust (Jednotka Evropské unie pro justiční spolupráci) je agenturou Evropské unie zřízenou za účelem zvýšení efektivity mezinárodní justiční spolupráce v trestních věcech mezi členskými státy Evropské unie, zejména v oblasti vyšetřování a stíhání závažné přeshraniční kriminality a organizovaného zločinu.

66) Částečné poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-5/ČJ-2020-990810.

67) Částečné poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodnémpřístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-5/ČJ-2020-990810.

68) Částečné poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-5/ČJ-2020-990810.

69) Pattynová J., Suchánková L., Černý J., Růžička M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. Str. 630, 2019. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-396-4.

70) Rozhodnutí Evropského soudního dvora ze dne 4. prosince 1974 ve věci Yvonne van Duyn proti Home Office (41/74).

71) Úřad pro ochranu osobních údajů. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Stanovisko ze dne 16. srpna 2019. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

72) Úřad pro ochranu osobních údajů. Výroční zpráva ÚOOÚ za rok 2019. [Online]. 2020. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019, str. 57. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocni%2Dzprava%2Dza%2Drok%2D2019

73) Úřad pro ochranu osobních údajů. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Verze 1.0. [Online]. Manuál Úřadu pro ochranu osobních údajů ze dne 8. ledna 2020. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/seznam-druhu-operaci-zpracovani-ne-podlehajicich-pozadavku-na-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=1&p1=3938

74) Úřad pro ochranu osobních údajů. Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech. Zpráva ze dne 27. března 2020. [cit. 2020-09-01]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40780&n=vyjadreni%2Duoou%2Dk%2Dnavrhu%2Dregulace%2Dnasili%2Dna%2Dfotbalovych%2Dstadionech

75) Česká televize. Pražští policisté „otevírají diskusi" o technologii na rozpoznávání obličejů. Hřib je proti. [Online]. 2019. [cit. 2020-09-15]. Dostupné z: https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologii-na-rozpoznavani

76) Úřad pro ochranu osobních údajů. Vyjádření k žádosti o konzultaci k městskému kamerovému systému hl. m. Prahy. Vyjádření ze dne 3. prosince 2019.

77) Poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 18. srpna 2020 vydané Odborem informatické infrastruktury Magistrátu hlavního města Praha pod číslem jednacím MHMP 1270148/2020.

78) Cidlina V., Prokůpek, J. Legalita zavedení technologie rozpoznávání obličeje. [Online]. Článek na Advokatnidenik.cz ze dne 14. 9. 2020 [cit. 2021-01-05] Dostupné na: https://advokatnidenik.cz/2020/09/14/legalita-zavedeni-technologie-rozpoznavani-obliceje/#_ftn2

79) Technologická agentura České republiky. Automatizovaný panoramatický dohledový systém pro ochranu osob a majetku na sportovních stadionech. [cit. 2020-09-14]. Dostupné z: https://starfos.tacr.cz/cs/project/VI20172020105?query_code=q4piaacjw5tq#project-main

80) Úřad pro ochranu osobních údajů. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Stanovisko ze dne 16. srpna 2019. [cit. 2020-08-09]. Dostupné z: https://www.uoou.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

81) Technologická agentura České republiky. Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob. [cit. 2020-09-14]. Dostupné z: https://starfos.tacr.cz/cs/project/FW01010562?query_code=q4piaacjw5tq

82) Smlouva o poskytnutí podpory mezi Česká republika – Technologická agentura České republiky a Cogniware, s.r.o. k projektu č . FW01010562 s názvem Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob.

83) Technologická agentura České republiky. Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob. [cit. 2020-09-14]. Dostupné z: https://starfos.tacr.cz/cs/project/FW01010562?query_code=q4piaacjw5tq

84) Cogniware. Umělá inteligence z Česka pomáhá chytat zločince po celém světě. Tisková zpráva společnosti Cogniware ze dne 3. 9. 2020.

85) Hlaváčová K. Stačí oči a kousek nosu či chůze. Česká kamera rozpozná člověka i konkrétní auto. [Online]. 2020. [cit. 2020-09-15]. Dostupné z: https://zpravy.aktualne.cz/domaci/staci-oci-a-kousek-nosu-ci-chuze-cesky-kamerovy-system-pozna/r~0db5c8b2ee8c11eaa6f6ac1f6b220ee8/

86) Klement P. Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019. V Brně dne 29. ledna 2020, 3 SE 101/2020, str. 17.

87) Částečné poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-5/ČJ-2020-990810.

88) Kupní smlouva mezi Českou republikou - Ministerstvem vnitra a společností AUROTON COMPUTER, spol. s r.o. uzavřená dne 22. prosince 2016 uzavřená na základě a v souladu s výsledky veřejné zakázky „Vybudování mobilního biometrického inspekčního systému a dodávka kontrolních zařízení". Číslo jednací objednatele PPR-22247-26/ČJ-2016-990656.

