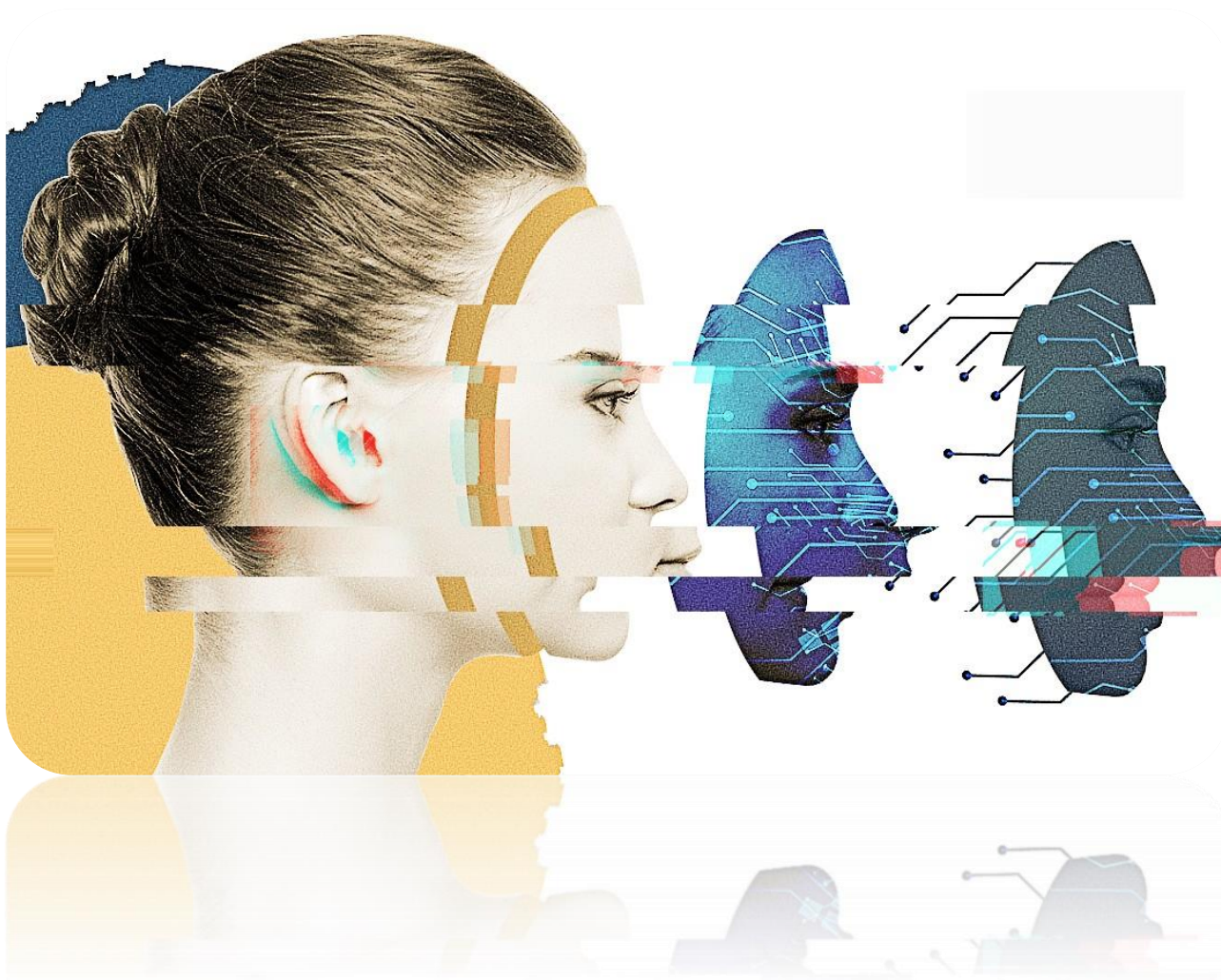


Český Minority Report: Využití umělé inteligence Policií České republiky



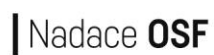
Iuridicum Remedium (IuRe), prosinec 2023

Mgr. et Mgr. Václav Mach, Ph.D.

