Univerzita Palackého v Olomouci
Právnická fakulta

Václav Mach

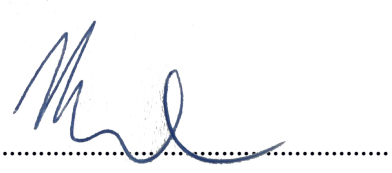
Kamerové systémy s biometrickým rozpoznáváním obličeje na veřejném prostranství

Diplomová práce

Olomouc 2024

Prohlašuji, že jsem diplomovou práci na téma "Kamerové systémy s biometrickým rozpoznáváním obličeje na veřejném prostranství" vypracoval samostatně a citoval jsem všechny použité zdroje. Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 119 266 znaků včetně mezer.

V Olomouci dne 25. března 2024



.....

Václav Mach

Obsah

Seznam použitých zkratek

ČR – Česká republika

DPIA – Posouzení vlivu na ochranu osobních údajů (z anglického *„data protection impact assessment“*)

ESLP - Evropský soud pro lidská práva

EU - Evropská Unie

EÚLP - Evropská úmluva o ochraně lidských práv

GDPR - Obecné nařízení ochrany údajů

IS DPO – Informační systém Digitální podoba osob

InfZ – Zákon o svobodném přístupu k informacím

KŘP ÚK – Krajské ředitelství policie Ústeckého kraje

LVHP – Letiště Václava Havla v Praze

LZPEU - Listina základních práv Evropské unie

LZPS - Listina základních práv a svobod České republiky

PČR – Policie České republiky

SDEU - Soudní dvůr Evropské unie

SFEU – Smlouva o fungování Evropské unie

SOÚPP - Směrnice o ochraně údajů při prosazování práva

ÚS - Ústavní soud České republiky

ÚOOÚ - Úřad na ochranu osobních údajů

ZPČR – Zákon o Policii České republiky

ZZOÚ - Zákon o zpracování osobních údajů

1. Úvod

Ve většině států Evropské unie se již využívají technologie biometrického rozpoznávání obličejů na veřejných prostranstvích, přičemž výjimkou není ani Česká republika.[1] [2] Tyto sledovací systémy jsou často zaváděny netransparentním způsobem, bez řádného posouzení jejich nezbytnosti a proporcionality, bez přiměřeného upozornění veřejnosti, a tedy i bez předchozí společenské debaty. Jak ukazuje praxe v Číně nebo Rusku nasazení biometrického rozpoznávání na veřejných prostranstvích může snadno sklouznout k programům plošného sledování, což představuje závažné riziko pro práva a svobody obyvatel a pro samotné demokratické směřování společnosti. Biometrické rozpoznávání obličeje může zasahovat do základních práv a omezovat ochotu občanů 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 lidské autonomie vůle, svobod a soukromí v nebývalém měřítku. Na druhou stranu zvyšující se požadavky na bezpečnost představují argumentační základ pro jejich čím dál větší nasazení.

Systémy zpracovávající biometrické údaje se rychle rozšiřují především díky pokroku v algoritmech umělé inteligence. Důsledkem technologického pokroku je analýza fotografií a obrazových materiálů v masovém měřítku stále levnější a dostupnější. Jako v případě jiných technologií, začalo být biometrické rozpoznávání obličeje fakticky využíváno, aniž by byly řešeny právní a etické důsledky. Sběr, zpracování a ukládání biometrických údajů by ovšem nemělo být jen otázkou technologickou, ale především otázkou etickou, právní a společenskou. 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.

Kamerové systémy s biometrickým rozpoznáváním obličeje na veřejném prostranství nebyly dosud v České republice (dále také „ČR“) předmětem systematického odborného

1 European Digital Rights. *Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States* [online]. Brusel: European Digital Rights, 2020, s. 7.

2 TELEFI Project. Towards the European Level Exchange of Facial Images Version 1.0. Závěrečná zpráva projektu TELEFI, 2021, 173 s.

zájmu. Zpracování tohoto tématu je proto vhodné především z důvodu absence komplexního řešení nastíněné problematiky v českém právním řádu. Navíc biometrické rozpoznávání obličeje na veřejných prostranstvích je již nasazeno bez řádného zhodnocení, zda je a může být využívané v souladu s právním řádem.

Hlavním cílem diplomové práce je zodpovězení dvou výzkumných otázek:

- Jsou systémy biometrické identifikace obličeje na veřejném prostranství nasazené za účelem prosazování práva v souladu s účinnou právní úpravou?
- Jsou systémy biometrické identifikace obličeje na veřejném prostranství nasazené za účelem prosazování práva proporcionální vzhledem k zásahům do základních práv?

Z důvodu malé známosti tématu nejprve vymezuji základní terminologii (kapitola 2) a dále celou problematiku zasazuji do širšího kontextu včetně možného budoucího společenského vývoje (kapitola 3). V dalších kapitolách představuji účinnou právní úpravu ve vztahu k využívání biometrického rozpoznávání obličeje z hlediska základních práv (kapitola 4), práva Evropské unie (kapitola 5) a práva ČR (kapitola 6). Dále na základě shromážděných poznatků popisuji současnou aplikační praxi v ČR (kapitola 7) a následně tyto poznatky konfrontuji s účinnou právní úpravou (kapitola 8) a provádím pro vybrané systémy test proporcionality (kapitola 9). Nakonec nastiňuji aktuální podobu připravované evropské legislativy (kapitola 10). V závěru (kapitola 11) shrnuji hlavní poznatky a odpovídám na výzkumné otázky. Z hlediska platnosti a účinnosti právní úpravy je tato práce zpracována ke dni 11. března 2024.

2. Vymezení zkoumané problematiky

Počátečním úkolem je především vymezení zkoumané problematiky, kterou jsou kamerové systémy s biometrickým rozpoznáváním obličeje na veřejných prostranstvích. Vzhledem k rychlému technologickému pokroku různých metod biometrického zpracovávání bude důležité vymezit zkoumanou metodu od ostatních metod založených na biometrii. Ke správnému terminologickému vymezení poslouží především právní prameny, které jsou blíže rozebrány v následujících kapitolách.

Z hlediska budoucí právní úpravy považuji za podstatné vymezení pojmu **systém umělé inteligence**. Termín je důležité vymezit z důvodu regulace v připravovaném nařízení o umělé inteligenci, kdy se zákazy a omezení budou týkat biometrického zpracovávání systémy umělé inteligence. Nelze totiž hovořit jen o jediném systému umělé inteligence, ale jedná se o celou řadu různých postupů a technik. Nejčastěji se jedná o přístupy známé jako strojové učení, neuronové sítě, dobývání znalostí (tzv. *data mining*), zpracování přirozeného jazyka (tzv. *natural language processing*), bayesovské sítě nebo evoluční algoritmy. Přesto je někdy pod souhrnný pojem umělá inteligence zahrnována širší paleta postupů. Z přípravy evropského nařízení o umělé inteligenci je patrná snaha postihnout v právní definici nejširší škálu postupů, které se používají pro výpočetní zpracování dat. Systém umělé inteligence je dle návrhu nařízení definován jako *„strojový systém navržený tak, aby fungoval s různou úrovní autonomie a který může po nasazení vykazovat přizpůsobivost, a který pro explicitní nebo implicitní cíle odvodí ze vstupu, který obdrží, jak generovat výstupy, jako jsou předpovědi, obsah, doporučení nebo rozhodnutí, která mohou ovlivnit fyzické nebo virtuální prostředí.“* Takovéto vymezení systémů umělé inteligence zahrnuje nejen systémy schopné samostatně přizpůsobovat své jednání na základě vyhodnocení výsledků předchozích akcí, ale také systémy využívající mnohem jednodušší výpočetní operace.

Biometrické údaje jsou v širším slova smyslu informace o biologických vlastnostech, fyziologických charakteristikách, znacích jedince nebo opakovatelném jednání, kdy jsou tyto rysy nebo jednání pro daného jedince jedinečné a měřitelné. Podle Obecného nařízení o ochraně osobních údajů (dále také „GDPR“) jsou biometrickými údaji *„osobní údaje*

vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“ (čl. 4 odst. 14). Právo tedy výslovně definuje biometrické údaje pouze v užším slova smyslu, tj. pouze pokud mohou vést k identifikaci osoby.[3]

Existují dvě hlavní kategorie biometrických údajů. Za prvé se jedná o údaje založené na **fyziologických rysech**, které měří fyziologické znaky určité osoby. Typickými příklady fyziologických rysů jsou otisky prstů, struktura obličeje, lidský hlas, ale také vzorky žil, struktura duhovky, struktura sítnice nebo DNA. Za druhé se jedná o údaje založené na **behaviorálních rysech**, které měří chování určité osoby. Mezi behaviorálních rysy patří některé hluboce zakořeněné dovednosti nebo jiné charakteristiky chování, jedná se například o vlastnoruční podpis, způsob úhozů na klávesnici, způsob chůze nebo vzorce chování naznačující určité podvědomé myšlení (např. lhaní).

Mezi formy zpracování struktury obličeje patří různé operace používané k analýze nasnímaného obrazu, z nichž nikoliv všechny představují stejné riziko pro ochranu osobních údajů. Mezi tyto operace se strukturou obličeje patří: rozpoznání, identifikace, autentizace a kategorizace. Nejpoužívanější pojmem je **rozpoznávání obličeje**, který je také v názvu této práce. Tento pojem lze chápat buď v širším významu jako automatické zpracování fotografií obsahující obličej osoby, za účelem identifikace, autentizace nebo kategorizace.[4] V tomto nejširším významu tak pojem rozpoznávání obličeje zahrnuje všechny tři další druhy operací s biometrickými daty obličeje. Rozpoznávání obličeje v užším, méně používaném, významu představuje nejméně problematickou operaci, která sama o sobě nezpracovává biometrické údaje. Jedná se o analýzu obrazu, kdy je rozpoznána přítomnost obličeje na fotografii. Taková operace může být využívána například k počítání osob na kamerových záběrech.

Kategorizace obličeje je operace zjišťující, zda jednotlivec patří do skupiny osob s určitou předem stanovenou charakteristikou. Ani v tomto případě není smyslem identifikovat nebo ověřit totožnost jednotlivce, nýbrž jej automaticky zařadit do určité kategorie. Jedná se o profilování a jeho účelem může nebo nemusí být provedení určitého

3 MATEJKA, Ján a kol. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, 2018, roč. 9, č. 17, s. 91-129.

4 Stanovisko k vývoji biometrických technologií Pracovní skupiny zřízení podle článku 29 č. 3/2012 ze dne 27. dubna 2012, s. 5-6.

úkonu. Jedná se o podmnožinu pojmu **systémem biometrické kategorizace**, který je v návrhu nařízení o umělé inteligenci definován jako *„systém umělé inteligence pro účely zařazení fyzických osob do určitých kategorií podle pohlaví, věku, barvy vlasů, barvy očí, tetování, etnického původu nebo sexuální či politické orientace, na základě jejich biometrických údajů“*. V praxi lze touto operací například sledovat zda do prostoru vstupují osoby určitého věku či osoby mající roušku nebo pokrývku hlavy. Rozpoznávání v užším smyslu ani kategorizaci nebude v této práci věnována pozornost a zaměří se na další dvě operace.

Autentizace a identifikace jsou operace, kdy dochází k porovnání shody konkrétní osoby s fotografií. 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 nebo fotografií.[5] **Autentizace obličeje** (někdy také verifikace či ověření) je v podstatě ověření totožnosti osoby pomocí biometrického systému. Jedná se o proces srovnávání biometrické struktury obličeje určité osoby s jednou uloženou biometrickou šablonou. Tato operace odpovídá na otázku: „objevuje se tato osoba na obrázku?“ Použití této operace může sloužit pro omezení přístupu do vymezených prostor jen pro určenou osobu nebo jako odemykací systém na chytrých telefonech. Od toho se liší **identifikace obličeje**, při které se nesrovnává jedna šablona s druhou šablonou, ale kdy dochází ke srovnávání jedné šablony s mnoha jinými. Identifikací jednotlivce pomocí biometrického systému je obvykle proces srovnávání biometrických údajů zachycených osob s řadou biometrických šablon uložených v databázi. Tato operace odpovídá na otázku: „kdo je tato osoba?“

Kamerový systém provádějící identifikaci dle biometrických údajů je v návrhu nařízení o umělé inteligenci nazýván jako **systémem biometrické identifikace na dálku**. Dle definice termínu v návrhu nařízení se jedná o systém pro účely identifikace osob na dálku na základě porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v referenční databázi, aniž by uživatel systému předem věděl, zda bude daná osoba přítomna a bude ji možné identifikovat. V zásadě se tudíž navrhovaná regulace neomezuje jen na biometrii obličeje, ale také na další biometrické charakteristiky, které je možné sledovat na dálku. Mezi

5 Agentura Evropské unie pro základní práva. *Facial recognition technology: fundamental rights considerations in the context of law enforcement* [online]. Vídeň: Agentura Evropské unie pro základní práva, 2020, s. 7-8.

takové lze zařadit například identifikace osoby dle chůze. Návrh nařízení o umělé inteligenci navíc systémy biometrické identifikace na dálku rozděluje na dvě praktické skupiny: „v reálném čase“ a „zpětné“. Systémem **biometrické identifikace na dálku v reálném čase** probíhá zachycení biometrických údajů, a následné porovnání a identifikace bez významné prodlevy. Někdy se tyto systémy nazývají jako „on-line“ nebo „živé“. Ostatní systémy mají být považovány za systémy **zpětné biometrické identifikace na dálku**. Někdy jsou nazývané jako systémy „ex-post“ identifikace. Uvedené rozdělení je významné pro policejní praxi. Zatímco systémy v reálném čase mohou být využívány k necílené identifikaci lidí na ulici, systémy zpětné mají sloužit k pozdější cílené identifikaci konkrétní neznámé podezřelé osoby zachycené na kamerových záběrech.

Specifickou operací, která již nepracuje s fyziologickými rysy, ale s rysy behaviorálními, je rozpoznávání emocí. Návrhu nařízení o umělé inteligenci definuje **systém rozpoznávání emocí** jako *„systém umělé inteligence pro účely zjišťování nebo odvozování emocí nebo záměrů fyzických osob na základě jejich biometrických údajů“*. Systémy rozpoznávání emocí jsou v této práci zmíněny jen okrajově, protože není známo, že by byly v současné době na veřejných prostranstvích používány.

V názvu použitý pojem veřejné prostranství je ekvivalent termínu **veřejně přístupné místo**. Veřejně přístupné místo je v návrhu nařízení o umělé inteligenci definováno jako *„jakékoli fyzické místo ve veřejném nebo soukromém vlastnictví přístupné neurčenému počtu fyzických osob bez ohledu na to, zda mohou platit určité podmínky pro přístup, a bez ohledu na potenciální omezení kapacity“*. Pojem tudíž zahrnuje jakékoli fyzické místo, které je přístupné veřejnosti, bez ohledu na to, zda je dané místo v soukromém nebo veřejném vlastnictví. Kromě ulic, příslušných částí státních budov a většiny dopravní infrastruktury, jsou za veřejně přístupné považovány také prostory jako kina, divadla, obchody a nákupní centra. Pojem nicméně nezahrnuje on-line prostory, protože se nejedná o prostory fyzické. Práce se tudíž ani blíže nevěnuje biometrickému rozpoznávání obličeje na fotografiích a videích, která jsou vytěžována na sociálních sítích a v on-line prostoru, ačkoliv se dnes jedná o problematiku neméně závažnou.

Důležitým pojmem je **prosazování práva**, které je v návrhu nařízení o umělé inteligenci definováno jako *„činnosti prováděné donucovacími orgány za účelem prevence, vyšetřování,*

odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení“. Možnost biometrické identifikace obličeje na veřejném prostranství pro jiné účely než prosazování práva (případně pro účely národní bezpečnosti) lze prakticky vyloučit. Předchozí definice užívá pojem **donucovací orgán**, což je orgán veřejné moci příslušný k prevenci, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Mezi české donucovací orgány patří Policie České republiky (dále také „PČR“), Generální inspekce bezpečnostních sborů, Celní správa ČR a Vězeňská služba ČR. Z uvedených donucovacích orgánů bude v této práci věnována pozornost jen PČR, protože se jedná o jediného známého provozovatele zájmových systémů.

Nakonec zbývá definovat poslední termín, který se nachází již v názvu práce. **Kamerový systém** definuji jako automatický technický systém schopný pořizovat obrazové záznamy. Tuto definici vyvozuji z § 62 zákona č. 273/2008 Sb., o policii České republiky (dále také „ZPČR“). Nicméně vzhledem k možnosti ex-post biometrické identifikaci, se práce věnuje také zpětnému zpracování záznamů z kamerových systémů.

Z výše uvedeného terminologického výkladu vyplývá, že vhodnější název práce by zněl: „biometrická identifikace osob na základě struktury obličeje prováděná na veřejném prostranství Policií České republiky“. Nicméně pro jistou společenskou zažitost jsem použil méně přesný název práce, což vzhledem k vývoji legislativy a neustálenosti tématu není na škodu.