89) Kupní smlouva mezi Českou republikou - Ministerstvem vnitra a společností AUROTON COMPUTER, spol. s r.o. uzavřená dne 22. prosince 2016 uzavřená na základě a v souladu s výsledky veřejné zakázky „Vybudování mobilního biometrického inspekčního systému a dodávka kontrolních zařízení". Číslo jednací objednatele PPR-22247-26/ČJ-2016-990656.

90) Webová prezentace AUROTON COMPUTER, spol. s r.o. [cit. 2020-09-16]. Dostupné z: https://www.auroton.cz/

91) Lee D. San Francisco is first US city to ban facial recognition. [Online]. 2019. [cit. 2020-08-09]. Dostupné z: https://www.bbc.com/news/technology-48276660

92) European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. [Online]. Str. 11, 2019. ISBN 978-92-9474-839-3, doi:10.2811/231789 [cit. 2020-09-18]. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra--2019-facial-recognition-technology-focus-paper-1_en.pdf

7. Zdroje

Barak A. Human Dignity: The Constitutional Value and the Constitutional Right. 2015. Human Rights Law Review, Vol. 16, Issue 1. https://doi.org/10.1093/hrlr/ngv042

Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

Botsman R. Big data meets Big Brother as China moves to rate its citizens. [Online]. 2017. Dostupné z: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Cidlina V., Prokůpek, J. Legalita zavedení technologie rozpoznávání obličeje. [Online]. Článek na Advokatnidenik.cz ze 14. 9. 2020 [cit. 2021-01-05] Dostupné na: https://advokatnidenik.cz/2020/09/14/legalita-zavedeni-technologie-rozpoznavani-obliceje/#_ftn2

Cogniware. Umělá inteligence z Česka pomáhá chytat zločince po celém světě. Tisková zpráva společnosti Cogniware ze 3. 9. 2020.

Česká televize. Pražští policisté „otevírají diskusi" o technologii na rozpoznávání obličejů. Hřib je proti. [Online]. 2019. Dostupné z: https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologii-na-rozpoznavani

Doffman Z. New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report. [Online]. 2019. Dostupné z: https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/

European Commission. White Paper: On Artificial Intelligence – A European approach to excellence and trust. 2020. Dostupné z: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Digital Rights. Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States. [Online]. 2020. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. [Online]. 2019. ISBN 978-92-9474-839-3, doi:10.2811/231789. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

Evropská komise. Stanovisko k některým klíčovým otázkám směrnice o prosazování práva (EU 2016/680). 2017. Stanovisko pracovní skupiny pro ochranu údajů zřízené podle článku 29 (Working Group 29) přijaté 29. 11. 2017.

Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test. Part 3: Demographic Effects. [Online]. 2019. National Institute of Standards and Technology. U.S. Department of Commerce. Dostupné z: https://doi.org/10.6028/NIST.IR.8280

Heller J. Bez otisku prstu vstup zakázán. Radnice zaplatí Pražanům nové zámky proti Airbnb. [Online]. Článek na Aktuálně 6. 3. 2020. Dostupné na: https://zpravy.aktualne.cz/regiony/praha/hosty-airbnb-maji-zastavit-zamky-na-otisk-prstu/r~295100105f8e11eab115ac1f6b220ee8/

Klement P. Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019. V Brně 29. 1. 2020, 3 SE 101/2020.

Krausová A., Matejka J., Ivančo A., Fialová E., Žolnerčíková V., Ščerba T. Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR. Výzkum potenciálu rozvoje umělé inteligence v České republice. Úřad vlády České republiky, 2018.

Krausová A. Zásada autonomie v ochraně soukromí: Možnosti a limity v rozhodování o vlastních biometrických údajích. Článek byl publikován v časopise Právní rozhledy, č. 6/2018, s. 191 an.

Kroupa J. E-shop na dálniční známky byl zástěrkou pro tajný sledovací systém. [Online]. Článek na Seznam Zprávy 3. 2. 2020. Dostupné z: https://www.seznamzpravy.cz/clanek/e-shop-na-dalnicni-znamky-byl-zasterkou-pro-tajny-sledovaci-system-87866

Lee D. San Francisco is first US city to ban facial recognition. [Online]. 2019. Dostupné z: https://www.bbc.com/news/technology-48276660

Lin L., Hou Z. Combat COVID-19 with artificial intelligence and big data. Journal of Travel Medicine, Vol. 27, Issue 5, (July 2020), https://doi.org/10.1093/jtm/taaa080

Malecký R. Velký bratr 2019: Pražská energetika, BIS, Avast. Pozitivní cenu má pražská koalice za odmítnutí sledovacího systému. [Online]. Článek na Hlídacím psu 4. 3. 2020. Dostupné na: https://hlidacipes.org/velky-bratr-2019-prazska-energetika-bis-avast-pozitivni-cenu-ma-prazska-koalice-za-odmitnuti-sledovaciho-systemu/

Ministerstvo vnitra České republiky. Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích. Tisková zpráva z 18. 2. 2018. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx

Ministerstvo vnitra České republiky. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů. Tisková zpráva z 4. 3. 2019. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx

Nonnemann F., Skácelová M. Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR). [Online]. 2017. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html

Pattynová J., Suchánková L., Černý J., Růžička M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. 2019. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-396-4.