www.iure.org / www.digitalnisvobody.cz



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



Obsah

1. Uvedení do problematiky	5
2. Směrem ke globální dystopii	8
2.1 Plošné sledování.....	8
2.2 Prohlubování nerovností.....	9
2.3 Akcelerace a rozlézáání sledování	10
2.4 Globální dystopie	12
3. Právní regulace	14
3.1 Ochrana základních práv	14
3.2 Právní úprava Evropské unie	20
3.2.1 Účinná právní úprava	20
3.2.2 Připravovaná právní úprava.....	23
3.3 Právní úprava v České republice.....	27
4. Současné aplikace	31
4.1 Biometrika obličeje	31
4.1.1 Kamerový systém na Letišti Václava Havla.....	34
4.1.2 Další navrhované systémy biometrické identifikace „v reálném čase“	39
4.1.3 Informační systém Digitální podoba osob.....	41
4.1.4 Další soukromé biometrické databáze	43
4.1.5 Zpětná biometrická identifikace softwarem EyeDentity	43
4.1.6 Biometrická autentizace	46
4.2 Analýza obrazu.....	47
4.3 Analýza audio	51
4.4 Analýza textu	53
4.5 Analýza zločinnosti	53
5. Výzkum a vývoj	57
6. Mezinárodní spolupráce.....	74
6.1 Sdílení biometrických dat v Evropské unii.....	74
6.2 Mezinárodní výzkum spojující soukromý a veřejný sektoru	78

7. Zdroje informací	81
7.1 Odborné	81
7.2 Zveřejněné dokumenty	82
7.3 Právní předpisy	85
7.4 Internet	86
7.5 Judikatura	88

1. Uvedení do problematiky

„Umělá inteligence je nebezpečnější než jaderné zbraně.“

Elon Musk, vlivný businessman a investor

Umělá inteligence se v posledním roce stala nejvíce diskutovanou technologií. Díky svému rychlému rozvoji nachází čím dál širší uplatnění při mnoha lidských činnostech. Výjimkou není ani využití umělé inteligence bezpečnostními složkami pro účely udržování veřejné bezpečnosti a vymáhání práva. Zapojení umělé inteligence do trestního řízení navíc požaduje také Nejvyšší státní zastupitelství.¹ Ovšem využití umělé inteligence při zpracování osobních údajů bezpečnostními službami může snadno sklouznout k programům plošného sledování, což představuje závažné riziko pro práva a svobody obyvatel a pro samotné demokratické směřování společnosti. Tato publikace si klade za cíl zmapovat současný stav využití umělé inteligence Policií České republiky, a to především aplikací s potenciálem zásahu do základních práv.

První problém by mohl nastat již při vymezení pojmu umělá inteligence. Význam termínu umělá inteligence není vždy jednoznačný a jeho zákonná definice zatím chybí. Především nelze hovořit jen o jediném systému umělé inteligence, ale jedná se o celou řadu různých postupů a technik a jejich vzájemných kombinací. 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. Pro účely této publikace jsou systémy umělé inteligence chápány jako informační postupy a techniky řešící komplexní úlohy, jako jsou rozpoznávání či klasifikace, zejména v oblastech zpracování obrazu, psaného textu

¹Nejvyšší státní zastupitelství. Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019. V Brně dne 29. ledna 2020, 3 SE 101/2020, str. 16.

či mluveného jazyka, nebo při plánování či řízení na základě zpracování velkých objemů dat. 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 informační operace.

Pozornost je v této publikaci kladena na systémy, které jsou používány k dohledu a plošnému sledování, a které tudíž mají potenciál zasáhnout do základních práv. Blíže je tudíž věnována pozornost systémům umělé inteligence, které nějakým způsobem využívají osobní údaje, nebo systémy, které provádějí profilování. Profilováním je chápána jakákoli forma automatizovaného hodnocení osobních aspektů osob týkajících se například ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. Zvláštní pozornost je pak kladena na systémy biometrického rozpoznávání dle obličeje, které představují novou rychle se šířící aplikaci umělé inteligence. Navíc právě biometrické rozpoznávání dle obličeje je předmětem bližšího zájmu také připravovaného nařízení s cílem regulovat umělou inteligenci na úrovni Evropské unie.