3. Společenský kontext

3.1 Plošné sledování

Kamerové systémy s biometrickou identifikací obličeje na veřejných prostranstvích jsou technologií sloužící k plošnému sledování. Jako plošné sledování, či **necílené sledování**, je označováno sledování, které není prováděno cíleně ve vztahu ke konkrétní podezřelé osobě. Jedná se v podstatě o opak **cíleného sledování**. Zásady ochrany soukromí a spravedlivého procesu vyžadují, aby u cíleného sledování, jako jsou odposlechy telefonů dle trestního řádu, měl donucovací orgán zákonné oprávnění a soudní povolení na základě důvodného podezření na konkrétní osobu. Plošné sledování je naopak opatřením s obecným dopadem na veřejnost, a probíhá bez předchozího podezření.

Plošné sledování obecně tvoří překážku ve výkonu občanských a politických práv. Dopady sledovacích systémů posílených o biometrickou identifikaci mohou mít velmi zásadní dopad na svobodu projevu a shromažďování, protože plošné sledování biometrickou identifikací znamená faktickou ztrátu anonymity na veřejných prostranstvích. Všudypřítomnost plošného sledování je způsobilá 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 ze sčítání lidu z roku 1983 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.“[6]

3.2 Prohlubování nerovností

Zkreslení a chybovost v důsledku diskriminačního nastavení může vést k traumatizujícím vyšetřujícím úkonům policie u příslušníků zranitelných skupin obyvatel. Zvýšené kontroly mohou v konečném důsledku prohlubovat diskriminaci těchto skupin. Biometrická identifikace je založena na pravděpodobnosti a existuje určitá míra chybné shody (tzv. falešně pozitivní shoda). Míra chybovosti, je ovlivněna řadou faktorů včetně vstupních údajů, podmínek snímání nebo samotného algoritmu. Důležitou roli při hodnocení výkonnosti systémů rozpoznávání obličejů vykazují demografické charakteristiky. Prokázalo se, že některé technologie k biometrické identifikaci obličeje mají vyšší chybovost u žen, mladých ve věkové skupině 18 až 30 let, Afričanů nebo Asiatů.[7] [8] [9] V důsledku chyby biometrického systému s umělou inteligencí došlo v lednu 2020 v americkém Detroitu k zatčení Afroameričana, který měl údajně 15 měsíců předtím ukrást hodinky. Důkazy pocházející z technologie biometrické identifikace obličejů se však později ukázaly jako chybné. Kvůli chybě technologie tak postižený musel nedobrovolně absolvovat několikahodinovou proceduru včetně odběru DNA a otisků prstů.[10] S Detroitem je spojen také případ neoprávněně zadržené Afroameričanky v pokročilém stadiu těhotenství, kdy v únoru 2023 systém biometrické identifikace obličeje vedl k chybnému výsledku.[11]

6 Nález německého ústavního soudu ze dne 15. prosince 1983. 1 BvR 209/83, bod 146.

7 GROTHER, Patric a kol. *Face Recognition Vendor Test. Part 3: Demographic Effects*. National Institute of Standards and Technology. U.S. Department of Commerce, 2019. 82 s.

8 EL KHIYARI, Hachim, WECHSLER, Harry. Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning. *Journal of Biometrics & Biostatistics*, 2016, roč. 7, č. 4.

9 KLARE, Brendan a kol. Role of Demographic Information. *IEEE Transactions on Information Forensics and Security*, 2012, roč. 7, č. 6, s. 1789-1801.

10 VÁCLAVÍKOVÁ, Jana. *"Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře* [online]. Aktualne.cz, 11. července 2020 [cit. 10. března 2024].

11 ALSHARIF, Mirna, SANTAN, Cristian. *Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology* [online]. nbcnews.com, 6. srpna 2023 [cit. 10. března 2024].

3.3 Funkční rozlézání

Využívání biometrické identifikace pro účely prosazování práva může vést k akceleraci všeobecného sledování. Systémy umělé inteligence dokážou mnoho procesů automatizovat a zjednodušit. Zvýšením možností a kapacit plošného sledování, tak pravděpodobně povede ke zvýšení poptávky ze strany donucovacích orgánů tyto systémy využívat. Mohlo by dojít k indukci poptávky. Jedná se o jev popsaný v ekonomii, při kterém se po zvýšení nabídky zvedne také poptávka. Využívání biometrické identifikace obličeje donucovacími orgán může vést k rozšíření sledování do čím dál širší sféry lidského chování. Sytém nasazený pro jeden konkrétní účel, může být postupem času používán k jiným účelům. Jakmile se objeví původně nezamýšlená možnost využití nějaké technologie k řešení jiného problému, veřejné autority často takové technologie využijí nad rámec původního cíle, pro který byla zavedena. V anglicky psaných zdrojích se pro tento jev používá pojem *function creep*, v překladu jako *funkční rozlézání*. Nelze proto spoléhat na to, že biometrické identifikační systémy budou v budoucnu sloužit jen proti závažné kriminalitě. Biometrické identifikační systémy dnes mnohdy deklarované pro odhalování teroristů mohou být v budoucnu normalizovány k předcházení mnohem méně závažných hrozeb.

3.4 Bezpečnostní rizika

V systémech zpracovávajících biometrické údaje může dojít k porušení zabezpečení. Získáním biometrických údajů určité osoby by mohlo v případě jejich užití k falešné autentizaci umožnit průnik do systému, kde jsou tyto biometrické údaje užívány jako přístupové. K odcizení dat by mohlo dojít obdobně jako v případě používání stejného hesla u dvou odlišných systémů. Na rozdíl od systémů založených na klasickém heslu, jednou kompromitované biometrické údaje nemohou být změněny. Biometrické údaje představují kategorii osobních údajů, jež až na výjimky není možné změnit, jsou tedy zranitelné a zneužitelné, nezřídka zcela nevratně.[12] Pokud byla dříve biometrická informace uložena

12 MATEJKA, Ján a kol. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, 2018, roč. 9, č. 17, s. 91-129.

ve více databázích, zvyšuje to pravděpodobnost úniku biometrických údajů. V několika případech došlo také k úniku celých databází biometrických údajů.[13] [14]

Plošné vytěžování biometrických údajů obličeje provádějí některé soukromé společnosti, které z internetu a sociálních sítí stahují fotografie, které následně automatizovaně biometricky zpracovávají. Tyto společnosti nabízejí zpoplatněné vyhledávací služby na základě biometrických údajů. Evropský parlament ve svém usnesení o využívání umělé inteligence v trestním právu nad těmito praktikami vyjádřil hluboké znepokojení a *"požaduje zákaz používání soukromých databází pro rozpoznávání obličeje při prosazování práva“*.[15]

3.5 Dystopická společnost

Kombinovaný dopad biometrické identifikace obličejů na veřejných prostranstvích a slučování různých veřejných databází představuje růst rizik pro bezpečnost, soukromí a základní práva. Ohrožení svobody občanů by ještě narostlo, pokud by data získaná z biometrických kamerových systémů byla dále analyzována a používána k vytváření profilů jednotlivců. Možnosti podobných scénářů se budou postupem času zvyšovat, protože stále více různých dat bude možné propojit. Ovšem také metadata nebo anonymizované údaje lze v kombinaci s dalšími možnými zdroji, které mají k dispozici veřejné a soukromé subjekty, použít k získání citlivých informací. Rozrůstající digitální prostor vytváří trvalé záznamy o našich životech, interakcích a chování bez možnosti to reálně ovlivnit.

Pokud by byly systémy plošné sledování navíc spolu se zpracováváním biometrických dat z veřejných prostranství normalizovány v běžném životě, mohlo by být snadněji zavedeno bodování a kategorizování obyvatel.[16] Protože jsou neustále zaváděny inovace s velkými daty a umělou inteligencí, existuje riziko, že jednou dojde ke kombinaci obrovského množství

13 DOFFMAN, Zak. *New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report* [online]. Forbes, 14. srpna 2019 [cit. 10. března 2020].

14 UNGERLEIDER, Neal. *The Dark Side Of Biometrics: 9 Million Israelis' Hacked Info Hits The Web* [online]. FastCompany.com, 24. října 2011 [cit. 10. března 2024].

15 Usnesení Evropského parlamentu ze dne 6. října 2021, o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech, bod 28.

16 DIXON, Pam, GELLMAN, Robert. *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*. World Privacy Forum, 2014, 90 s.

údajů z různých evidencí veřejné správy, veřejně přístupných rejstříků a dalších zdrojů. Propojování databází by mohlo být spojeno se zaznamenáváním fyzického výskytu jedinců na ulicích, přičemž by to umožňovalo monitorovat jejich interakce a pohyb způsobem, který by vytvářel podrobné a důvěrné obrazy jejich životů. To by při 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, který je již několik let budován prostřednictvím masivního shromažďování a zpracování osobních údajů občanů na sociálních sítích a prostřednictvím sledovacích kamer. Jedná se o státní systém hodnocení obyvatel na základě různých aspektů jejich ekonomického a společenského chování, na jehož základě mají jednotlivý občané různou úroveň přístupu k veřejným službám.[17]

17 BOTSMAN, Rachel. *Big data meets Big Brother as China moves to rate its citizens* [online]. Wired.co.uk, 21. října 2017 [cit. 10. března 2024].

4. Základní práva

Systém ochrany základních práv představují nejvyšší stupeň právních norem dopadající na biometrickou identifikaci obličeje na veřejných prostranstvích. Systémy biometrické identifikace obličeje zasahují celou řadu základních práv. V první řadě se jedná o **právo na soukromí** a **právo na ochranu osobních údajů**. Prostřednictvím práva na soukromí a práva na ochranu osobních údajů zasahuje plošné sledování do dalších základních práv, mezi které patří **lidská důstojnost, svoboda projevu a svoboda shromažďování a sdružování**. Kromě zmíněných práv mohou systémy biometrické identifikace obličeje zasahovat také do dalších základních práv, jako jsou **právo na spravedlivý proces** a **zákaz diskriminace**. Zásah do některých základních práv vyplývá z chybovosti technologie, ale zásah do jiných práv přetrvává, pokud je technologie bezchybná. Uvedená základní práva jsou vymahatelná skrze právní dokumenty na vnitrostátní, evropské a mezinárodní úrovni. Výčet dotčených ustanovení v lidskoprávních dokumentech v souvislosti s uvedenými základními právy je uveden v tabulce 1. Kromě základních práv uvedených ve výčtu v tabulce 1 mohou být dle Agentury Evropské unie pro základní práva technologií biometrické identifikace obličeje zasažena některá další základní práva: práva dítěte a starších osob, práva osob se zdravotním postižením a právo na řádnou správu.[18]

Kromě obecných lidskoprávních dokumentů se problematiky týká Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (vypracovaná Radou Evropy v roce 1981). ČR ratifikovala úmluvu v roce 2001, tudíž na základě čl. 10 Ústavy ČR je součástí českého právního řádu s předností před zákonem. V květnu 2018 byl přijat protokol o změně úmluvy, kterým byla úmluva modernizována. Konsolidované znění úmluvy po přijetí protokolu stanoví v čl. 6, že *„zpracování (…) biometrických údajů umožňujících jedinečnou identifikaci fyzické osoby (…) se povoluje pouze za podmínky, že v právních předpisech jsou zakotveny vhodné záruky“*.

18 Agentura Evropské unie pro základní práva. *Facial recognition technology: fundamental rights considerations in the context of law enforcement* [online]. Vídeň: Agentura Evropské unie pro základní práva, 2020, s. 4.

Tabulka 1: Přehled základních práv, která mohou být systémy biometrické identifikace zasažena, a příslušná ustanovení v obecných lidskoprávních dokumentech.

	Všeobecná deklarace lidských práv OSN	***Mezinárodní pakt o občanských a politických právech***	***Evropská úmluva o ochraně lidských práv***	***Listina základních práv Evropské unie***	***Listina základních práv a svobod ČR***
Právo na soukromí	čl. 12	čl. 17	čl. 8	čl. 7	čl. 7 odst. 1 čl. 10 odst. 2
Právo na ochranu osobních údajů	čl. 12	čl. 17	čl. 8	čl. 8	čl. 10 odst. 3
Důstojnost	čl. 1	Preambule	Preambule (odkaz na Všeobecnou deklaraci lidských práv)	čl. 1	čl. 10 odst. 1
Svoboda projevu	čl. 19	čl. 19 odst. 2	čl. 10	čl. 11	čl. 17
Svoboda shromažďování	čl. 20	čl. 21	čl. 11	čl. 12	čl. 19
Svoboda sdružování	čl. 20	čl. 22	čl. 11	čl. 12	čl. 20
Právo na spravedlivý proces	čl. 8 až 11	čl. 9	čl. 6	čl. 47 a 48	čl. 8 odst. 2
Zákaz diskriminace	čl. 2 a 7	čl. 26	čl. 14	čl. 21	čl. 3

Zachycení podoby kamerou představuje především zásah do soukromí. **Soukromý život** je dle Evropského soudu pro lidská práva (dále také „ESLP“) *"široký pojem, který není poddajný vyčerpávající definici"*.[19] ESLP vyjádřil, že extenzivní interpretace pojmu soukromý život je ve shodě s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat, 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*

19 ESLP: rozsudek velkého senátu ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, bod 66.

identifikovatelné fyzické osoby (čl. 2).“[20] ESLP rozhodl, že tajné sledování za účelem odhalování nebo prevence trestné činnosti a sdílení kamerových záznamů spadá do oblasti působnosti čl. 8 Evropské úmluvy o ochraně lidských práv (dále také „EÚLP“), který chrání právo na soukromý a rodinný život.[21] Judikatura ESLP tudíž z práva na soukromí dovozují také právo na ochranu osobních údajů, kdy právo na soukromí se vztahuje také na ochranu před sledováním, hlídáním a pronásledováním ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech.

V Listině základních práv a svobod (dále také „LZPS“) není právo na soukromí garantováno v jednom všezahrnujícím článku (jako je tomu v EÚLP). Ochrana soukromé sféry jednotlivce je v LZPS rozložena a doplňována dalšími aspekty práva na soukromí, deklarovanými na různých místech LZPS. 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.[22] Jak konstatoval Ústavní soud ČR (dále také „ÚS“): *"...právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsah, jakým způsobem a za jakých okolností mají být skutečnosti z jeho osobního soukromí zpřístupněny jiným subjektům."*[23] Jde o aspekt práva na soukromí zahrnující ochranu před sledováním a pronásledováním především ze strany veřejné moci, nejen v soukromých prostorech, ale také ve veřejném prostoru či na veřejně přístupných místech.

Odmítnutí **plošného sledování** v souvislosti s ochranou soukromí a ochranou osobních údajů je v judikatuře často odůvodněn tím, že sledování probíhá bez dostatečně zdůvodněného podezření. V tomto ohledu je znám případ S. a Marper proti Spojenému království, ve kterém ESLP shledal, že "plošné a nerozlišující" uchovávání biometrických údajů je "nepřiměřeným zásahem" do práva na soukromí.[24] V případu společnosti Digital Rights Ireland zkoumal Soudní dvůr Evropské unie (dále také „SDEU“) slučitelnost směrnice o uchovávání údajů 2006/24/ES s čl. 7 a 8 Listiny základních práv Evropské unie (dále také „LZPEU“). Zvláště vzal na vědomí skutečnost, že směrnice: *"pokrývá obecně všechny osoby a všechny*

20 ESLP: rozsudek velkého senátu ESLP ze dne 16. února 2000, *Amann proti Švýcarsku*, č. 27798/95, bod 65.
21 ESLP: rozsudek ESLP ze dne 28. dubna 2003, *Peck proti Spojenému království*, č. 44647/98, bod 133.
22 Bartoň, Michal a kol. *Základní práva.* Praha: Leges, 2016, s 290.
23 ÚS: nález pléna ÚS ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 29.
24 ESLP: rozsudek velkého senátu ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, bod 125.

prostředky elektronické komunikace (...), aniž by došlo k jakékoli diferenciaci, omezení nebo výjimce s ohledem na cíl boje proti závažné trestné činnosti."[25] SDEU v případu poznamenal, že napadená opatření "*pravděpodobně vyvolala v myslích dotčených osob pocit, že jejich soukromý život je předmětem neustálého sledování*." Problematické je především plošné sledování občanů, kteří nejsou podezřelými z protiprávních činů nebo z ohrožení veřejného pořádku. Jak uvedl v dalším případu SDEU: *"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..."*[26]

Nakládání s každým bezvýjimečně jako s podezřelým zakládá **zásah do důstojnosti člověka**. Základní práva EU jsou založena na důstojnosti člověka podle čl. 1 LZPEU, který stanoví: *"Lidská důstojnost je nedotknutelná. Musí být respektována a chráněna."* Další nástroje v oblasti základních práv jsou podobně centrálně založeny na všeobecné a nezcizitelné lidské důstojnosti. To vedlo k tomu, že důstojnost je někdy považována za "mateřské právo".[27] V pojetí ÚS představuje právo na lidskou důstojnost v čl. 10 odst. 1 LZPS subjektivní právo jednotlivce a je chápáno ve významu přirozené hodnoty člověka, která mimo jiné vylučuje jednat s jednotlivcem jako s objektem.[28]

Plošné sledování zasahuje také svobodu projevu a svobodu shromažďování a sdružování, protože působí tzv. **odrazujícím účinkem** (*chilling effect*) k výkonu těchto práv. V případě svobody shromažďování judikoval ELSP, že zásah do shromažďovacího práva představuje nejen naprosté znemožnění shromáždění, ale také jeho omezení v důsledku opatření přijatých před jeho konáním, v jeho průběhu či po něm.[29] K zásadě nepřípustnosti opatření s odrazujícím účinkem ve vztahu k právu na svobodu projevu a svobodu shromažďovací přihlížel ve své judikatuře také ÚS. Porušení svobody shromažďování konstatoval v případě excesivních kontrol totožnosti účastníků shromáždění, když konstatoval: *„Do práva pokojně se shromažďovat přitom zasahují i ta opatření, která mají*

25 SDEU: rozsudek velkého senátu SDEU ze dne 8. dubna 2014, *Digital Rights Ireland a Seitlinger a další*, C-293/12 a C-594/12, bod 57.
26 SDEU: rozsudek velkého senátu SDEU ze dne 6. října 2015, *Schrems*, C-362/14, bod 94.
27 BARAK, Aharon. Human Dignity. The Constitutional Value and the Constitutional Right. *Human Rights Law Review*, 2015, roč. 16, č. 1, s 175 – 176.
28 Bartoň, Michal a kol. *Základní práva.* Praha: Leges, 2016, s 286.
29 ESLP: rozsudek velkého senátu ESLP ze dne 15. října 2015, *Kudrevičius proti Litvě*, č. 37553/05, bod 100.

ve vztahu k nositelům tohoto práva v konkrétní situaci tzv. odrazující účinek (chilling effect), tedy jim plný výkon práva sice neznemožňují, ovšem odrazují je od něho.“[30]

Právo na spravedlivý proces představuje možnost každého jedince využít všech právních institutů a záruk, které právní řád nabízí. Samotný pojem právo na spravedlivý proces byl vytvořen judikaturou ESLP a projevuje se v celé řadě právních zásad. V souvislosti s biometrickým rozpoznáváním obličeje může dojít především k porušení zásady stíhání jen ze zákonných důvodů, kdy čl. 8 odst. 2 LZPS stanoví: *„Nikdo nesmí být stíhán nebo zbaven svobody jinak než z důvodů a způsobem, který stanoví zákon.“* To znamená, že také všechny důkazy musí být získány zákonnou cestou, přičemž také nedostatek transparentnosti by mohl toto právo narušit. S možnou systematickou chybovostí systémů biometrické identifikace souvisí zásah do **zákazu diskriminace**. Diskriminace je termín označující rozlišování lidí založené na předpokladu vlastností nebo schopností na základě rasy, pohlaví, věku nebo jiných skupinových charakteristik. Zákaz diskriminace je zcela elementární předpoklad k fungování spravedlivé společnosti.