Schwartz J. Facial recognition challenged by French administrative court. [Online]. 2020. Dostupné z: https://www.engage.hoganlovells.com/knowledgeservices/news/facial-recognition-challenged-by-french-administrative-court

Smith A. Sweden Gets First GDPR Fine After Facial Recognition Used in School. [Online]. 2019. Dostupné z: https://www.pcmag.com/news/sweden-gets-first-gdpr-fine-after-facial-recognition-used-in-school

The iPhone X's Face ID thinks these two brothers are the same person. [Online]. 2017. MSPoweruser. Dostupné z: https://mspoweruser.com/iphone-xs-face-id-thinks-two-brothers-person

Tři česká města testují chytré kamery, které rozpoznají SPZ, barvu a výrobce vozidla. [Online]. 2019. Dostupné z: https://www.systemonline.cz/zpravy/tri-ceska-mesta-testuji-chytre-kamery-ktere-rozpoznaji-spz-barvu-a-vyrobce-vozidla-z.htm

Ungerleider N. The Dark Side Of Biometrics: 9 Million Israelis' Hacked Info Hits The Web. [Online]. 2011. Dostupné z: https://www.fastcompany.com/1790444/dark-side-biometrics-9-million-israelis-hacked-info-hits-web

Úřad pro ochranu osobních údajů. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Verze 1.0. [Online]. Manuál Úřadu pro ochranu osobních z 8. 1. 2020. Dostupné z: https://www.uoou.cz/seznam-druhu-operaci-zpracovani-ne-podlehajicich-pozadavku-na-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=1&p1=3938

Úřad pro ochranu osobních údajů. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Stanovisko z 16. 8. 2019. Dostupné z: https://www.uoou.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

Úřad pro ochranu osobních údajů. Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech. Zpráva z 27. 3. 2020. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40780&n=vyjadreni%2Duoou%2Dk%2Dnavrhu-%2Dregulace%2Dnasili%2Dna%2Dfotbalovych%2D-stadionech

Úřad pro ochranu osobních údajů. Výroční zpráva ÚOOÚ za rok 2019. [Online]. 2020. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocni%2Dzprava%2Dza%2Drok%2D2019

Úřad pro ochranu osobních údajů. Změna v hodnocení úrovně právní ochrany biometrických údajů. [Online]. Stanovisko Úřadu pro ochranu osobních údajů z 8. 6. 2017. Dostupné z: https://www.uoou.cz/zmena-v-hodnoceni-urovne-pravni-ochrany--biometrickych-udaju/d-23850

Václavíková J. „Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře. [Online]. 2020. Dostupné z: https://zpravy.aktualne.cz/zahranici/pocitac-se-spletl-policie-zatkla-spatneho-muze-kvuli-technol/r~b3cdeb14c1cb11ea-8972ac1f6b220ee8/

Zákonné předpisy

Úmluva o ochraně lidských práv a základních svobod. Rada Evropy 1950. Úmluva byla ratifikována 18. 3. 1992 a publikována pod č. 209/1992 Sb.

Listina základních práv a Evropské unie 2012/C 326/02.

Listina základních práv a svobod. Ústavní zákon č. 2/1993 Sb.

Nařízení Evropského parlamentu a Rady (EU) z 27. 4. 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).

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.

Zákon č. 110/2019 Sb., o zpracování osobních údajů.

Zákon č. 273/2008 Sb., o Policii České republiky.

Zákon č. 89/2012 Sb., občanský zákoník.

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky.

Zákon č. 111/2019 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Zákon č. 300/2013 Sb., o Vojenské policii a o změně některých zákonů.

Zákon č. 262/2006 Sb., zákoník práce.

Zákon č. 115/2001 Sb., o podpoře sportu.

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

Využití biometriky při sledování veřejného prostoru v České republice

Mgr. et Mgr. Václav Mach, Ph.D.
Mgr. et Mgr. Jan Vobořil, Ph.D.

Vydalo Iuridicum Remedium, z.s.
Přístavní 1236/35, 170 00 Praha 7 (sídlo)
Jeseniova 10, 130 00 Praha 3 (kancelář)

Kontakt
420 776 703 170
iure@iure.org
www.iure.org
www.digitalnisvobody.cz
www.bigbrotherawards.cz