Aplikace automatizovaných dohledových systémů policejních složek založených na umělé inteligenci se rozšiřují, a to především kvůli rostoucímu financování z veřejných rozpočtů a pokroku v počítačových algoritmech. Důsledkem technologického pokroku je analýza fotografií, videa, textů a dalších multimediálních zdrojů v masovém měřítku stále dokonalejší, levnější a dostupnější. Různé automatizované dohledové a profilovací systémy jsou i díky tomu často zaváděny netransparentním způsobem, bez řádného posouzení jejich nezbytnosti a proporcionality, bez přiměřeného upozornění veřejnosti, a tedy i bez předchozí společenské debaty. Automatizované plošné sledovací systémy mohou porušovat lidská práva – především právo na soukromí, informační sebeurčení, spravedlivý proces a důstojnost; mohou mít negativní dopad na svobodu projevu a shromažďování; a omezovat ochotu obyvatel účastnit se veřejných, společenských nebo politických aktivit. Vzhledem k zásadnímu významu soukromí a práva na

informační sebeurčení pro svobodné rozhodování může nasazení umělé inteligence k plošnému dohledu umožnit trvalý průnik do naší autonomie v masovém měřítku.

Automatizované dohledové a profilovací systémy s prvky umělé inteligence dosud nebyly předmětem hlubší veřejné diskuse. Začaly být fakticky používány, aniž by byly řešeny právní a etické důsledky. Společenské diskusi by měly být automatizované dohledové a profilovací systémy podrobeny z hlediska možného zesílení existujících nerovností a diskriminace. Na základě typických charakteristik, které se opakují u odsouzených osob, mohou algoritmy umělé inteligence vytipovat ty, na které se následně zaměří pozornost policie. Ostatně různé „pre-crime“ programy připomínající známé sci-fi Minority Report se ve světě používají již několik let. Otázkou tak je, zda je jejich rozvoj v souladu s koncepcí demokracie, svobody, rovnosti a sociální spravedlnosti.

Mnohdy je navíc sporná již zákonnost v současnosti nasazených automatických dohledových a profilovacích systémů. Například Evropský inspektor na ochranu osobních údajů udělil v říjnu 2020 napomenutí Europolu² za to, že nashromáždil celkem čtyři petabajty dat obsahující trestní spisy z členských států, data získaná z veřejně dostupných databází, z kompromitovaných komunikací celých on-line platforem a řady dalších zdrojů. Tento balík dat obsahující informace nejen o konkrétních odsouzených, ale také osobní údaje získané necíleně na osoby bez jakéhokoliv podezření na protiprávní jednání, plánoval Europol vytěžit pomocí systémů umělé inteligence. Problém je zejména v tom, že policejní orgány si interpretují zákonná ustanovení velice široce a před nasazením neprochází aplikace automatizovaných dohledových systémů vnějšími nezávislými kontrolami. Podle našich zjištění trpí nezákonností také systémy biometrického rozpoznávání dle obličeje, které provozuje Policie České republiky.

²European Data Protection Supervisor. EDPS Decision on the own initiative inquiry on Europol's big data challenge. Vydáno 5. října 2020. Dostupné na: https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europol_en

2. Směrem ke globální dystopii

„Argumentovat tím, že vás nezajímá ochrana soukromí, protože nemáte co skrývat, není nic jiného než říkat, že vás nezajímá svoboda slova, protože nemáte co říct.“

Edward Snowden, americký whistleblower

2.1 Plošné 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 tzv. **cíleného sledování**. Zásady ochrany soukromí a spravedlivého procesu vyžadují, aby u cíleného sledování, jako jsou odposlechy telefonů dle trestního řádu, měl policejní 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 systémy umělé inteligence a biometrickou identifikaci mohou mít velmi zásadní dopad na svobodu projevu a shromažďování, protože plošné sledování znamená faktickou ztrátu anonymity na veřejných prostranstvích. Všudypřítomnost plošného sledování je způsobilé omezovat účast občanů na společenském, veřejném a politickém životě a má dopad na možnost žít svobodně bez nutnosti přizpůsobovat své chování kvůli obavám z dopadů neustálého sledování. Německý ústavní soud ve svém nálezu 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] člancích 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.³

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

2.2 Prohlubování nerovností

Automatizované dohledové a profilovací systémy jsou technologie, které třídí lidi do různých kategorií. Jejich účelem je posoudit a ustanovit riziko u sledovaných osob a ve výsledku s nimi na základě toho zacházet odlišně. Takovéto profilování diskriminuje skupiny obyvatel na základě jejich "rizikovitosti", a prohlubuje nerovnost, protože vybrané skupiny jsou podřízeny vyšší míře dohledu. Diskriminaci ještě zhoršuje skutečnost, že vstupní údaje, které se používají k trénování systémů umělé inteligence, nejsou neutrální, ale odrážejí ve svých algoritmech předsudky a strukturální diskriminaci ve společnosti.