30 ÚS: nález ÚS ze dne 10. října 2021, sp. zn. II. ÚS 1022/21, bod 21.

5. Právo Evropské unie

Na kamerové systémy s biometrickým rozpoznáváním obličeje na veřejných prostranstvích dopadá evropská regulace ochrany osobních údajů. Z primárního práva Evropské unie (dále také „EU“) je nutné odkázat na čl. 16 Smlouvy o fungování Evropské unie (dále také „SFEU“), podle kterého má každý *„právo na ochranu osobních údajů, které se jej týkají.“* SFEU dále ukládá přijmutí společných unijních pravidel o ochraně osob při zpracovávání osobních údajů orgány EU a členskými státy. Na základě tohoto zmocnění byla přijata sekundární legislativa EU k ochraně osobních údajů.

V účinném sekundárním právu EU jsou dva základní právní předpisy, které se týkají ochrany osobních údajů ve členských státech a dotýkají se jmenovitě také zpracovávání biometrických údajů. Jedná se o **Obecné nařízení o ochraně osobních údajů**, které stanoví obecné zásady ochrany osobních údajů. GDPR stanovuje obecná pravidla pro zpracování osobních údajů v členských státech EU a vztahuje se na zpracování osobních údajů veřejnými a soukromými subjekty s několika výjimkami věcné působnosti, kterou je mimo jiné zpracování údajů za účelem prosazování práva (čl. 2 odst. 2 písm. d) GDPR). Druhým právním aktem je **Směrnice o ochraně údajů v oblasti prosazování práva** (dále také „SOÚPP“), která se vztahuje na zpracování osobních údajů právě za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Oba právní instrumenty byly přijaté současně jako součást jednoho souborného balíčku. Jedná se o vzájemně se doplňující právní nástroje založené na obdobných principech s tím, že SOÚPP má užší specifickou oblast věcné působnosti, kterou je oblast prosazování práva.[31]

Zde je třeba uvést významnou oblast, ve které dochází k biometrické identifikaci obličejů, a na kterou evropské právo ochrany osobních údajů nedopadá. Jedná se o oblast tzv. národní bezpečnosti, kam spadají zpravodajské služby (Bezpečnostní informační služba, Vojenské zpravodajství a Úřad pro zahraniční styk a informace) a případně také armáda. EU má na základě zásady svěření pravomocí pouze takové kompetence, které jsou jí svěřeny členskými státy. Podle uvedené zásady může EU jednat pouze v mezích pravomocí, které jí

31 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář*. 2. aktualizované vydání. Praha: Leges, 2019, s. 540.

byly svěřeny v zakládacích smlouvách EU za účelem dosažení cílů v nich stanovených. Pravomoci, které nebyly svěřeny EU, zůstávají členským státům. V souladu s tím také GDPR (čl. 2 odst. 2 písm. a) vylučuje svou věcnou působnost ze zpracovávání osobních údajů *„při výkonu činností, které nespadají do oblasti práva Unie“*. Oblast národní bezpečnosti přitom nepatří mezi žádnou z kategorií kompetencí EU (čl. 2 SFEU).

Zpracovávání osobních údajů donucovacími orgány spadá někdy pod věcnou působnost GDPR a jindy pod SOÚPP, v závislosti na tom, jakou svou činnost tyto orgány právě vykonávají. Například pokud by donucovací orgán zavedl docházkový systém svých zaměstnanců založený na biometrickém rozpoznávání obličeje, spadal by tento systém pod režim GDPR. Navíc mohou existovat situace, ve kterých dochází k překryvu více účelů zpracování a není tak jednoznačné, kterou právní úpravu použít. Nicméně v případě nasazení biometrické identifikace obličeje na veřejném prostranství si nelze představit jiný účel než je prosazování práva. V následujícím textu bude tudíž věnována pozornost především SOÚPP, protože biometrická identifikace obličeje na veřejných prostranstvích spadá právě pod ní. GDPR a SOÚPP se liší v tom, že na rozdíl od GDPR není dle SOÚPP souhlas subjektu údajů jedním z právních důvodů zpracování, což nemá pro biometrickou identifikaci obličeje na veřejných prostranstvích žádný význam.

Významnějším rozdílem mezi GDPR a SOÚPP je přímý účinek. Samotná SOÚPP není v zásadě přímo účinná, protože pravidla v ní stanovená se transponují do českého právního řádu až skrze národní legislativu. Nicméně je třeba dodat, že transpozice SOÚPP neproběhla bezproblémově. Je proto vhodné pro potřeby této práce dále pracovat také s přesným znění SOÚPP, protože interpretace národní legislativy musí být souladná právě se SOÚPP. V případě rozporu národní legislativy se SOÚPP má přednost SOÚPP.

SOÚPP stanoví, že při využívání osobních údajů, musí být splněny určité zásady uvedené v čl. 4 SOÚPP. Těmito principy se řídí také výklad souvisejících národních právních předpisů. Mezi tyto zásady dle čl. 4 SOÚPP patří: **zásada minimalizace** využívaných údajů, která ukládá, aby zpracování údajů bylo omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány; **zásada účelového omezení**, která ukládá, aby byly údaje shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nebyly zpracovávány způsobem, který je s těmito účely neslučitelný; **požadavek na kvalitu údajů** zakazující

použití nedostatečně přesných osobních údajů; **zásada zákonnosti a korektnosti** a další zásady. Svébytný **požadavek zákonnosti zpracování** je v článku 8 odst. 2 SOÚPP, který ukládá, že právo členského státu musí stanovit alespoň cíle zpracování, osobní údaje, jež mají být zpracovány, a účely zpracování. Článek 11 SOÚPP dále zakazuje plně automatizovaná rozhodnutí založená na využívání osobních údajů.

SOÚPP v čl. 6 ukládá také povinnost rozdílného zacházení s osobními údaji osob odsouzených nebo podezřelých z trestných činů (když má donucovací orgán závažné důvody se domnívat, že konkrétní osoba spáchala nebo se chystá spáchat trestný čin) a mezi osobními údaji osob, které nejsou odsouzené, obviněné 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 necíleným zpracováváním osobních údajů kterékoliv náhodné osoby.

Podle SOÚPP (stejně jako dle GDPR) je definována tzv. **zvláštní kategorie údajů**, což jsou osobní údaje obzvláště citlivé mající zvýšenou ochranu. Mezi tyto zvláště citlivé údaje patří zpracování biometrických údajů, jako jsou biometrie obličeje 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. Tím jsou osobní údaje prakticky rozděleny do dvou kategorií, jimiž jsou **„běžné“ a „citlivé“ osobní údaje**. SOÚPP definuje biometrické údaje v čl. 3 odst. 13 totožně jako jsou definovány v GDPR. Je tudíž zřejmé, že osobní údaje zpracovávané systémy biometrického identifikace obličeje spadají mezi citlivé osobní údaje.

Podle SOÚPP je zpracování biometrických údajů povoleno za podmínek stanovených v čl. 10: *„(…) zpracovaní (...) biometrických údajů za účelem jedinečné identifikace fyzické osoby (...) je povoleno pouze tehdy, pokud je zcela nezbytné, pokud existují vhodné záruky práv a svobod subjektu údajů a: a) pokud je povoleno právem Unie nebo členského státu; b) na ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; nebo c) pokud se týká údajů zjevně zveřejněných subjektem údajů.“*

SOÚPP proto vyžaduje pro kamerové systémy s biometrickou identifikací obličeje na veřejných prostranstvích minimálně dvě kumulativní podmínky. Za prvé je možné je nasazovat pouze v případech naprosté nezbytnosti, pokud existují vhodné záruky práv

a svobod subjektu údajů, a za druhé pouze v případě, že takové zpracování povoluje právo EU nebo právo členského státu.

6. Právo v České republice

V českém právním řádu není biometrické rozpoznávání obličeje na veřejných prostranstvích regulováno zvláštním zákonem. Na problematiku se tak vztahují jen právní předpisy, které do českého právního řádu transponují SOÚPP. Především se jedná o zákon č. 110/2019 Sb., o zpracování osobních údajů (dále také „ZZOÚ“), a dále zvláštní zákony, které se vztahují k jednotlivým donucovacím orgánům. Jak je uvedeno výše tato práce se z nich věnuje pouze PČR, jejíž činnost upravuje zákon č. 273/2008 Sb., o Policii České republiky.

Zpracováním a ochranou osobních údajů orgány veřejné moci za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů se zaobírá hlava III části první **zákona č. 110/2019 Sb., o zpracování osobních údajů**. Hlava III ZZOÚ nestanoví nad rámec SOÚPP více podrobností, ani konkrétní zmocnění nakládat s osobními údaji jednotlivým donucovacím orgánům. Tato zmocnění se nacházejí až v právních předpisech upravujících činnost jednotlivých donucovacích orgánů.

Do hlavy III ZZOÚ jsou přepsány v hrubých rysech hlavní povinnosti donucovacích orgánů při zpracování osobních údajů a práva subjektů zpracovávaných údajů. Mezi základní práva subjektu údajů patří zejména právo na přístup k osobním údajům; právo na opravu, omezení zpracování nebo výmaz osobních údajů; právo podat podnět o ověření zákonnosti zpracování osobních údajů. Mezi povinnosti donucovacích orgánů patří zejména povinnost vedení záznamů (logování) při operacích prováděných v databázích osobních údajů, povinnost zpracovat posouzení vlivu na ochranu osobních údajů (dále také „DPIA“ z anglického *data protection impact assessment*) a povinnost projednat s Úřadem pro ochranu osobních údajů (dále také „ÚOOÚ“) takové operace s osobními údaji, které představují vysoké riziko pro ochranu osobních údajů. V hlavě III ZZOÚ jsou tudíž uvedeny především obecné povinnosti zpracování osobních údajů pro donucovací orgány.

Zákonné zmocnění ke zpracování osobních údajů PČR se nachází v **zákoně č. 273/2008 Sb., o Policii České republiky**. Samotné zmocnění ke zpracování osobních údajů je upraveno v ustanovení § 79 odst. 2 ZPČR. Podle tohoto ustanovení může PČR zpracovávat osobní

údaje, je-li to nezbytné za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti ČR nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Tento obecný titul má dle zákonodárce opravňovat k jakémukoliv zpracování osobních údajů, protože v důvodové zprávě prakticky rezignoval na rozlišování mezi „běžnými“ a „citlivými“ osobními údaji, když uvádí: *„Stejně jako v obdobných ustanoveních dalších předpisů není nutné (...) uvádět výslovně, že policie může zpracovávat „jakékoliv“ osobní údaje, včetně údajů „citlivých“ nebo jiných, protože je to nepochybné. Z povahy věci neexistují (...) kategorie osobních údajů, které by policie zpracovávat nesměla.“*[32]

Výslovné omezením zpracování osobních údajů představuje § 79 odst. 3, který uvádí: *„Shromažďovat údaje o rasovém nebo etnickém původu, náboženském, filosofickém nebo politickém přesvědčení, členství v odborové organizaci, zdravotním stavu, sexuálním chování nebo sexuální orientaci lze pouze tehdy, je-li to nezbytné pro účely šetření konkrétního trestného činu nebo přestupku, nebo při poskytování ochrany osob.“* Výčet osobních údajů v citovaném ustanovení nekoresponduje plně se zvláštní kategorií osobních údajů, jak je definuje SOÚPP, protože omezení je užší a nevztahuje se na biometrické a genetické údaje. Biometrická struktura obličeje přitom není v ZPČR zmíněna vůbec.

Podle výkladu PČR je možné provádět biometrickou identifikaci z kamerových záběrů v reálném čase i zpětně bez bližší právní úpravy. Pro **biometrickou identifikaci v kamerových systémech v reálném čase** je dle PČR podstatný § 62 odst. 1 ZPČR, podle kterého může policie pořizovat zvukové, obrazové nebo jiné záznamy osob na veřejně přístupných místech. Ve spojení s obecným titulem ke zpracování osobních údajů (§ 79 odst. 2), je policie dle vlastního výkladu oprávněna provádět tento druh plošného sledování. Povinností policie je ovšem zveřejnění informací o pořizování záznamů, pokud je prováděno prostřednictvím stálých automatických technických systémů (§ 62 odst. 2 ZPČR).

Podobně „inovativní“ je policejní výklad § 66 odst. 1 a 2 ZPČR, podle kterého je možné provádět **biometrickou identifikaci z kamerových záznamů „zpětně“** oproti databázi všech osob žijících v ČR. Podle uvedeného ustanovení může PČR získávat a zpracovávat digitální fotografie a identifikátory lidí vedených v informačních systémech, konkrétně v informačním

32 Důvodová zpráva k zákonu č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, s. 156.

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 způsob zpracování digitálních fotografií, tak důvodová zpráva k novele ZPČR 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.“*[33] Zákon tudíž poněkud nepřímo počítá s tím, že záběry z kamer může PČR pomocí softwaru na identifikaci obličejů analyzovat a porovnávat s fotografiemi z databáze prakticky všech osob žijících v ČR.

Detailní regulace systémů biometrické identifikace na veřejných prostranstvích je upravena v podzákonných právních předpisech. Jedná se o **vnitřní předpisy** PČR, které jsou z velké části neveřejné a z nichž policie poskytla pouze torza na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále také „InfZ“). Některé detaily z těchto vnitřních předpisů jsou uvedeny u popisu jednotlivých systémů v následující kapitole.

33 Důvodová zpráva k zákonu č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, s. 154.

7. Nasazení v České republice

Rozsah nasazení systémů biometrické identifikace obličeje není s jistotou veřejně známý. Ze strany PČR a dalších donucovacích orgánů nedochází ke zveřejňovaní všech informací o nasazení této technologie, tudíž je možná situace, že veřejnost není dosud informována o všech systémech, které jsou v současnosti nasazeny. Navíc se jedná o rychle se rozvíjející oblast a informace v ní rychle zastarávají. Dosud jsou známy jen systémy biometrické identifikace obličeje, které provozuje PČR. V této kapitole jsou popsány dosud známé systémy biometrické identifikace a autentizace, které využívá či využívala PČR, a současně některé pokusy rozšířit jejich nasazení. Jejich základní přehled se nachází v tabulce 2.

Tabulka 2: Dosud známé systémy biometrické identifikace a autentizace obličeje na veřejných prostranstvích provozovaných PČR.

	Biometrická identifikace obličeje		**Biometrická autentizace obličeje**
	v reálném čase	**zpětná**	
Nasazené	Kamerový systém na Letišti Václava Havla v Praze	Informační systém Digitální podoba osob	Biometrické kontrolní brány na letišti Václava Havla v Praze
		Software EyeDentity	Mobilní inspekční biometrické systémy
Navrhované	Městský kamerový systém Hlavního města Praha	(nejsou známy)	(nejsou známy)
	Kamerový systém na Pražském hradě		
	Kamerové systémy na fotbalových stadionech		
	Kamerové systémy na mezinárodních letištích v Brně, Ostravě, Pardubicích a Karlových Varech		
	Prostory podzemní hromadné dopravy (metra) v Praze		

7.1 Kamerový systém Letiště Václava Havla v Praze

Zatím jediný v ČR známý kamerový systému biometrické identifikace v reálném čase se nachází na Letišti Václava Havla v Praze (dále také „LVHP“). Podle tiskové zprávy Ministerstva vnitra bylo rozmístěno celkem 145 kamer ve veřejném prostoru letiště na místech s vysokou koncentrací osob.[34] Systém biometrické identifikace byl spuštěn do zkušebního provozu dne 15. června 2018, ve kterém je provozován dodnes.

Dodavatelé biometrického identifikačního systému na LVHP 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."*[35] Systém funguje tak, že porovnává biometrické profily obličeje extrahované z obrazu zachyceného kamerovým systémem s policejní databází biometrických profilů obličeje zájmových osob, do níž jsou data čerpána z informačního systému Pátrání po osobách (PATROS). V tomto informačním systému jsou zpracovávány údaje o hledaných a pohřešovaných osobách. Systém umožňuje jak porovnávání v reálném čase, tak zpětné porovnávání díky uchovávání biometrických profilů obličejů, které byly zaznamenány kamerovým systémem v posledních 30 dnech. Podle sdělení PČR je pro snímání biometrických profilů obličeje v kamerovém systému užívána softwarová technologie NEC NeoFace Watch a NeoFace Archiver.[36] Celý kamerový systém s biometrickým zpracováním je dále propojen s dalšími bezpečnostními systémy a databázemi provozu letiště.

Vnitřní předpis policie, kterým se systém řídí je rozkaz policejního prezidenta č. 123/2018, ze dne 14. června 2018, kterým se upravuje zkušební provoz integrovaného bezpečnostního systému LETIŠTĚ. Krom toho, že tento rozkaz upravuje role jednotlivých policejních funkcionářů, obsahuje přílohu „Zásady zkušebního provozu systému LETIŠTĚ“. Tento dokument představuje zásadní předpis fungování systému, protože upravuje bližší

34 Ministerstvo vnitra. *Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů* [online]. mvcr.cz, 4. března 2019 [cit. 10. března 2024].

35 Ministerstvo vnitra. Smlouva o dílo ze dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV, č.j. PPR-27225-108/ČJ-2015-990656.

36 Rozhodnutí o odmítnutí žádosti podle InfZ Policejního prezidia ze dne 6. března 2023, č.j. PPR-11093-5/ČJ-2023-9908100.

podmínky, jako jsou účel, evidence přístupů nebo uschovací lhůty a likvidace údajů. Nicméně provozovatel a gestor systému - Ředitelství služby cizinecké policie – považuje vnitřní předpisy z podstatné části za neveřejné.[37]

Dle čl. 4 zásad zkušebního provozu systému využívají kromě PČR osobní údaje ze systému také další bezpečnostní sbory, kterými jsou Celní správa ČR, Bezpečnostní informační služba, Úřad pro zahraniční styk a informace a Vojenské zpravodajství. Každý z těchto bezpečnostních sborů přitom má vlastní oddělené úložiště určené ke zpracovávání údajů o osobách, které jsou předmětem zájmu těchto orgánů. Žádný z těchto orgánů nemá přístup k údajům o osobách (ani k informacím o jejich záchytu), která jsou předmětem zájmu jiného orgánu. Od spuštění systému dne 15. června 2018 až do 31. prosince 2023 došlo k celkem 259 shodám s osobami vedenými v zájmových databázích PČR.[38] Údaje o počtech policií hledaných osob zachycených kamerovým systémem v jednotlivých měsících od začátku provozu kamerového systému až do konce roku 2023 jsou v tabulce 3. V průběhu let je zřejmý především trend snižování efektivity systému.

Tabulka 3. Počet hledaných osob, které byly ztotožněny kamerovým systémem na LVHP za jednotlivé měsíce v letech 2018 až 2022.

Rok	Leden	Únor	Březen	Duben	Květen	Červen	Červenec	Srpen	Září	Říjen	Listopad	Prosinec	Celkem
2018	-	-	-	-	-	5	10	22	9	6	8	12	**72**
2019	11	10	13	2	4	15	5	22	6	2	6	6	**102**
2020	9	7	2	6	0	1	2	0	1	0	3	1	**32**
2021	0	0	0	0	0	0	0	0	0	0	0	0	**0**
2022	1	0	3	0	12	3	0	1	1	3	3	1	**28**
2023	0	5	3	0	0	3	2	4	3	2	1	2	**25**

7.2 Navrhované systémy biometrické identifikace obličeje v reálném čase

Systém biometrické identifikace obličeje byl navrhován v roce 2019 pro vstup na fotbalové stadiony. 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

37 Rozhodnutí o částečném odmítnutí žádosti podle InfZ Policejního prezidia ze dne 20. srpna 2020, č.j. PPR-24979-6/ČJ-2020-990810.

38 Informace poskytnutá dle InfZ ze dne 12. února 2024 vydaná Ředitelstvím služby cizinecké policie, č.j. PPR-6809-3/ČJ-2024-990810.

těchto osob na fotbalové stadiony. V reakci na to v srpnu 2019 vydal ÚOOÚ stanovisko, podle kterého *"nelze najít dostatečný právní důvod ke zpracování biometrických osobních údajů návštěvníků fotbalového utkání technologií face recognition."*[39] Následně se ÚOOÚ v březnu 2020 vyjádřil k navrhované novele zákona, která by uvedené zákonné zmocnění obsahovala. Návrh zákona ÚOOÚ nepodpořil, protože nebyla dostatečně zdůvodněna nezbytnost zpracování biometrických údajů ve srovnání s jinými možnostmi eliminace rizik násilí na stadionech.[40]

Dále proběhl pokus nasadit biometrickou identifikaci obličeje v reálném čase v městském kamerovém systému hlavního města Prahy v roce 2019.[41] Na základě žádosti PČR o aktivaci funkce identifikace obličeje na šesti lokalitách městského kamerového systému v Praze se Magistrát hlavního města Prahy obrátil na ÚOOÚ se žádostí o konzultaci.[42] Z důvodu nutnosti zpracování DPIA dle § 37 ZZOÚ byl další postup ze strany Magistrátu hlavního města Prahy přenechán PČR, která měla být současně zpracovatelem biometrických údajů získaných z pražského kamerového systému.[43] K dalším krokům ze strany PČR následně nedošlo.

Ministerstvo vnitra ve spolupráci s PČR dále plánovalo nasazení kamerových systémů s biometrickou identifikací obličeje v reálném čase na všech zbývajících mezinárodních letištích v ČR: Brno, Ostrava, Pardubice a Karlovy Vary. Instalace těchto kamerových systémů měla být dle plánu Ministerstva vnitra realizována do konce roku 2020.[44] Nicméně od tohoto plánu bylo z dosud neupřesněných důvodů upuštěno. Podobně došlo ke krokům

39 ÚOOÚ. *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech* [online]. uoou.gov.cz, 16. srpna 2019 [cit. 10. března 2024].

40 ÚOOÚ. *Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech* [online]. uoou.gov.cz, 27. března 2020 [cit. 10. března 2024].

41 Česká televize. *Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti* [online]. Česká televize, 20. listopadu 2019 [cit. 10. března 2024].

42 Vyjádření ÚOOÚ k žádosti o konzultaci k městskému kamerovému systému hl. m. Prahy ze dne 3. prosince 2019, č.j. UOOU-04829/19-2.

43 Informace poskytnutá dle InfZ ze dne 18. srpna 2020 vydaná Magistrátem hlavního města Praha, č.j. MHMP 1270148/2020.

44 Ministerstvo vnitra. *Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích* [online]. mvcr.cz, 18. února 2018 [cit. 10. března 2024].

rozmístit kamerové systémy s biometrickou identifikací obličeje v reálném čase na Pražském hradě[45] a v pražském metru[46].

7.3 Informační systém Digitální podoba osob

Informační systém Digitální podoba osob (dále také „IS DPO“) představuje systém provozovaný PČR ke zpětné biometrické identifikaci na dálku, což znamená, že v něm nedochází k rozpoznávání osob v reálném čase. Účelem informačního systému je ztotožnění zájmové osoby důležitých pro konkrétní trestní řízení (pachatele, svědka či poškozeného), které byly zachyceny na fotografii nebo jiném obrazovém záznamu. Zkušební provoz systému probíhá od 22. srpna 2022 dodnes. Vnitřní předpis PČR, kterým se systém řídí je rozkaz policejního prezidenta č. 194/2022, k zajištění zkušebního provozu informačního systému Digitální podoba osob. Rozkaz upravuje především kompetence jednotlivých složek PČR v souvislosti se zahájením zkušebního provozu, nicméně jeho součástí je příloha „Zásady zkušebního provozu systému DPO“. V zásadách zkušebního provozu jsou uvedeny podrobnosti ohledně účelu systému, evidence přístupů a další pravidla využívání systému, přičemž podstatné části tohoto pokynu PČR odmítá poskytnout na základě InfZ.

V rámci IS DPO dochází ke zpětnému biometrickému porovnání fotografie neznámé osoby oproti referenční databázi, která se skládá z fotografií poskytnutých ze zdrojových databází. Zdrojovými databázemi jsou digitální fotografie z a) informačního systému evidence občanských průkazů; b) informačního systému evidence cestovních dokladů; c) informačního systému evidence diplomatických a služebních pasů; d) registru řidičů; e) centrálního registru řidičů; f) informačního systému cizinců. V databázi se tudíž nachází prakticky každá osoba zdržující se trvale v ČR a dle vyjádření Policejního prezidia se v červenci 2023 nacházelo v referenční databázi celkem 19 666 787 fotografií osob.[47] Systém by měl do 15 sekund poskytnout požadovaný počet jednoznačných identifikátorů fotografií osob, u nichž je

45 Česká televize. *Události komentáře (čas 33:22)* [online]. Česká televize, 17. dubna 2023 [cit. 10. března 2024].

46 MAREŠ, Miroslav a kol. *Kamerový systém Dopravního podniku hlavního města Prahy v komparativním kontextu bezpečnosti a ochrany osobních údajů.* Praha: Dopravní podnik Hlavního města, 2021, 139 s.

47 Informace poskytnutá dle InfZ ze dne 16. srpna 2023 vydaná Policejním prezidiem, č.j. PPR-35618-5/ČJ-2023-990810.

nejvyšší míra shody se zájmovou osobou na vložené fotografii. Každá fotografie v databázi je spojena s individuálním identifikátorem, přes nějž se policista dostane jednoduše k dalším údajům, jako je jméno, příjmení, bydliště, či datum narození osoby na fotografii.

Do informačního systému má přístup celkem 73 osob, které jsou zařazeny na 3 útvarech PČR: Policejním prezidiu, Národní centrále proti organizovanému zločinu a Národní centrále proti terorismu, extremismu a kybernetické kriminalitě. Jedná se o 37 operačních důstojníků z důvodu zastupitelnosti a směnnosti služby, z nich 7 osob zajišťuje technický provoz, zbývající osoby jsou příslušníci služby kriminální policie a vyšetřování. Ke dni 22. července 2023 (za prvních 11 měsíců provozu) bylo vyřízeno celkem 149 žádostí o využití funkce porovnání zaznamenané fotografie oproti celé referenční databázi.[48]

7.4 Software EyeDentity

Krajské ředitelství policie Ústeckého kraje (dále také „KŘP ÚK“) v minulosti používalo software EyeDentity, který slouží ke zpětné biometrické identifikaci obličeje z obrazových záznamů. Softwarová společnost Eyedea Recognition poskytla krajskému ředitelství software EyeDentity s licencí a technickou podporou na dva roky (od listopadu 2018 do listopadu 2020).[49] EyeDentity je počítačový software, který slouží k automatickému prohledávání digitálních obrazových dat za účelem lokalizace, kategorizace, identifikace a autentizace osob. Program zpracovává obrázky a videa v různých formátech, rozlišení a kvalitě; detekuje v nich obličeje; a provádí na nich další biometrické operace.

Software umožňuje zejména: lokalizovat obličeje v rozsáhlých souborech videozáznamů a fotografií; odhadovat věk a pohlaví zachycené osoby; řadit a vyhledávat obličeje na základě vizuální podobnosti k obličejům v interní databázi. Součástí software je databáze obsahující vyobrazení a identifikační údaje zájmových osob. Databáze je spravována skrze uživatelské rozhraní, přičemž uživatel může přidávat a odebírat osoby, editovat identifikační údaje

48 Tamtéž

49 KŘP ÚK. Licenční smlouvy ze dne 20. listopadu 2018 a dne 19. listopadu 2019. Poskytnutí licence pro software EyeDentity, č.j. KRPU-209961-6/ČJ-2018-0400IT-02A a KRPU-167484-6/ČJ-2019-0400IT-03.

a poznámky. Analytické jádro softwaru je založeno na algoritmech umělé inteligence. Aplikace může pracovat s databází obsahující až několik tisíc osob.

KŘP ÚK sdělilo, že užívání softwaru EyeDentity nebylo formalizované vnitřními předpisy. Software byl nainstalován na jednom počítači a měl k němu přístup pouze jeden policista, který byl zařazen na odboru analytiky a kybernetické kriminality krajského ředitelství. Software neprováděl logování činností, protože nebyl napojen na žádné evidence či informační systémy, a tudíž ani není zaevidováno, v kolika případech byl software během licence využit. Policista, který software EyeDentity obsluhoval, nebyl v době podání žádosti o informace dle InfZ ve služebním poměru, tudíž informace, pro jak závažné případy (přestupky či trestné činy) a pro jaké procesní postavení osob (svědek či podezřelý) byl software využíván, již nebylo možné zjistit. Užívání software probíhalo v zásadě tak, že dožadující policista dodal v případě potřeby policistovi, který software obsluhoval, fotografii neznámé zájmové osoby a zároveň množinu fotografií, se kterou měla být fotografie neznámé zájmové osoby biometricky porovnána.[50]

7.5 Biometrická autentizace

PČR využívá systémy biometrické autentizace obličeje. Především to jsou tzv. mobilní inspekční biometrické systémy. Jedná se o informační systém pro kontrolu osob pomocí biometrických prvků. Pokud probíhá kontrola totožnosti konkrétní osoby informační systém je schopný na základě na místě pořízené fotografie nebo odebraného otisku prstu kontrolované osoby ověřit její totožnost. Systém umožňuje mobilní kontrolu identity využitím biometrických prvků a prověření na výskyt v databázích PČR a ostatních bezpečnostních sborů, členských států EU a mezinárodních organizací.[51]

Další systém biometrické autentizace obličeje provozovaný PČR jsou biometrické kontrolní brány na LVHP.[52] Jedná se o systém biometrického odbavování cestujících, kteří

50 Informace poskytnutá dle InfZ ze dne 14. září 2023 vydaná KŘP ÚK, č.j. KRPU-166623-2/ČJ-2023-0400KR-PI.

51 Ministerstvo vnitra. Kupní smlouva ze dne 22. prosince 2016. Vybudování mobilního biometrického inspekčního systému a dodávka kontrolních zařízení, č.j. PPR-22247-26/ČJ-2016-990656.

52 PČR. *eGATE - rychlejší odbavování na letišti* [online]. policie.cz, 23. července 2015 [cit. 10. března 2024].

jsou občané EU, Evropského hospodářského prostoru a Švýcarska, starší 15 let, a kteří létají mimo Schengenský prostor a vlastní cestovní pas s biometrickými údaji. Cestující vloží cestovní doklad do čtecího zařízení, kde proběhne kontrola dat, poté přistoupí k bráně a pohyblivá biometrická kamera provede biometrickou autentizaci obličeje. Pokud biometrické údaje pořízené kamerou souhlasí s těmi uloženými v cestovním pasu, otevřou se vstupní dveře brány a cestující může překročit hranici.

8. Právní posouzení nasazených systémů

V této kapitole je posouzena souladnost nasazených systémů biometrické identifikace obličeje popsaných v kapitole 7 s právním řádem. Nasazené systémy biometrické autentizace obličeje posouzeny nejsou, protože jejich užívání není z hlediska ochrany osobních údajů natolik problematické. Právní posouzení v této kapitole systémy analyzuje z hlediska evropské a české právní úpravy. Posouzení nasazených systémů z hlediska proporcionality zásahu do základních práv je předmětem kapitoly 9.

8.1 Kamerový systém Letiště Václava Havla v Praze

Podle mých zjištění je provoz kamerového systému s biometrickou identifikací na LVHP provozován bez řádného splnění všech zákonných povinností. Za porušení zákona považuji skutečnost, že PČR před spuštěním provozu systému nezpracovala obligatorní DPIA dle čl. 27 SOÚPP a § 37 ZZOÚ. Dalším problémem zpracování je zákonnost, kdy PČR za zákonný titul k provozu kamerového systému s biometrickou identifikací na LVHP považuje § 62 odst. 1 a § 79 odst. 2 ZPČR, výkladem který je uveden v kapitole 6.

Povinnost zpracovat DPIA je stanoven ve čl. 27 SOÚPP, který je proveden v § 37 ZZOÚ. 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, s přihlédnutím k povaze, rozsahu, kontextu a účelům, bude mít za následek vysoké riziko pro práva a svobody fyzických osob.[53] Používání kamerových systémů k biometrické identifikaci osob na veřejných prostranstvích v reálném čase tyto podmínky naplňuje a DPIA bude podléhat prakticky vždy.[54] DPIA 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 mechanismy

53 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář.* 2. aktualizované vydání. Praha: Leges, 2019, s. 630.