Zkreslení a chybovost v důsledku **diskriminačního nastavení** může vést k traumatizujícím vyšetřujícím úkonům policie u příslušníků některých skupiny obyvatel. Zvýšené kontroly mohou v konečném důsledku prohlubovat diskriminaci těchto skupin.

³Nález německého ústavního soudu ze dne 15. prosince 1983. 1 BvR 209/83, bod 146, Dostupné na: https://www.bverfg.de/e/rs19831215_1bvr020983.html

Diskriminační nastavení již bylo zdokumentováno u systémů biometrické identifikace obličeje. Ta je založena na pravděpodobnosti a existuje určitá míra chybné shody (tzv. falešně pozitivní) a chybné neshody (tzv. falešně negativní). Míra chybovosti je ovlivněna celou řadou faktorů včetně vstupních údajů, podmínek snímání nebo v podobě samotného algoritmu. Prokázalo se, že některé technologie k rozpoznávání obličeje mají vyšší chybovost u Afričanů nebo Asiatů.⁴ 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 na rozpoznávání obličejů se však později ukázaly jako chybné. Kvůli chybě biometrické technologie tak musel nedobrovolně absolvovat několikahodinovou proceduru včetně odběru DNA a otisků prstů.⁵ S Detroitem je spojen i případ neoprávněně zadržené Afroameričanky v pokročilém stadiu těhotenství v únoru 2023, kdy systém na rozpoznávání obličejů a způsob provádění rekognice vedl k chybným výsledkům.⁶

2.3 Akcelerace a rozlézáání sledování

Využívání umělé inteligence pro účely policejní praxe může vést k akceleraci všeobecného sledování. Systémy umělé inteligence dokážou celou řadu procesů automatizovat a zjednodušit. Zvýšením možností a kapacit pro plošné i cílené sledování tak pravděpodobně povede ke zvýšení poptávky ze strany policejních orgánů tyto systémy využívat více. Jedná se v podstatě o obdobu jevu, který je v ekonomii nazýván jako **indukce poptávky**. Jedná se o fenomén, při kterém se po zvýšení nabídky zvedne také poptávka. Platí v mnoha oborech, jak v ekonomii, tak například v dopravě, což se

⁴Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test. Part 3: Demographic Effects. Str. 2, 2019. National Institute of Standards and Technology. U.S. Department of Commerce. Dostupné z: <https://doi.org/10.6028/NIST.IR.8280>

⁵Václavíková J. "Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře. 2020. Dostupné z: <https://zpravy.aktualne.cz/zahranici/pocitac-se-spletl-policie-zatkla-spatneho-muze-kvuli-technol/r~b3cdeb14c1cb11ea8972ac1f6b220ee8/>

⁶Alsharif M., Santan C. Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology. 2023. Dostupné z <https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447>

nazývá dopravní indukce. Systémy umělé inteligence v policejní praxi tak obdobně způsobí indukci plošného sledování.

Indukce všeobecné míry sledování ovšem platí také pro využití umělé inteligence pro naprosto běžné administrativní úkony. Systémy umělé inteligence, které například pomohou k rychlému automatickému přepisu a vyhodnocení desítek hodin prostorových odposlechů, budou vytvářet poptávku po pořizování čím dál většího množství odposlechů. Limitující faktor v podobě zpracování odposlechů, kamerových záznamů nebo rozsáhlých textů byl především čas vyšetřovatelů. Strojovým zpracováním tato překážka padá a policie tak získá kapacity na zpracování mnohem většího množství informací. To může zvýšit atraktivitu sledovacích nástrojů a celkově tak akcelarovat míru nejen plošného, ale také cíleného sledování.

Využívání automatizovaných dohledových systémů policejními orgány povede k rozšíření sledování do čím dál širší sféry lidského chování. Systém automatizovaného dohledu a profilování 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, vlády a úřady často tuto technologii využijí nad rámec původního cíle, pro který byla zavedena. V anglicky psaných zdrojích – včetně orgánů Evropské unie – se pro tento jev používá pojem „*function creep*“, v překladu „**funkční rozlézáání**“. Nelze proto spoléhat na to, že nové automatizované sledovací systémy budou sloužit jen proti závažné kriminalitě. Nové automatizované dohledové systémy určené původně pro sledování teroristů či pedofilů mohou být v budoucnu použity k předcházení méně závažných hrozeb. Dalším důsledkem bude nárůst nerovnováhy moci mezi lidmi a státem a také zvýšení potenciálu zneužívání automatizovaných dohledových systémů.

2.4 Globální dystopie

Kombinovaný dopad nasazení automatických dohledových systémů, rozpoznávání obličejů na veřejných prostranstvích a vytěžování různých datových databází představuje nárůst rizik pro soukromí a základní práva. Ohrožení svobody občanů by ještě narostlo, pokud by data získaná systémem plošného sledování byla dále analyzována a používána k vytváření profilů jednotlivců. Možnosti této funkce se budou postupem času zvyšovat, protože stále více různých dat (sociální sítě, data veřejných orgánů) bude možné propojit se záznamy z automatizovaných sledovacích systémů. Vývoj podobných funkcí provádí také česká společnost Cogniware, která pro českou policii vyvíjí algoritmy propojující sledovací systémy s daty ze sociálních sítí.⁷ 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 se sledovací sítě vytvářejí 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.⁸ Protože jsou neustále zaváděny inovace s velkými daty a umělou inteligencí, existuje riziko, že jednou dojde ke kombinaci obrovského množství údajů z různých evidencí veřejné správy, veřejně přístupných rejstříků a dalších zdrojů, které mají k dispozici komerční subjekty. Propojování databází by mohlo být spojeno se zaznamenáváním fyzického výskytu jedinců na ulicích, přičemž by to umožňovalo monitorovat jejich interakce a pohyb způsobem, 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.

⁷Cogniware. Umělá inteligence z Česka pomáhá chytat zločince po celém světě. Tisková zpráva společnosti Cogniware ze dne 3. září 2020.

⁸Dixon P., Gellman R. The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future. 2014. World Privacy Forum. Dostupné z: www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf

Jedná se o státní systém hodnocení obyvatel na základě různých aspektů jejich ekonomického a společenského chování, na jehož základě mají jednotliví občané různou úroveň přístupu k veřejným službám.⁹

⁹Botsman R. Big data meets Big Brother as China moves to rate its citizens. 2017. Dostupné z: <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

3. Právní regulace

„Vytěžení kompletně celého komunikačního systému je jako když policie prohledá všechny byty v bloku, aby našla důkaz o zločinu: porušuje to právo na soukromí a je to prostě nezákonné.“

Robin Binsard, francouzský právník

Využívání umělé inteligence policejními orgány není v českých a evropských právních předpisech zatím dostatečně upraveno, přestože tyto technologie mohou poměrně významně zasáhnout do základních práv. Systémy umělé inteligence a s nimi spojené biometrické rozpoznávání na dálku jsou v České republice zaváděny bez dostatečného zhodnocení jejich možných dopadů, a to přestože mají tyto technologie potenciál k plošnému a hlubokému zásahu do lidské autonomie. Následující část se pokusí shrnout současnou a částečně také připravovanou právní úpravu na národní a evropské rovině.

3.1 Ochrana základních práv

Automatizované dohledové a profilovací systémy policie 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 dat zasahuje plošné sledování do dalších základních práv, mezi které patří **právo na důstojnost, svoboda projevu a svoboda shromažďování a sdružování**. Kromě zmíněných práv může využívání systémů umělé inteligence policejními orgány zasahovat také do dalších základních práv. Jedná se především o **právo na spravedlivý proces** a také o **zákaz diskriminace**. Všechna uvedená základní práva jsou vymahatelná skrze právní dokumenty na vnitrostátní, evropské a mezinárodní úrovni. Výčet dotčených ustanovení Úmluvy o ochraně lidských práv a základních svobod (Rady Evropy), Listiny základních práv Evropské unie a Listiny základních práv a svobod České republiky v souvislosti s uvedenými základními právy je uveden v tabulce 1.