54 ÚOOÚ. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2020, s 8-16.

k zajištění ochrany osobních údajů a k doložení souladu se SOÚPP, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

ZZOÚ vešel v účinnost až dne 24. dubna 2019, což je více než deset měsíců poté, kdy byl spuštěn kamerový systém s biometrickou identifikací na LVHP. Tudíž povinnost zpracovat DPIA nelze dovodit přímo ze ZZOÚ, nicméně jde tato povinnost dovodit z přímého účinku SOÚPP. SOÚPP byla přijata již 27. dubna 2016 a stanovovala členským státům povinnost provést ji do dvou let. Přesto nebylo DPIA pro kamerový systém s biometrickou identifikací na LVHP zpracováno minimálně do 24. srpna 2020. PČR tuto skutečnost obhajuje tvrzením, že v době spuštění sledovacího systému do zkušebního provozu, nebyla SOÚPP do národní legislativy transformována a postačovala prý ohlašovací povinnost na ÚOOÚ.[55] Mám za to, že tato argumentace není správná a to zejména z důvodu přímé aplikace SOÚPP.

Směrnice nemají obecně přímý účinek ve vnitrostátním právu členských států, jako je to u nařízení. Nicméně čl. 63 odst. 1 SOÚPP, který stanový podmínky provedení ve vnitrostátním právu, ukládá povinnost členských států přijmout, zveřejnit a uvést v platnost právní předpisy nezbytné pro dosažení souladu se SOÚPP do 6. května 2018. Evropský soudní dvůr ve své judikatuře stanovil, že směrnice mají přímý účinek, jsou-li jejich ustanovení bezpodmínečná, dostatečně jasná a přesná a pokud členský stát EU neprovedl směrnici ve stanovené lhůtě.[56] Tyto požadavky jsou dle mého názoru splněny. Přestože bylo později Evropským soudním dvorem určeno, že přímý účinek směrnic je jen vertikální vzestupný, tj. jednotlivec se může dovolávat svých práv vyplývajících ze směrnice proti příslušnému členskému státu, který směrnici netransponoval či ji transponoval nesprávně.[57] V našem případě je také tento požadavek splněn, protože SOÚPP ukládá povinnost členskému státu chránit citlivé osobní údaje jeho občanů. SOÚPP totiž dostatečně určitě ukládá členskému státu chránit citlivé osobní údaje jednotlivců a PČR je nepochybně orgánem státu, kterému tak ze SOÚPP vyplývá přímá povinnost. Z výše uvedeného důvodu mám za to, že v daném případě došlo k porušení povinnosti vyplývající z evropského práva. K možnosti přímého účinku SOÚPP z důvodu její pozdní implementace do českého práva se vyjadřuje

55 Informace poskytnutá dle InfZ ze dne 24. srpna 2020 vydané Policejním prezidiem, č.j. PPR-24979-5/ČJ-2020-990810.

56 Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 4. prosince 1974, *Van Duyn proti Home Office*, 41/74.

57 Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 26. února 1984, *Marshall proti Southampton and South-West Hampshire Area Health Authority*, 152/84.

také komentář nakladatelství Leges, který uvádí: *„(…) v případě směrnice 2016/680 tak bylo možné zvažovat její přímou aplikaci zejména v mezidobí od 6. května 2018, kdy měla být nejpozději transponována, do nabytí účinnosti ZZOÚ.“*[58]

SOÚPP v čl. 57 ukládá členským státům povinnost stanovit sankce za porušení předpisů přijatých na základě směrnice a přijmout veškerá opatření nezbytná k zajištění jejich uplatňování. Sankce musí být účinné, přiměřené a odrazující. ZZOÚ provádí sankce v hlavě VI, kde je v § 63 odst. 1. písm. k) stanoveno, že právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s § 37 ZZOÚ neprovede DPIA. Podle § 63 odst. 3. ZZOÚ lze za tento přestupek uložit pokutu do 10 000 000 Kč. Možná sankce ovšem v tomto případě nemůže vyplývat přímo ze SOÚPP, protože znění SOÚPP v případě sankcí nesplňuje judikaturou dovozenou podmínku přesnosti tak, aby mohlo být ustanovení přímo aplikována. O sankci lze tudíž uvažovat až od účinnosti ZZOÚ, přičemž zpracování skutečně započalo před účinností. Již od listopadu 2021 prověřuje ÚOOÚ v souvislosti kamerovým systémem s biometrickou identifikací na LVHP podnět, který se týká neprovedení DPIA.

Problematická je také otázka právního základu provozu kamerových systémů s biometrickou identifikací obličeje v reálném čase. V souladu s čl. 10 SOÚPP lze zpracovávat biometrické osobní údaje pouze tehdy, pokud je to zcela nezbytné, pokud existují vhodné záruky práv a svobod subjektu údajů a pokud je povoleno právem EU nebo členského státu. Obdobně jsou pro zpracování osobních údajů kladeny požadavky v zásadě zákonnosti v čl. 8 odst. 2 SOÚPP, podle kterého: *"Právo členského státu upravující zpracování v oblasti působnosti této směrnice stanoví alespoň cíle zpracování, osobní údaje, jež mají být zpracovány, a účely zpracování."* V této souvislosti je navíc potřeba připomenout také princip zákonnosti v národním právním řádu či z něj vyplývající zásadu enumerativnosti veřejnoprávních pretenzí zakotvenou v čl. 2 odst. 3 Ústavy ČR a čl. 2 odst. 2 LZPS, která stanovuje, že státní moc lze uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví. Podle mého názoru dostatečný právní základ zpracování v českém právním řádu v dostatečné kvalitě chybí a nelze za ně považovat § 62 odst. 1 a § 79 odst. 2 ZPČR.

58 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář*. 2. aktualizované vydání. Praha: Leges, 2019, 752 s.

Podle § 62 odst. 1 ZPČR může policie, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu. O toto ustanovení se opírá provoz běžných kamerových systémů. Z uvedeného ustanovení ZPČR tudíž nevyplývá oprávnění zpracovávat obrazové záznamy za účelem sestavení biometrických profilů obličeje, tyto biometrické profily dále uchovávat a využívat k porovnávání s biometrickými profily obličeje uloženými v databázi. Toto oprávnění nevyplývá ani z žádných dalších ustanovení ZPČR. Mám za to, že v daném případě není možné aplikovat obecné oprávnění PČR zpracovávat osobní údaje dle § 79 odst. 2 ZPČR, které říká, že osobní údaje může PČR zpracovávat, pokud je to nezbytné k plnění jejích úkolů. Domnívám se, že ZPČR nijak neupravuje oprávnění PČR zpracovávat biometrické údaje obličeje provozem kamerového systému na biometrickou identifikaci obličeje. Mám tedy za to, že biometrická identifikace obličeje v kamerových systémech je v rozporu evropským právem (čl. 8 odst. 1 a 2 a čl. 10 SOÚPP).

Pochybnosti o minimálního rozsahu právní úpravy členského státu vyplývající z čl. 10 SOÚPP má v souvislosti se zpracováváním zvláštní kategorie osobních údajů také sedmý senát Nejvyššího správního soudu. Ten v případě projednávaní zásahové žaloby na uchovávání profilu DNA v databázi PČR předložil[59] před SDEU předběžnou otázku ve znění:

> *„3) V případě zvláště citlivých osobních údajů spadajících pod čl. 10 Směrnice č. 2016/680, jaký je minimální rozsah hmotně-právních či procesních podmínek získávání, uchovávání, a vymazání těchto údajů, který musí být v právu členského státu upraven „obecně závazným předpisem“? Může mít kvalitu „práva členského státu“ ve smyslu článku 8 odst. 2 ve spojení s čl. 10 Směrnice 2016/680 také judikatura soudní?“*[60]

Předložená předběžná otázka, která dosud nebyla SDEU závazně interpretována, bude mít jistě mnohem širší dopad, než jen na konkrétní řízení, ve kterém byla předložena. Policejní databáze profilů DNA má alespoň základní (i když minimální) zákonnou úpravu

59 NSS: usnesení NSS o předložení předběžné otázky ze dne 26. ledna 2023, č.j. As 172/2022-56.
60 Řízení je vedeno před SDEU jako věc C-57/23, doručená dne 2. února 2023.

oproti systémům biometrické identifikace obličeje, jejichž úprava je pouze interpretována z obecného zákonného ustanovení o zpracování osobních údajů.

8.2 Informační systém Digitální podoba osob

PČR považuje za zákonné oprávnění k provozu IS DPO § 66a a § 79 odst. 2 ZPČR (viz kapitola 6). Ustanovení § 66a odst. 1 ZPČR dává PČR oprávnění vytěžovat a následně zpracovávat digitální fotografie ze státních evidencí. Dále § 66a odst. 3 ZPČR uvádí: *„Osobní údaje podle odstavce 1 může policie využívat pouze pro identifikaci konkrétní osoby při plnění účelů uvedených v § 79 odst. 1“*. Nicméně ustanovení přímo neuvádí možnost plošného biometrického zpracování obličeje všech občanů, ani základní parametry a pravidla pro fungování a užití IS DPO. Podle mého názoru se nemůže jednat o dostatečné zákonné oprávnění v souladu s pravidly stanovenými v SOÚPP. V tomto případě nastává obdobná situace, jako v případě nedostatečné právní úpravy kamerových systému s biometrickou identifikací obličeje v reálném čase. Jistotu může také v tomto případě přinést závazná interpretace SDEU výše uvedené předběžné otázky, která by mohla také v tomto případě ujasnit minimální nezbytný rozsah právní úpravy.

Pro IS DPO zpracovala PČR v roce 2023 DPIA dle § 37 ZZOÚ, který zní: *„Je-li pravděpodobné, že určitý druh připravovaného zpracování osobních údajů povede (...) k vysokému riziku neoprávněného zásahu do práv a svobod subjektů údajů, vypracuje spravující orgán posouzení vlivu takového zpracování na ochranu osobních údajů.“* Nicméně DPIA nebylo zpracováno souladně s dikcí čl. 27 SOÚPP, který uvádí: *„Pokud je pravděpodobné, že určitý druh zpracování (...) bude (...) mít za následek vysoké riziko pro práva a svobody fyzických osob, členské státy stanoví, že správce* ***před zpracováním*** *provede posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.“* Uvedené ustanovení SOÚPP uvádí, že DPIA musí být zpracováno před započetím zpracování, což dle dostupných informací nebylo. Zpracování bylo započato již v srpnu 2022, tedy dříve, než bylo v roce 2023 zpracováno DPIA.

V uvedeném případu se uplatní eurokonformní výklad, neboli tzv. nepřímý účinek práva EU. Podstata euro-konformního výkladu spočívá v tom, že unijní norma není aplikována přímo, ale je zohledněna při výkladu vnitrostátního práva. Jinými slovy pokud je možné interpretovat vnitrostátní právo různým způsobem, musí se zvolit ten, který vede k výsledku odpovídajícímu znění a účelu unijní normy.[61] Tato zásada byla formulována judikaturou SDEU.[62] Z tohoto důvodu se domnívám, že je nutné vykládat ustanovení § 37 ZZOÚ tak, že je nutné vypracovat DPIA ještě před započetím zpracovávání. Stejný názor, že DPIA musí být zpracováno ještě před začátkem zpracování, uvádí také dostupná komentářová literatura,[63] [64] [65] ač v souvislosti s tímto konkrétním ustanovením eurokonformní výklad nezmiňuje. Nicméně k nutnosti eurokonformního výkladu celé hlavy ZZOÚ nabádá komentář nakladatelství Leges, když uvádí: *„Pokud tak budou některý ustanovení hlavy III ZZOÚ nejasný či mohou nabízet dvojí různý výklad, soudy jsou povinny vykládat tyto vnitrostátní normy eurokonformně, tj. ve světle znění a účelu směrnice 2016/680 a jí poskytovaných práv, a to takovým způsobem, aby byl vždy upřednostněn z možných výkladů vnitrostátního práva takový, který nejlépe umožní zajistit efektivitu unijního práva."*[66]

V souladu s tím by mělo být vykládáno také ustanovení o přestupcích v § 63 odst. 1. písm. k) ZZOÚ stanovující, že právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s § 37 ZZOÚ neprovede DPIA. Zde je třeba uvést, že hrozba pokuty dle § 63 odst. 3 ZZOÚ až do výše 10 000 000 Kč je reálná, protože orgány veřejné moci nejsou za přestupky předvídané v čl. 57 SOÚPP osvobozeny od sankcí, tak jako tomu je v případě přestupků ukládaných dle GDPR. Skutečnost, že lze za nedodržení ustanovení SOÚPP ukládat sankce také orgánům veřejné moci, uvádí dostupná komentářová

61 TOMÁŠEK, Michal a kol. *Právo Evropské unie*. 3. aktualizované vydání. Praha: Leges, 2021, 512 s.
62 Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 10. dubna 1984, *Von Colson a Kamann*, C-14/83.
63 NULÍČEK, Michal a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Praha: Wolters Kluwer, 2019, 212 s.
64 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář.* 2. aktualizované vydání. Praha: Leges, 2019, 752 s.
65 BAČA, Ján a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Plzeň: Aleš Čeněk, 2020, 361 s.
66 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář.* 2. aktualizované vydání. Praha: Leges, 2019, 752 s.

literatura.[67] [68] [69] [70] V uvedeném případě by byl orgánem veřejné moci odpovědným za přestupek Ministerstvo vnitra, které je zpravidla pasivně legitimované v případech, kdy vystupuje PČR v roli bezpečnostního sboru.

8.3 Software EyeDentity

Podle vyjádření KŘP ÚK před používáním softwaru EyeDentity nebylo zpracováno DPIA podle § 37 ZZOÚ, ani nebylo zpracování konzultováno s ÚOOÚ ve smyslu § 38 ZZOÚ.[71] Povinnost zpracovat DPIA se dle mého názoru vztahuje také na využívání softwaru EyeDentity, protože je pravděpodobné, že zpracování biometrických údajů softwarem bude mít za následek vysoké riziko pro práva a svobody fyzických osob. V souvislosti s tím, zda dané zpracování podléhá nebo nepodléhá vypracování DPIA byl ÚOOÚ vytvořen manuál.[72] Uvedený manuál obsahuje seznam deseti kritérií, přičemž zpracování osobních údajů se dle každého kritéria dělí do tří úrovní: kritické hodnoty, významné hodnoty, nízké hodnoty. Zařazení mezi zpracování spojené s povinností zpracovat DPIA se stanoví dle počtu dosažených úrovní v jednotlivých kritériích. Pokud úroveň dvou a více kritérií dosáhne mezi kritické, nebo pokud jedna úroveň zasáhne mezi kritické a zároveň nejméně pět kritérií dosáhne úrovně významné, potom se DPIA zpracovává. Uvedené zpracování softwarem EyeDentity dosahuje dle mého hodnocení kritických hodnot minimálně ve třech kritériích uvedených v manuálu.

Přestože byla licence softwaru EyeDentity zakoupena ještě před účinností ZZOÚ, který tuto povinnost stanovil v národním právním řádu, byla zakoupena po uplynutí implementační lhůty v čl. 63 odst. 1 SOÚPP. Z uvedeného důvodu vznikla povinnost KŘP ÚK povinnost

67 NULÍČEK, Michal a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Praha: Wolters Kluwer, 2019, 212 s.
68 PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář*. 2. aktualizované vydání. Praha: Leges, 2019, 752 s.
69 BAČA, Ján a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Plzeň: Aleš Čeněk, 2020, 361 s.
70 VLACHOVÁ, Barbora, MAISNER, Martin. *Zákon o zpracování osobních údajů. Komentář*. Praha: C. H. Beck, 2019, 163 s.
71 Informace poskytnutá dle InfZ ze dne 11. září 2023 vydaná KŘP ÚK, č.j. KRPU-160885-2/ČJ-2023-0400KR-PI.
72 ÚOOÚ. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2020, s. 8-16.

řídit se SOÚPP již před schválením ZZOÚ, a zpracovat DPIA a to na základě přímého účinku směrnice argumentací, která je uvedena v kapitole 8.1.

Dle mého názoru tak chybně argumentují autoři komentáře k ZZOÚ nakladatelství Aleš Čeněk, když k § 27 ZZOÚ uvádí: *„Jazykovým výkladem tohoto ustanovení lze dojít k závěru, že spravující orgán není povinen toto posouzení provádět pro zpracování, které je v působnosti hlavy III ZZOÚ a zároveň bylo zahájeno před přijetím zmiňovaného zákona.“*[73] Autoři nicméně pokračují: *„(...) lze doporučit, aby spravující orgán, pokud přistoupí ke změnám či úpravám v rámci stávajících činností zpracování, provedl posouzení vlivu na ochranu osobních údajů (...) byť již existujícího zpracování (...)"*[74] Takovou situaci lze uvažovat v případě využití software EyeDentity, protože v listopadu 2019 – tudíž již v době účinnosti ZZOÚ – byla KŘP ÚK zakoupena nová/prodloužena licence. Nicméně není jisté, zda by zakoupení nové licence či prodloužení staré mohlo být považováno za započetí nového zpracování. To by dle mého názoru nepochybně nastalo pokud by došlo k úpravám algoritmu nebo jiným změnám softwaru v rámci nové licence.