Jakýkoli zásah do uvedených základních práv – včetně zpracovávání osobních dat systémy umělé inteligence nebo využívání biometrických technologií v kamerových systémech – podléhá splnění určitých hodnotících kritérií, která se promítají do tzv. testu proporcionality. Předně musí být zásah do základních práv stanoven zákonem, může být aplikován pouze, pokud je vhodný (naplňuje legitimní cíl v podobě veřejného zájmu nebo ochrany práv a svobod druhých) a nezbytný (legitimního cíle nelze dosáhnout vhodnějším způsobem) a nakonec takový zásah musí být proporcionální (oproti konkrétnímu veřejnému zájmu). Evropský inspektor ochrany údajů¹⁰ stanoví k prokázání nezbytnosti a proporcionality přísné pokyny,¹¹ přičemž dosavadní využívání biometrických technologií na veřejných prostranstvích splnění těchto právních kritérií zatím neprokázala. Podobné obavy platí pro další automatizované dohledové systémy policie.

¹⁰Evropský inspektor ochrany údajů je nezávislý dozorový úřad, jehož hlavním cílem je zajistit, aby orgány a instituce EU respektovaly právo na soukromí a ochranu údajů při zpracování osobních údajů.

¹¹European Data Protection Supervisor. Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. 2019. Dostupné z: https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

Tabulka 1: Přehled základních práv, která mohou být automatizovanými sledovacími systémy policie zasažena, a příslušná ustanovení v základních lidskoprávních dokumentech.

	Úmluva o ochraně lidských práv a základních svobod	Listina základních práv Evropské unie	Listina základních práv a svobod České republiky
Právo na soukromí	Článek 8	Článek 7	Článek 7 odstavec 1
Právo na ochranu osobních údajů	Článek 8	Článek 8	Článek 10 odstavec 3
Důstojnost	Preambule (odkazem na Všeobecnou deklaraci lidských práv)	Článek 1	Článek 10 odstavec 1
Svoboda projevu	Článek 10	Článek 11	Článek 17
Svoboda shromažďování	Článek 11	Článek 12	Článek 19
Svoboda sdružování	Článek 11	Článek 12	Článek 20
Právo na spravedlivý proces	Článek 6	Články 47 a 48	Článek 8 odstavec 2 Hlava pátá (Články 36 až 40)
Zákaz diskriminace	Článek 14	Článek 21	Článek 3

Soukromý život je dle Evropského soudu pro lidská práva "široký pojem, který není poddajný vyčerpávající definici".¹² Obecně chrání možnosti jednotlivce žít svůj život bez nepřiměřených zásahů a omezení. V základech tohoto práva je koncept svobody, ve smyslu "být nechán na pokoji", tedy koncept existence soukromé zóny, do které by neměl nikdo neoprávněně vstupovat nebo zasahovat.¹³ Evropský soud pro lidská práva také vyjádřil, že extenzivní interpretace pojmu soukromý život je ve shodě s Úmluvou o

¹²Rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2008. S. a Marper proti Spojenému království, číslo stížnosti 30562/04, bod 66.

¹³Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 294, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

ochraně osob se zřetelem na automatizované zpracování osobních dat,¹⁴ jejímž cílem je „zaručit na území každé smluvní strany každé fyzické osobě (...) respektování jejích práv a základních svobod, a zejména jejího práva na soukromý život, v souvislosti s automatizovaným zpracováním údajů osobního charakteru, které se jí týkají (čl. 1), přičemž ty jsou definovány jako jakékoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (čl. 2).“¹⁵ Evropský soud pro lidská práva také rozhodl, že tajné sledování za účelem odhalování nebo prevence trestné činnosti a sdílení kamerových záznamů spadá do oblasti působnosti čl. 8 Úmluvy o ochraně lidských práv a základních svobod, který chrání právo na soukromý a rodinný život.¹⁶

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.¹⁷ Jak konstatoval Ústavní soud ČR: *“Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti z jeho osobního soukromí zpřístupněny jiným subjektům.”*¹⁸

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 vůči sledovaným osobám. V tomto ohledu je znám případ S. a Marper proti Spojenému království, ve kterém Evropský soud pro lidská práva shledal, že “plošné a nerozlišující” uchovávání biometrických údajů je “nepřiměřeným zásahem” do práva na soukromí.¹⁹

¹⁴Úmluva je pod Radou Evropy, v České republice publikovaná jako Smlouva č. 115/2001 Sb. m. s.

¹⁵Rozsudek Evropského soudu pro lidská práva ze dne 10. února 2000. Amann proti Švýcarsku, číslo stížnosti 27798/95, bod 65.