Z výše uvedených skutečností se domnívám, že použitím softwaru EyeDentity mohlo dojít k přestupku dle § 63 odst. 1. písm. k) ZZOÚ, dle kterého právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů neprovede DPIA. Problematická je také uživatelská praxe softwaru EyeDentity, která byla popsána v kapitole 7.4. Popsaná praxe zpracování osobních údajů opět signalizuje, že během užívání mohlo dojít k celé řadě přestupků. Zejména by se mohlo jednat o přestupky dle dle § 63 odst. 1 ZZOÚ dle písmen:

g) nepřijetí technických a organizačních opatření a nevedení jejich dokumentace,

i) nepořizování záznamů,

n) nepřijetí organizačních a technických opatření k zajištění odpovídající úrovně zabezpečení osobních údajů,

o) nepřijetí nezbytných opatření, a

s) poruší omezení zpracování zvláštních kategorií osobních údajů.

Za výše uvedené přestupky by bylo odpovědné Ministerstvo vnitra (pokud KŘP ÚK jednalo jako bezpečnostní sbor), případně samotné KŘP ÚK (pokud jednalo jako správní orgán). Nicméně vzhledem ke skutečnosti, že činnosti zanechalo již v listopadu 2020, kdy

73 BAČA, Ján a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Plzeň: Aleš Čeněk, 2020, 361 s.
74 Tamtéž

vypršela licence užívání software, uplynula již tříletá promlčecí lhůta stanovená dle § 30 písm. b) zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

9. Hodnocení proporcionality

V této kapitole se pokouším zhodnotit proporcionalitu zásahu do základních práv u dvou systémů biometrické identifikace obličeje popsaných v kapitole 7. Těmito systémy jsou kamerový systém s biometrickou identifikací obličej na LVHP a IS DPO. Pozornost zde není věnována systémům biometrické autentizace (či verifikace) obličeje, protože tyto systémy nepředstavují zvýšené riziko zásahu do základních práv. Podobně není věnována pozornost ani softwaru EyeDentity, protože jeho nasazení představovalo pravděpodobně jen dočasnou a lokální záležitost a nadále již není policií využíván.

Jakýkoli zásah do základních práv – včetně zpracovávání osobních údajů systémy biometrické identifikace obličeje – podléhá splnění určitých hodnotících kritérií, která se promítají do tzv. testu proporcionality. Jedná se o test, který je aplikovaný ÚS[75] při hodnocení zásahů do základních práv, přičemž se skládá ze tří kroků. Prvním krokem je posouzení, zda je zásah do základních práv vhodný, to znamená, že naplňuje legitimní cíl v podobě veřejného zájmu nebo ochrany práv a svobod druhých. Druhým krokem je posouzení, zda je zásah nezbytný, to znamená, že legitimního cíle nelze dosáhnout vhodnějším způsobem. Třetím krokem je posouzení proporcionality v užším smyslu, tj. posouzení, zda význam zásahu je dostatečně závažný, aby převážil zájem na ochraně základních práv. Dosavadní nasazení biometrické identifikace obličeje na veřejných prostranstvích splnění těchto právních kritérií podle mého názoru neprokázala.

Před provedením testu proporcionality je nezbytné vymezit **zasažená základní práva** a také veřejný zájem, v jehož zájmu je opatření v podobě biometrické identifikace obličeje na veřejném prostranství nasazeno. Výčet zasažených základních práv se nachází v tabulce 1 v kapitole 4. Nejprve je však třeba rozhodnout, zda je nutné podrobit všechna uvedená základní práva testu proporcionality. Domnívám se, že v případě zákazu diskriminace a práva na spravedlivý proces není provedení testu nutné, protože zásahy do těchto dvou práv lze úspěšně eliminovat či minimalizovat. K diskriminaci dochází samotným algoritmem, který může vykazovat systematickou chybovost pro zranitelné menšiny. Nicméně je možné

75 ÚS: nález pléna ÚS ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94.

takovéto diskriminaci předcházet, pokud bude vytvořen algoritmus biometrické identifikace na datech, která reprezentují všechny demografické skupiny.[76] Zdokonalením rozpoznávacích algoritmů biometrické identifikace obličeje tak lze dosáhnout souladu se zákazem diskriminace. Vhodnými provozními podmínkami včetně důsledné transparence se lze vyhnout či minimalizovat zásah do práva na spravedlivý proces. V případě důstojnosti je situace složitější, protože se jedná o základní právo, nad kterým nemůže žádný veřejný zájem převážit, neboť si zasluhuje nekompromisní ochranu.[77] Z tohoto důvodu na lidskou důstojnost neaplikuje test proporcionality ani ÚS. Nicméně pokud by skutečně došlo k zásahu do lidské důstojnosti, nasazené technologie by z hlediska ochrany základních práv nemohly obstát.

Biometrickou identifikací obličeje na veřejném prostranství dochází nepochybně vždy k zásahu do práva na informační sebeurčení a také do práva na soukromí. Obě tato základní práva jsou omezitelná, takže na zásahy do nich se test proporcionality aplikuje. Zásahům do těchto dvou základních práv se použitím biometrické identifikace obličeje nelze prakticky vyhnout. Navíc nasazením biometrické technologie v kamerovém systému na LVHP, tak v IS DPO, k zásahu do těchto práv nepochybně dochází.

Zásah do základního práva, má-li být přípustný, musí mít **zákonný podklad**, což vyplývá z čl. 4 odst. 2 LZPS, podle kterého meze základních práv a svobod mohou být upraveny pouze zákonem. Daná právní úprava musí být přesná a zřetelná ve svých formulacích a dostatečně předvídatelná, aby potenciálně dotčeným jednotlivcům poskytovala dostatečnou informaci o okolnostech a podmínkách, za kterých je veřejná moc oprávněna k zásahu do jejich základních práv. Rovněž musí být striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování.[78]

K takovému zákonnému podkladu ÚS uvedl v plenárním nálezu Data retention II následující: *„Nezbytnost disponovat takovými zárukami je o to větší, když se jedná o ochranu osobních údajů podrobených automatickému zpracování, zejména pokud jsou tyto údaje využívané k policejním cílům a v situaci, kdy se dostupné technologie stávají stále*

76 DOMINGO JARAMILLO, Cristina. Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital*, 2021, roč. 9, č. 1, s. 20-37.
77 BARAK, Aharon. Human Dignity. The Constitutional Value and the Constitutional Right. *Human Rights Law Review*, 2015, roč. 16, č. 1, s 175 – 176.
78 ÚS: nález pléna ÚS ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11.

komplikovanějšími.“[79] Také ESLP, který konstatoval porušení práva na respektování soukromého života v souvislosti s biometrickou technologií, uvedl k požadavku na „kvalitu práva“ následující: *„Soud se domnívá, že v kontextu zavádění technologie rozpoznávání obličeje je zásadní mít podrobná pravidla upravující rozsah a aplikaci opatření stejně jako silné záruky proti riziku zneužití a svévole. Potřeba ochranných opatření bude o to větší, pokud jde o použití technologie živého rozpoznávání obličeje.“*[80]

Domnívám se, že dostatečná zákonná úprava zásahu do práva na soukromí v důsledku biometrické identifikace obličeje v českém právním řádu absentuje. Zde odkazuji na kapitolu 8, kde je podrobněji rozebrána problematika nedostatků právní úpravy z hlediska požadavků evropského práva. Přestože je možné skončit závěrem, že nasazení biometrické identifikace obličeje na veřejném prostranství nesplňuje nutné požadavky ochrany základních práv, jedná se o nedostatek formální, do budoucna v zásadě napravitelný přijmutím legislativních změn.

Účelem nasazení biometrického rozpoznávání v kamerovém systému na LVHP a IS DPO, je prevence a ochrana před trestnou činností a také odvrácení závažných ohrožení veřejné bezpečnosti a pořádku. Tento účel lze podřadit pod **zájem na veřejné bezpečnosti**. Přestože LZPS výslovně neuvádí, kterými veřejnými zájmy lze právo na soukromí a na informační sebeurčení omezit, je nepochybné, že tímto veřejným zájmem může být veřejná bezpečnost, což je v souladu s judikaturou ÚS.[81] Veřejná bezpečnost obstojí také jako zájem aprobovaný čl. 8 odst. 2 EÚLP, který umožňuje, zasáhnout do práva na respektování soukromého života v zájmu ochrany práv a svobod jiných, národní a veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti či ochrany zdraví a morálky. Máme tudíž vymezena základní práva (právo na soukromý a na informační sebeurčení) a veřejný zájem (veřejná bezpečnost), které v testu proporcionality mezi sebou poměřujeme.

Prvním krokem testu proporcionality je **posouzení způsobilosti** naplnění účelu (nebo také vhodnosti). Zjišťujeme zda je biometrické rozpoznávání obličeje na veřejném prostranství schopno předcházet trestné činnosti a odvracet závažná ohrožení veřejné bezpečnosti a pořádku. V případě IS DPO, který představuje nástroj zpětné biometrické

79 ÚS: nález pléna ÚS ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11, bod 40.
80 ESLP: rozsudek ESLP ze dne 4. července 2023, *Glukhin proti Rusku*, č. 11519/20, bod 82.
81 ÚS: nález pléna ÚS ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11.

identifikace obličeje, je odpověď poměrně snadná. Podle mého názoru je nástroj vhodný cíle dosáhnout. Pokud PČR potřebuje k vyřešení některého úkolu identifikovat osobu na fotografii, je nástroj v současné podobě skutečně efektivní. Podle sdělení PČR je úspěšnost vyhledání identity osoby na fotografii 40 – 45 % a to v závislosti na kvalitě vstupní fotografie.[82]

V případě kamerového systému s biometrickou identifikací obličeje v reálném čase na LVHP si myslím, že je situace odlišná. V první řadě je potřeba si uvědomit, že stálé kamerové systémy mají podle kriminologických studií vliv na četnost a strukturu kriminality.[83] Také počet záchytů hledaných osob na LVHP (tabulka 3 v kapitole 7.1) vykazuje v průběhu let sestupný trend, ač může hrát roli také snížení počtu obsloužených pasažérů v období lockdownu. Navíc data nevypovídají o skutečném statusu zachycených hledaných osob a nelze poznat kolik těchto zachycených osob představovalo závažnější riziko, kterým se nejčastěji argumentuje v souvislosti s tímto systémem. Vzhledem k propojení s informačním systémem PATROS bude složení zachycených osob odrážet nejčastější trestnou činnost (krádeže, neplacení výživného a maření výkonu rozhodnutí).

Riziko jedné z nejzávažnějších hrozeb, kterou je teroristický útok, lze systémem biometrické identifikace odvrátit jen za velmi specifických podmínek. Identita pachatelů, respektive jejich podoba, by musela být známá dopředu. Podle některých autorů zabývajících se bezpečností a kriminologií nebyli dokonce nikdy odhaleni skuteční teroristé díky kamerovým systémům.[84] Navíc autoři dále argumentují, že zavedení různých bezpečnostních opatření nevede k podstatnému snížení teroristických trestných činů, ale spíše k posunům v typech teroristických útoků, protože teroristické aktivity jsou oproti jiným druhům trestné činnosti do značné míry plánované. Domnívám se, že biometrická identifikace obličeje v reálném čase na LVHP může být vhodná pro vyhledání pachatelů běžných trestných činů, ale nevhodná pro zachycení pachatelů organizované a plánovité trestné činnosti.

Druhým krokem testu proporcionality je **posouzení potřebnosti**, v němž je zkoumáno, zda byl při výběru prostředků použit ten prostředek, který je k základnímu právu nejšetrnější.

82 PČR. *Vyjádření k provozování informačního systému Digitálních podob osob* [online]. policie.cz, 20. července 2023 [cit. 10. března 2024].

83 GILL, Martin, SPRIGGS, Angela. *Vyhodnocení účinku kamerových systémů.* Praha: Institut pro kriminologii a sociální prevenci, 2007, s. 109.

84 STUTZER, Alois, ZEHNDER, Michael. Is camera surveillance an effective measure of counterterrorism? *Defence and Peace Economics*, 2013, roč. 24, č. 1, s. 1-14.

V tomto kroku je třeba zkoumat, zda ve vztahu k účelu zásahu nelze užít jiného srovnatelného prostředku, jímž by docházelo k menšímu zásahu do práv dotčených subjektů údajů. Opět v případě IS DPO je odpověď poměrně snadná. Neexistuje šetrnější objektivně srovnatelná metoda nebo nástroj odhalení totožnosti zájmové osoby zachycené na fotografii. Možnost tipování možných konkrétních osob a následné pohledové srovnání jejich fotografie z centrálních registrů s fotografií neznámé osoby není ve většině případů reálné. Nástroj se tak jeví jako nejvhodnější metodou k identifikaci neznámé osoby na fotografii. Možnou alternativou, namísto srovnávací databáze fotografií z civilních registrů obyvatel, by mohlo být použití databáze fotografií obviněných nebo odsouzených pachatelů trestných činů. Taková databáze by mola fungovat za obdobných podmínek jako databáze profilů DNA nebo otisků prstů. To by ovšem databázi čítající několik milionů osob zredukovalo na databázi čítající řádově desítky tisíc osob. Nelze tudíž očekávat, že by takový nástroj byl pro stanovený účel srovnatelně účinný.

Ani v případě kamerového systému s biometrickou identifikací obličeje v reálném čase na LVHP si nelze představit mírnější nebo šetrnější prostředek, který by odhalil pachatele běžné trestné činnosti, kteří vstupují do před-tranzitního prostoru LVHP. Zavedení kontrol totožnosti policistou všech vstupujících osob by jistě dopadlo do základních práv více než současná jen stěží zaznamenatelná kontrola kamerovým systémem. Navíc by takový režim měl ještě větší dopad na to, že by na letiště hledané osoby vůbec nevstupovali. Domnívám se tudíž, že se za daných okolností jedná o nejšetrnější prostředek k vyhledání pachatelů běžné trestné činnosti, kteří vstoupí do veřejného prostoru LVHP.

Posledním třetím krokem testu je **proporcionalita v užším smyslu**, což znamená zjistit, zda společenský prospěch dosažený realizací určitého zásahu bude větší než újma způsobená na základních právech. V tomto kroku klademe na obě strany argumenty a hodnotíme, zda převáží zájem na ochraně veřejné bezpečnosti nebo na straně ochrany práva na soukromí a na informační sebeurčení. Nicméně je zde třeba zvážit také zásah do dalších práv, ke kterému dochází prostřednictvím zásahu do práva na informační sebeurčení, což vyjádřil ÚS v plenárním nálezu Data retention I: „*Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné*

moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.[85] Očekávání obyvatel, že nejsou na veřejném prostranství v anonymitě má za následek také přímý negativní dopad na výkon svobody projevu, shromažďování a sdružování.

Argumentem v neprospěch využívání biometrických databází obličejů nebo biometrické identifikace obličejů v reálném čase je možnost zneužití těchto technologií, ke kterým v budoucnu jistě dojde. V případě zneužití biometrických osobních údajů osobami pověřenými obsluhou biometrických systémů může dojít k protiprávní činnosti.[86] Trestný čin neoprávněné nakládání s osobními údaji (podle § 180 trestního zákoníku) lze navíc spáchat i nedbalostním jednáním. Samotná existence biometrických dohledových systémů tudíž také představují riziko pro veřejnou bezpečnost.

K IS DPO osob sloužící ke zpětné biometrické identifikaci obličeje konstatuji, že v současné podobě nemůže ve třetím kroku testu proporcionality uspět. Důvodem je především skutečnost, že jsou v této biometrické databázi prakticky všichni obyvatelé ČR. Podle mého názoru IS DPO v daném provedení zahrnuje zpracování biometrických údajů nepřiměřeného počtu subjektů údajů a potenciálně tak zasahuje do práva na soukromí nerozlišujícím způsobem. Vedení databáze fotografií z civilních registrů, které jsou následně určeny pro biometrickou identifikaci obličeje je navíc v rozporu s tím, jak by měla být vykládána judikatura ESLP.

Ve věci Gaughran proti Spojenému království[87] rozhodoval ESLP o neomezeném uchování fotografie stěžovatele odsouzeného za řízení s nadměrným množstvím alkoholu. Stěžovatelova fotografie byla pořízena při jeho zatčení a měla být uchována po neomezenou dobu v policejní databázi. Podle ESLP rychlý vývoj stále důmyslnějších technik, které mimo jiné umožňují použití biometrické identifikace obličeje na fotografie jednotlivců, činí pořizování fotografií a jejich uchovávání a případné šíření výsledných dat problematické. ESLP proto shledal, že uchování stěžovatelovy fotografie v databázi na neomezenou dobu představovalo porušení práva na soukromý život.

85 ÚS: nález pléna ÚS ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 30.
86 DOMINGO JARAMILLO, Cristina. Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital*, 2021, roč. 9, č. 1, s. 20-37.
87 ESLP: rozsudek ESLP ze dne 13. února 2020, *Gaughran proti Spojenému království*, č. 45245/15.

Domnívám se, že za využití logického argumentu *a minori ad maius*, tedy pokud je určitý právní následek přiřazen k méně závažnému zásahu do základního práva, pak musí tím spíše platit pro závažnější zásah. Pokud je porušením práva na soukromý život neomezené uchovávání fotografie odsouzené osoby v policejní databázi, tím spíše bude stejným porušením také neomezené uchovávání fotografií bezúhonných osob z civilních registrů. Na základě uvedené argumentace se domnívám, že vedení IS DPO způsobem, kdy jsou do něj vkládány fotografie všech osob vedených v civilních registrech, je neslučitelná s právem na soukromý život.

Ke kamerovému systému s biometrickým rozpoznáváním obličeje v reálném čase na LVHP konstatuji, že rovněž nemůže ve třetím kroku testu proporcionality uspět. Uvedený kamerový systém slouží především k vyhledávání osob, které se dopustily běžné kriminality a využívá k tomu metody nepřetržitého necíleného sledování způsobem, který zpracovává citlivé osobní údaje nejen pasažérů letecké přepravy, ale také osob, které vstupují do veřejného prostoru letiště. Osobní údaje musí být zpracovávány pro dosažení závažného cíle nikoliv proto, že by mohly příslušnému orgánu potenciálně přijít vhod a ulehčit práci s hledáním osob v pátrání. Referenčním bodem by měl být jednotlivec a jeho přirozená základní práva, nikoliv potřeba orgánů veřejné moci užívat plošné biometrické sledování na veřejném prostranství k vyhledání pachatelů běžné trestné činnosti. Nasazení biometrické identifikace obličeje v reálném čase neobstojí, protože bezpečnostní výhody nepřeváží závažné zásahy do základních práv. Ačkoli biometrická identifikace obličeje v reálném čase přichází s příslibem zajištění větší bezpečnosti, spíše nás přibližuje orwellovskému scénáři společnosti založené na všudypřítomné kontrole.

10. Shrnutí přípravy nové legislativy EU

Systémy biometrické identifikace obličeje jsou rychle se rozvíjející technologií, jejíž regulace je v EU nevyhnutelná. Z připravované legislativy se problematiky dotýkají dvě nařízení. První z nich je připravované nařízení o umělé inteligenci (známé jako „Akt o umělé inteligenci“) a dále nařízení o automatizované výměně údajů pro policejní spolupráci (známé jako „Prüm II“).

Na biometrické rozpoznávání obličeje na veřejném prostranství bude mít nařízení o umělé inteligenci zásadní dopad. Již v únoru 2020 vydala Evropská komise Bílou knihu o umělé inteligenci, která nastínila směřování regulace pro širokou škálu aplikací umělé inteligence včetně biometrické identifikace na veřejných prostranstvích.[88] V dubnu 2021 Evropská komise zveřejnila samotný **návrh Nařízení o umělé inteligenci**.[89] Jeho cílem je harmonizovat pravidla týkající se systémů založených na umělé inteligenci a dále doplnit pravidla a povinnosti stanovené v GDPR a SOÚPP. V červnu 2023 přijal Evropský parlament k návrhu velké množství významných zpřísňujících pozměňovacích návrhů, ovšem základní architektura návrhu zůstala zachována. Kategorický postoj Evropského parlamentu předznamenalo již jeho usnesení o umělé inteligenci v trestním právu z října 2021, ve kterém apeloval na členské státy k zavedení moratoria na systémy biometrické identifikace obličeje.[90] V prosinci 2023 však v rámci trialogu – diskuse mezi poslanci Evropského parlamentu, Komise a členských států – došlo k výrazným ústupkům v regulaci zejména právě biometrické identifikace na veřejných prostranstvích. Protože finální znění nařízení o umělé inteligenci není (ke dni 11. března 2024) schváleno, může ještě dojít ke změnám. V textu této práce pracuji s finální podobou návrhu nařízení o umělé inteligenci, o kterém by měl během března 2024 hlasovat Evropský parlament.

88 Bílá kniha Evropské komise ze dne 19. února 2020, o umělé inteligenci – evropský přístup k excelenci a důvěře.

89 Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie.

90 Usnesení Evropského parlamentu ze dne 6. října 2021, o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech, bod 27.

Návrh nařízení o umělé inteligenci je založen na široké definici pojmu *systém umělé inteligence*, aby pokrýval co největší okruh možných případů. Systémy umělé inteligence se dle návrhu mají členit do čtyř kategorií na základě posouzení rizik. Těmito kategoriemi jsou systémy umělé inteligence, které vytvářejí: 1) nepřijatelné riziko, 2) vysoké riziko, 3) omezené riziko a 4) nízké nebo minimální riziko.

Systémy umělé inteligence s nepřijatelným rizikem budou zakázané, a to z důvodu jejich rozporu s hodnotami EU. Nařízením by mělo být zakázáno používat systémy, které zjevně ohrožují život, zdraví, bezpečnost nebo práva jednotlivců. Podle čl. 5 návrhu nařízení o umělé inteligenci bude zakázána celá řada praktik z nichž následující praktiky se týkají biometrického rozpoznávání pro účely prosazování práva:

1) používání biometrické identifikace na dálku v reálném čase na veřejně přístupných místech;

2) uvádění do provozu nebo používání systémů, které vytvářejí nebo rozšiřují databáze rozpoznávání obličejů prostřednictvím necíleného vytěžování obrázků z internetu nebo kamerových záznamů.

Ze zákazu biometrické identifikace na dálku v reálném čase by měly platit tři výjimky: vyhledávání pachatelů a podezřelých z trestných činů, hledání potenciálních obětí trestných činů a naposledy také případy konkrétních ohrožení života fyzických osob včetně hrozeb teroristických útoků. Každé použití systému biometrické identifikace na dálku v reálném čase by mělo podléhat konkrétnímu povolení justičního orgánu nebo nezávislého správního orgánu členského státu.

Systémy umělé inteligence s vysokým rizikem budou systémy, které představují vysoké riziko pro zdraví a bezpečnost nebo pro základní práva. Při využívání systémů umělé inteligence vykazujících vysoká rizika mají být kladeny přísnější požadavky. Mezi tyto požadavky budou patřit zejména: management řízení rizik, na jehož základě budou přijímána potřebná opatření; vypracování technické dokumentace a její aktualizace; transparentnost používaného systému umělé inteligence; a potřeba lidského dohledu zaměřeného na prevenci nebo minimalizaci rizik. Mezi další povinnost pro provoz systémů umělé inteligence, které vykazují vysoké riziko, by měla být povinná registrace před uvedením do provozu ve veřejně přístupné databázi spravované Evropskou komisí.

Vysoce rizikové systémy umělé inteligence podle čl. 6 odst. 2 a přílohy III návrhu nařízení jsou systémy umělé inteligence uvedené v některé z následujících oblastí biometrie:

1) systémy biometrické identifikace na dálku;

2) systémy umělé inteligence určené k použití pro biometrickou kategorizaci podle citlivých nebo chráněných atributů nebo charakteristik;

3) systémy umělé inteligence určené pro rozpoznávání emocí.

První z uvedených praktik nasazená na veřejně přístupných místech za účelem prosazování práva se bude týkat zpětné biometrické identifikace na dálku, protože biometrická identifikace na dálku v reálném čase patří mezi systémy umělé inteligence s nepřijatelným rizikem.

Systémy umělé inteligence s omezeným rizikem by měly splňovat minimální požadavky na transparentnost. Zbytková kategorie **systémů umělé inteligence s nízkým nebo minimálním rizikem** by neměla být limitována žádnými specifickými požadavky. Poslední dvě kategorie jsou bez zásadních požadavků a z biometrických systémů sem spadá biometrická autentizace.

Nařízením o umělé inteligenci nebudou dotčeny pravidla stanovená v SOÚPP. Stejně tak nařízení o umělé inteligenci neposkytuje právní základ zpracování osobních údajů podle čl. 8 a čl. 10 SOÚPP. Znamená to, že všechny dosavadní požadavky na biometrickou identifikaci obličeje na veřejných prostranství za účelem prosazování práva zůstávají zachovány a budou doplněny souborem nových pravidel. Nová harmonizovaná pravidla budou mít dopad na dnes nasazené systémy biometrické identifikace provozované PČR. Kamerový systém s biometrickou identifikací obličeje v reálném čase na LVHP, jakožto systém biometrické identifikace na dálku v reálném čase, by spadal do kategorie systémů umělé inteligence s nepřijatelným rizikem. IS DPO, jakožto systém zpětné biometrické identifikace na dálku, bude spadat do kategorie systémů umělé inteligence s vysokým rizikem. Do budoucna zůstane provoz obou systémů zřejmě zachován, přičemž systém biometrické identifikace obličeje v reálném čase na LVHP bude vyžadovat přijetí doprovodné legislativy. V současné době již Ministerstvo vnitra předložilo do meziresortního

připomínkového řízení novelu, která s předstihem upravuje v ZZOÚ podmínky využívání biometrických systémů k identifikaci obličeje v reálném čase.

Další nástroj evropského práva, který zasahuje právní úpravu biometrické identifikace obličeje je tzv. **prümský systém**. Za účelem řešení mezinárodní kriminality byla dne 27. května 2005 v německém městě Prüm dojednána Prümská úmluva.[91] Prvních sedm států na základě této mezivládní úmluvy začalo sdílet otisky prstů, profily DNA a registrační značky vozidel. Donucovací orgány států, které jsou strany úmluvy, získaly možnost porovnat otisky prstů a profily DNA v databázích ostatních států úmluvy. Základní prvky Prümské úmluvy byly v roce 2008 převzaty Prümským rozhodnutím,[92] které umožnilo sdílení údajů mezi všemi členskými státy EU. Kromě členských států EU se prümského systému účastní nebo na něm přislíbilo účast Norsko, Island, Velká Británie, Švýcarsko a Lichtenštejnsko.

V současnosti probíhá „modernizace“ prümského systému. Tato iniciativa předpokládá rozšíření rozsahu sdílených údajů o biometrii obličeje a také vytvoření nové architektury, která umožní rychlejší výměnu údajů mezi členskými státy. V souvislosti s tím předložila Evropská komise dne 8. prosince 2021 návrh nařízení o automatizované výměně údajů pro policejní spolupráci.[93] Návrh předpokládá automatizovanou výměnu obrázků obličeje vedených v databázích donucovacích orgánů členských států. Návrh dále předpokládá vytvoření centrálního směrovače, který by fungoval jako spojovací body mezi členskými státy. Jedná se o hybridní přístup mezi decentralizovaným a centralizovaným řešením, ovšem bez nutnosti ukládání dat na centrální úrovni. Znamená to, že se všechny vnitrostátní databáze v každém členském státě budou připojovat k centrálnímu směrovači, místo aby se připojovaly jedna k druhé. Popsaná struktura by měla zjednodušit a zásadně zkrátit proces předávání údajů mezi donucovacími orgány.

91 Úmluva mezi Belgickým královstvím, Spolkovou republikou Německo, Španělským královstvím, Francouzskou republikou, Lucemburským velkovévodstvím, Nizozemským královstvím a Rakouskou republikou o posílení přeshraniční spolupráce, zejména v boj proti terorismu, přeshraniční trestné činnosti a nelegální migraci.

92 Rozhodnutí Rady EU 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti a rozhodnutí Rady 2008/616/SVV o provádění rozhodnutí 2008/615/SVV.

93 Návrh Nařízení Evropského parlamentu a Rady, o automatizované výměně údajů pro policejní spolupráci („Prüm II“), kterým se mění rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nařízení Evropského parlamentu a Rady (EU) 2018/1726, 2019/817 a 2019/818.

Zpětná biometrická identifikace obličeje na dálku byla k prosinci 2020 implementována v jedenácti členských státech EU, ve Spojeném království, dále také Europolem a Interpolem. V sedmi členský státech EU včetně ČR dosáhla příprava na nasazení zpětné biometrické identifikace na dálku fáze, že bylo očekáváno spuštění během jednoho až dvou let. Přitom vzhledem k uvedeným poznatkům bylo v ČR nasazeno v roce 2022 jako IS DPO. Devět zástupců členských států uvádělo, že zatím nemají konkrétní plány na zavedení biometrické identifikace obličeje.[94]

Zásadní kvalitativní změnou v prümském systému je právě rozšíření o vyobrazení obličeje a možnost spouštět proti nim algoritmy pro rozpoznávání obličejů. Fotografie obličeje v databázích mohou zahrnovat podezřelé, obviněné, odsouzené, žadatele o azyl a neidentifikovaná mrtvá těla. Nicméně některé členské státy, včetně ČR, mají dnes vytvořeny databáze zobrazení obličejů na základě civilních registrů.

PČR již provedla technické kroky k tomu, aby přizpůsobila svou infrastrukturu na budoucí prümský systém a současně integrovala dílčí biometrické databáze. Tímto krokem je budování **Centrálního biometrického informačního systému**. Jedná se o komplexní informační systém, který by měl integrovat různé způsoby biometrické identifikace. Centrální biometrický informační systém by měl nahradit stávající policejní databázi otisků prstů (AFIS). Bude navíc pracovat s identitami, které jsou vedeny v policejní databázi profilů DNA (FODAGEN) a informačním systému Cizinci s povoleným pobytem. Centrální biometrický informační systém bude sloužit k výměně dat dle mezinárodních smluv a nařízení EU, bude tudíž vybaven rozhraními se systémy Prüm, Eurodac, a dalšími.[95]

94 TELEFI Project. Towards the European Level Exchange of Facial Images Version 1.0. Závěrečná zpráva projektu TELEFI, 2021, 173 s.

95 Ministerstvo vnitra. Rámcová dohoda na dodání, technickou podporu, rozvoj a předání systému cBIS, č.j. PPR-3045-34/ČJ-2022-990656.

11. Závěr

Diplomová práce se věnuje aktuálnímu tématu, kterým jsou kamerové systémy s technologií biometrické identifikace obličeje na veřejných prostranstvích. První část práce je svou podstatou spíše teoretická. Na úplném začátku v druhé kapitole je představena základní terminologie postihující současné technické prostředky biometrického rozpoznávání a umělé inteligence. Představuji v ní zásadní pojmy, jako je biometrická identifikace obličeje „v reálném čase“ a „zpětná“. Terminologie vychází z účinného, ale především z teprve připravovaného práva evropské unie. Ve třetí kapitole je problematika zasazena do společenského kontextu, přičemž jsou představeny koncepty, jako jsou plošné sledování, diskriminační algoritmy, funkční rozlézání a dystopický scénář vývoje společnosti. Dodává to řešené problematice společenskou naléhavost, kterou si jistě zaslouží.

Následuje přehled právních úprav různé úrovně, které na problematiku biometrické identifikace obličeje dopadají. První z nich je systém ochrany základních práv s celou řadou instrumentů na mezinárodní, evropské a vnitrostátní úrovni. Jako zásadní základní práva v souvislosti s biometrickou identifikací obličeje jsou identifikována právo na soukromí a právo na informační sebeurčení. Následuje právní úprava Evropské unie, kde jsou představeny právní instrumenty věnující se ochraně osobních údajů. Na problematiku ochrany osobních údajů za účelem prosazování práva – tudíž také na biometrickou identifikaci obličeje donucovacími orgány – dopadá Směrnice o ochraně údajů při prosazování práva, což je řešeno také výlukou z věcné působnosti Obecného nařízení o ochraně osobních údajů. Nakonec z české právní úpravy jsou představeny zákon o zpracování osobních údajů, který implementuje většinu ustanovení směrnice, a dále zákon o Policii České republiky, který obsahuje zmocnění pro zpracování osobních údajů pro policii. Do teoretické části práce lze zařadit také desátou kapitolu týkající se připravované evropské právní úpravy biometrické identifikace obličeje, která je ovšem zařazena až na konec práce. V této kapitole jsou představeny návrhy dvou nařízení: Akt o umělé inteligenci a nařízení o automatizované výměně údajů pro policejní spolupráci (Prüm II).

Za praktickou část práce lze označit tři kapitoly (7, 8 a 9), které popisují systémy biometrického rozpoznávání obličeje používané Policií České republiky, které konfrontují s účinnou právní úpravou, a které podrobují testu proporcionality z důvodu jejich zásahu do základních práv. Na základě této praktické části lze také zodpovědět dvě výzkumné otázky, které jsem si vytyčil v úvodu práce:

- Jsou systémy biometrické identifikace obličeje na veřejném prostranství nasazené za účelem prosazování práva v souladu s účinnou právní úpravou?
- Jsou systémy biometrické identifikace obličeje na veřejném prostranství nasazené za účelem prosazování práva proporcionální vzhledem k zásahům do základních práv?

Z aplikační praxe Policie České republiky představuji tři systémy biometrické identifikace obličeje na veřejných prostranstvích. Dva z nich představují systémy používané v současnosti. Prvním z nich je kamerový systém s biometrickou identifikací obličeje v reálném čase nasazený na Letišti Václava Havla v Praze a druhý je celostátně využívaný nástroj ke zpětné biometrické identifikaci obličeje – informační systém Digitální podoba osob, který využívá digitální fotografie z civilních registrů. Třetím systémem biometrické identifikace obličeje je softwarový nástroj EyeDentity, který byl v minulosti využíván Krajským ředitelstvím policie Ústeckého kraje.

Na základě mé právní analýzy na první výzkumnou otázku odpovídám tak, že žádný ze třech nasazených systémů biometrické identifikace obličeje není, či nebyl, v souladu s účinnou právní úpravou. Zaprvé všechny tři systémy trpí nedostatečným zákonným zmocněním, což je požadavek stanovený ve Směrnici o ochraně údajů při prosazování práva. Dalším zásadním nedostatkem je fakt, že pro systémy nebylo před jejich spuštěním zpracováno obligatorní posouzení vlivu na ochranu osobních údajů, kdy by se mohlo v případě všech tří systémů jednat o přestupky dle zákona o zpracování osobních údajů, přičemž skutkový stav u každého ze systémů je trochu odlišný. Navíc v případě softwaru EyeDentity připadá v úvahu několik dalších přestupků dle zákona o zpracování osobních údajů.

Na základě provedeného testu proporcionality na druhou výzkumnou otázku odpovídám tak, že kamerový systém s biometrickou identifikací obličeje na Letišti Václava Havla v Praze, tak informační systém Digitální podoba osob v současné podobě nesplňují požadavky

na proporcionality zásahu do základních práv. V testu proporcionality jsem poměřil právo na soukromí a na informační sebeurčení se zájmem na veřejné bezpečnosti. Prvním problémem je skutečnost, že zásah do základních práv není dostatečně upraven v účinném právu, takže zásah není předvídatelný. Ačkoliv oba systém mohou projít prvními dvěma kroky testu – způsobilost a potřebnost, nemohou dle mého názoru projít krokem třetím – proporcionalitou v užším smyslu. Zásadní problém vidím v tom, že oba systémy využívají citlivé osobní údaje nerozlišujícím a necíleným způsobem, takže zájem na ochraně veřejné bezpečnosti v daném případě nemůže převážit nad ochranou práva na soukromí a na informační sebeurčení. V případě informačního systému Digitální podoba osob doporučuji upravit systém tak, že by namísto fotografií z civilních registrů zahrnoval jen fotografie odsouzených a obviněných osob. V takovém případě by mohlo být dosaženo ochrany základních práv. Kamerový systém s biometrickou identifikací obličeje v reálném čase na veřejných prostranstvích nelze dle mého názoru uzpůsobit souladně s dostatečnou ochranou základních práv.

12. Bibliografie

12.1 Monografie a komentáře

BAČA, Ján a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Plzeň: Aleš Čeněk, 2020, 361 s.

BARTOŇ, Michal a kol. *Základní práva*. Praha: Leges, 2016, 608 s.

DIXON, Pam, GELLMAN, Robert. *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*. World Privacy Forum, 2014, 90 s.

GILL, Martin, SPRIGGS, Angela. *Vyhodnocení účinku kamerových systémů.* Praha: Institut pro kriminologii a sociální prevenci, 2007, 142 s.

GROTHER, Patric a kol. *Face Recognition Vendor Test. Part 3: Demographic Effects*. National Institute of Standards and Technology. U.S. Department of Commerce, 2019. 82 s.

MAREŠ, Miroslav a kol. *Kamerový systém Dopravního podniku hlavního města Prahy v komparativním kontextu bezpečnosti a ochrany osobních údajů.* Praha: Dopravní podnik Hlavního města, 2021, 139 s.

NULÍČEK, Michal a kol. *Zákon o zpracování osobních údajů. Praktický komentář*. Praha: Wolters Kluwer, 2019, 212 s.

PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář.* 2. aktualizované vydání. Praha: Leges, 2019, 752 s.

TOMÁŠEK, Michal a kol. *Právo Evropské unie*. 3. aktualizované vydání. Praha: Leges, 2021, 512 s.

VLACHOVÁ, Barbora, MAISNER, Martin. *Zákon o zpracování osobních údajů. Komentář.* Praha: C. H. Beck, 2019, 163 s.

12.2 Odborné články

BARAK, Aharon. Human Dignity. The Constitutional Value and the Constitutional Right. *Human Rights Law Review*, 2016, roč. 16, č. 1, s 175 – 176.

DOMINGO JARAMILLO, Cristina. Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital*, 2021, roč. 9, č. 1, s. 20-37.

EL KHIYARI, Hachim, WECHSLER, Harry. Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning. *Journal of Biometrics & Biostatistics*, 2016, roč. 7, č. 4.

KLARE, Brendan a kol. Role of Demographic Information. *IEEE Transactions on Information Forensics and Security*, 2012, roč. 7, č. 6, s. 1789-1801.

MATEJKA, Ján a kol. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*, 2018, roč. 9, č. 17, s. 91-129.

STUTZER, Alois, ZEHNDER, Michael. Is camera surveillance an effective measure of counterterrorism? *Defence and Peace Economics*, 2013, roč. 24, č. 1, s. 1-14.

12.3 Právní předpisy

- mezinárodní dokument: Všeobecná deklarace o lidských práv Organizace spojených národů.

- mezinárodní smlouva: Evropská úmluva o ochraně lidských práv. Publikována jako sdělení č.209/1992 Sb.

- mezinárodní smlouva: Mezinárodní pakt o občanských a politických právech. Publikována jako vyhláška ministra zahraničních věcí č. 120/1976 Sb.

- mezinárodní smlouva: Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Publikována jako sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s.

- mezinárodní smlouva: Smlouva o fungování Evropské unie. 2012/C 326/01.

- mezinárodní smlouva: Listina základních práv Evropské unie 2012/C 326/02.

- mezinárodní smlouva: Úmluva mezi Belgickým královstvím, Spolkovou republikou Německo, Španělským královstvím, Francouzskou republikou, Lucemburským velkovévodstvím, Nizozemským královstvím a Rakouskou republikou o posílení přeshraniční spolupráce, zejména v boj proti terorismu, přeshraniční trestné činnosti a nelegální migraci.

- legislativa ES/EU: Nařízení Evropského parlamentu a Rady (EU) 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).

- legislativa ES/EU: 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.

- legislativa ES/EU: Rozhodnutí Rady EU 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti a rozhodnutí Rady 2008/616/SVV o provádění rozhodnutí 2008/615/SVV.

- legislativa ES/EU: Bílá kniha Evropské komise ze dne 19. února 2020, o umělé inteligenci – evropský přístup k excelenci a důvěře.

- legislativa ES/EU: Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie.

- legislativa ES/EU: Návrh Nařízení Evropského parlamentu a Rady, o automatizované výměně údajů pro policejní spolupráci („Prüm II“), kterým se mění rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nařízení Evropského parlamentu a Rady (EU) 2018/1726, 2019/817 a 2019/818.

- legislativa ES/EU: Usnesení Evropského parlamentu ze dne 6. října 2021, o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech.

- legislativa ES/EU: Stanovisko k vývoji biometrických technologií Pracovní skupiny zřízení podle článku 29 č. 3/2012 ze dne 27. dubna 2012.

- aktuální znění: Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

- aktuální znění: Ústavní zákon č. 1/1993 Sb., Ústava ČR, ve znění pozdějších předpisů.

- aktuální znění: Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

- aktuální znění: Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

- aktuální znění: Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

- aktuální znění: Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

- aktuální znění: Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

- důvodové zprávy: Důvodová zpráva k zákonu č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

- vnitřní podzákonný předpis: Rozkaz policejního prezidenta č. 123/2018 ze dne 14. června 2018, kterým se upravuje zkušební provoz integrovaného bezpečnostního systému LETIŠTĚ.

- vnitřní podzákonný předpis: Rozkaz policejního prezidenta č. 194/2022 ze dne 19. srpna 2022, k zajištění zkušebního provozu informačního systému Digitální podoba osob.

12.4 Judikatura

ESLP: rozsudek velkého senátu ESLP ze dne 16. února 2000, *Amann proti Švýcarsku*, č. 27798/95.

ESLP: rozsudek velkého senátu ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04.

ESLP: rozsudek velkého senátu ESLP ze dne 15. října 2015, *Kudrevičius proti Litvě*, č. 37553/05.

ESLP: rozsudek ESLP ze dne 28. dubna 2003, *Peck proti Spojenému království*, č. 44647/98.

ESLP: rozsudek ESLP ze dne 13. února 2020, *Gaughran proti Spojenému království*, č. 45245/15.

ESLP: rozsudek ESLP ze dne 4. července 2023, *Glukhin proti Rusku*, č. 11519/20.

SDEU: rozsudek velkého senátu SDEU ze dne 8. dubna 2014, *Digital Rights Ireland a Seitlinger a další*, C-293/12 a C-594/12.

SDEU: rozsudek velkého senátu SDEU ze dne 6. října 2015, *Schrems*, C-362/14.

Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 26. února 1984, *Marshall proti Southampton and South-West Hampshire Area Health Authority*, 152/84.

Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 4. prosince 1974, *Van Duyn proti Home Office*, 41/74.

Evropský soudní dvůr: rozsudek Evropského soudního dvora ze dne 10. dubna 1984, *Von Colson a Kamann*, C-14/83.

ÚS: nález pléna ÚS ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94.

ÚS: nález pléna ÚS ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

ÚS: nález pléna ÚS ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11.

ÚS: nález ÚS ze dne 10. října 2021, sp. zn. II. ÚS 1022/21.

NSS: usnesení NSS o předložení předběžné otázky ze dne 26. ledna 2023, č.j. As 172/2022-56.

Německý ústavní soud: Nález německého ústavního soudu ze dne 15. prosince 1983, 1 BvR 209/83.

12.5 Získané dokumenty

Informace poskytnutá dle InfZ ze dne 18. srpna 2020 vydaná Magistrátem hlavního města Praha, č.j. MHMP 1270148/2020.

Informace poskytnutá dle InfZ ze dne 24. srpna 2020 vydaná Policejním prezidiem, č.j. PPR-24979-5/ČJ-2020-990810.

Informace poskytnutá dle InfZ ze dne 16. srpna 2023 vydaná Policejním prezidiem, č.j. PPR-35618-5/ČJ-2023-990810.

Informace poskytnutá dle InfZ ze dne 11. září 2023 vydaná KŘP ÚK, č.j. KRPU-160885-2/ČJ-2023-0400KR-PI.

Informace poskytnutá dle InfZ ze dne 14. září 2023 vydaná KŘP ÚK, č.j. KRPU-166623-2/ČJ-2023-0400KR-PI.

Informace poskytnutá dle InfZ ze dne 12. února 2024 vydaná Ředitelstvím služby cizinecké policie, č.j. PPR-6809-3/ČJ-2024-990810.

Rozhodnutí o částečném odmítnutí žádosti podle InfZ Policejního prezidia ze dne 20. srpna 2020, č.j. PPR-24979-6/ČJ-2020-990810.

Rozhodnutí o odmítnutí žádosti podle InfZ Policejního prezidia ze dne 6. března 2023, č.j. PPR-11093-5/ČJ-2023-9908100.

KŘP ÚK. Licenční smlouvy ze dne 20. listopadu 2018 a dne 19. listopadu 2019. Poskytnutí licence pro software EyeDentity, č.j. KRPU-209961-6/ČJ-2018-0400IT-02A a KRPU-167484-6/ČJ-2019-0400IT-03.

Ministerstvo vnitra. Kupní smlouva ze dne 22. prosince 2016. Vybudování mobilního biometrického inspekčního systému a dodávka kontrolních zařízení, č.j. PPR-22247-26/ČJ-2016-990656.

Ministerstvo vnitra. Smlouva o dílo ze dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV, č.j. PPR-27225-108/ČJ-2015-990656.

Ministerstvo vnitra. Rámcová dohoda na dodání, technickou podporu, rozvoj a předání systému cBIS, č.j. PPR-3045-34/ČJ-2022-990656.

TELEFI Project. Towards the European Level Exchange of Facial Images Version 1.0. Závěrečná zpráva projektu TELEFI, 2021, 173 s.

Vyjádření ÚOOÚ k žádosti o konzultaci k městskému kamerovému systému hl. m. Prahy ze dne 3. prosince 2019, č.j. UOOU-04829/19-2.

12.6 Internet

Agentura Evropské unie pro základní práva. *Facial recognition technology: fundamental rights considerations in the context of law enforcement* [online]. Vídeň: Agentura Evropské unie pro základní práva, 2020. Dostupné z: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

ALSHARIF, Mirna, SANTAN, Cristian. *Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology* [online]. nbcnews.com, 6. srpna 2023 [cit. 10. března 2024]. Dostupné z: https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447

BOTSMAN, Rachel. *Big data meets Big Brother as China moves to rate its citizens* [online]. Wired.co.uk, 21. října 2017 [cit. 10. března 2024]. Dostupné z: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Česká televize. *Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti* [online]. Česká televize, 20. listopadu 2019 [cit. 10. března 2024]. Dostupné z:

https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologii-na-rozpoznavani

Česká televize. *Události komentáře (čas 33:22)* [online]. Česká televize, 17. dubna 2023 [cit. 10. března 2024]. Dostupné z: https://www.ceskatelevize.cz/porady/1096898594-udalosti-komentare/223411000370417/

DOFFMAN, Zak. *New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report* [online]. Forbes, 14. srpna 2019 [cit. 10. března 2020]. 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 Digital Rights. *Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States* [online]. Brusel: European Digital Rights, 2020. Dostupné z: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Ministerstvo vnitra. *Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích* [online]. mvcr.cz, 18. února 2018 [cit. 10. března 2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx

Ministerstvo vnitra. *Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů* [online]. mvcr.cz, 4. března 2019 [cit. 10. března 2024]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx

PČR. *eGATE - rychlejší odbavování na letišti* [online]. policie.cz, 23. července 2015 [cit. 10. března 2024]. Dostupné z: https://www.policie.cz/clanek/egate-rychlejsi-odbavovani-na-letisti.aspx

PČR. *Vyjádření k provozování informačního systému Digitálních podob osob* [online]. policie.cz, 20. července 2023 [cit. 10. března 2024]. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx

ÚOOÚ. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2020. Dostupné z: https://uoou.gov.cz/media/profesional/seznam-operaci-zpracovani-nepodlehajicich-pozadavku-na-dpia.pdf

ÚOOÚ. *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech* [online]. uoou.gov.cz, 16. srpna 2019 [cit. 10. března 2024]. Dostupné z: https://uoou.gov.cz/cs/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech

ÚOOÚ. *Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech* [online]. uoou.gov.cz, 27. března 2020 [cit. 10. března 2024]. Dostupné z: https://uoou.gov.cz/cs/vyjadreni-uoou-k-navrhu-regulace-nasili-na-fotbalovych-stadionech

UNGERLEIDER, Neal. *The Dark Side Of Biometrics: 9 Million Israelis' Hacked Info Hits The Web* [online]. FastCompany.com, 24. října 2011 [cit. 10. března 2024]. Dostupné z: https://www.fastcompany.com/1790444/dark-side-biometrics-9-million-israelis-hacked-info-hits-web

VÁCLAVÍKOVÁ, Jana. *"Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře* [online]. Aktualne.cz, 11. července 2020 [cit. 10. března 2024]. Dostupné z: https://zpravy.aktualne.cz/zahranici/pocitac-se-spletl-policie-zatkla-spatneho-muze-kvuli-technol/r~b3cdeb14c1cb11ea8972ac1f6b220ee8/

Shrnutí

Kamerové systémy s biometrickým rozpoznáváním obličeje na veřejném prostranství

Práce věnující se tématu kamerových systémů s biometrickou identifikací obličeje na veřejných prostranstvích podává přehled právních předpisů různých úrovní, které se k problematice vztahují. Rozebírá ochranu základních práv, které mohou být biometrickými kamerovými systémy dotčeny, dále pak související účinnou a připravovanou právní úpravu Evropské unie, a také účinnou českou právní úpravu. Praktickým přínosem práce je vytvoření přehledu doposud známých systémů biometrické identifikace obličeje na veřejných prostranstvích provozovaných Policií České republiky. Podává tak informace o provozu kamerového systému na Letišti Václava Havla v Praze, kde je využívána biometrická identifikace obličeje v reálném čase, a o provozu informačního systému Digitální podoba osob a softwaru EyeDentity, které využívají zpětnou biometrickou identifikaci obličeje. Uvedené tři systémy jsou konfrontovány s účinnou právní úpravou, kterou jsou Směrnice o ochraně osobních údajů při prosazování práva a zákon o Policii České republiky. Dále je pro první dva systémy proveden test proporcionality v souvislosti se zásahem do základních práv. Hodnocen je střet práva na soukromí a práva na informační sebeurčení se zájmem na veřejné bezpečnosti. Právní analýza odpovídá na dvě položené výzkumné otázky vytyčené v úvodu práce, a to zda systémy biometrické identifikace obličeje na veřejném prostranství nasazené za účelem prosazování práva jsou v souladu s účinnou právní úpravou, a zda jsou proporcionální vzhledem k zásahům do základních práv.

Klíčová slova: biometrika, rozpoznání na základě obličeje, základní práva, umělá inteligence, ochrana osobních údajů

Abstract

Camera systems with biometric facial recognition in public spaces

The thesis devoted to the topic of camera systems with biometric facial identification in public spaces provides an overview of the legal regulations of different levels that relate to the issue. It discusses the protection of fundamental rights that may be affected by biometric camera systems, as well as the related effective and upcoming legislation of the European Union, as well as effective Czech legislation. The practical contribution of the thesis is the creation of an overview of the hitherto known systems of biometric facial identification in public spaces operated by the Police of the Czech Republic. It thus provides information on the operation of the camera system at Vaclav Havel Airport in Prague, where "real-time" biometric facial identification is used, and on the operation of the Digital Image of Persons information system and the EyeDentity software, which use "post" biometric facial identification. The three systems mentioned are confronted with effective legal regulation, which are the Law Enforcement Directive and the Law on the Police of the Czech Republic. Furthermore, a proportionality test is carried out for the first two systems in connection with interference with fundamental rights. The conflict between the right to privacy and the right to informational self-determination with the interest in public safety is assessed. The legal analysis answers the two research questions posed at the beginning of the thesis, namely whether biometric facial identification systems in public spaces deployed for the purpose of law enforcement are in accordance with effective legal regulation, and whether they are proportionate to interference with fundamental rights.

Key worlds: biometrics, facial recognition, fundamental rights, artificial intelligence, data protection