¹⁶Rozsudek Evropského soudu pro lidská práva ze dne 28. dubna 2003. Peck proti Spojenému království, číslo stížnosti 44647/98, bod 133.

¹⁷Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 290, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

¹⁸Nález pléna Ústavního soudu České republiky ze dne 22. března 2011. Pl. ÚS 24/10, bod 29.

¹⁹Rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2008. S. a Marper proti Spojenému království, číslo stížnosti 30562/04, bod 125.

V případě společnosti Digital Rights Ireland zkoumal Soudní dvůr Evropské unie slučitelnost směrnice o uchovávání údajů 2006/24/ES s čl. 7 a 8 Listiny základních práv Evropské unie. Zvláště vzal na vědomí skutečnost, že směrnice: *"pokrývá obecně všechny osoby a všechny prostředky elektronické komunikace (...), aniž by došlo k jakékoli diferenciaci, omezení nebo výjimce s ohledem na cíl boje proti závažné trestné činnosti."*²⁰ Soud v případě 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 podezříváni z protiprávních činů nebo ohrožení veřejného pořádku. Jak uvedl v dalším případě Soudní dvůr Evropské unie: *"právní úprava, která veřejným orgánům umožňuje globální přístup k obsahu elektronických komunikací, musí být považována za zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny..."*²¹

V případně plošného sledování je dále zasaženo do **důstojnosti**, protože s osobami, které nejsou podezřelé z ničeho protiprávního, je zacházeno stejným způsobem jako s podezřelými. Základní práva Evropské unie jsou založena na důstojnosti člověka podle čl. 1 Listiny základních práv Evropské unie, který stanoví: *"Lidská důstojnost je nedotknutelná. Musí být respektována a chráněna."* Další nástroje v oblasti lidských práv jsou podobně centrálně založeny na všeobecné a nezcizitelné lidské důstojnosti. To vedlo k tomu, že důstojnost je někdy považována za "mateřské právo".²² V pojetí Ústavního soudu České republiky představuje právo na lidskou důstojnost v čl. 10 odst. 1 Listiny základních práv a svobod subjektivní právo jednotlivce a je chápáno ve

²⁰Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 8. dubna 2014. Spojené věci C-293/12 a C-594/12, Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další, bod 57.

²¹Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 6. října 2015. C-362/14, Schrems proti Data Protection Commissioner, bod 94.

²²Barak A. Human Dignity: The Constitutional Value and the Constitutional Right. 2015. *Human Rights Law Review*, Vol. 16, Issue 1, str. 176. Dostupné z: <https://doi.org/10.1093/hrlr/ngv042>

významu přirozené hodnoty člověka, která mimo jiné vylučuje jednat s jednotlivcem jako s objektem.²³

Plošné sledování pak zasahuje také svobodu projevu a svobodu shromažďování a sdružování, protože působí tzv. **odrazujícím účinkem** k výkonu těchto práv. K zásadě nepřípustnosti opatření s odrazujícím účinkem ve své judikatuře ve vztahu k právu na svobodu projevu a svobodě shromažďovací přihlížel i Ústavní soud ČR ve své judikatuře. Porušení svobody shromažďování pak konstatoval v případě excesivních kontrol totožnosti účastníků shromáždění, když konstatoval: *„Do práva pokojně se shromažďovat přitom zasahují i ta opatření, která mají 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.“*²⁴

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 Evropského soudu pro lidská práva a projevuje se v celé řadě právních zásad. V souvislosti s automatizovanými dohledovými systémy policie může dojít především k porušení zásady stíhání jen ze zákonných důvodů, kdy čl. 8 odst. 2 Listiny základních práv a svobod České republiky 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 legální cestou. Výkon tohoto práva spočívá především v tom být informován, přičemž nedostatek transparentnosti by mohl toto právo narušit.²⁵

Problém využití umělé inteligence a identifikace na základě obličeje v trestním řízení spočívá právě v netransparentnosti, na kterou mohou navíc dopláct také nevinní. Evropský inspektor ochrany osobních údajů v souvislosti se zpracováním dat umělou

²³Bartoň M., Kratochvíl J., Kopa M., Tomoszek M., Jirásek J., Svaček O. Základní práva. Str. 286, 2016. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-128-1.

²⁴Nález Ústavního soudu České republiky ze dne 10. října 2021. II. ÚS 1022/21.

²⁵Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 21. prosince 2016. Spojené věci C-203/15 a C-698/15, Tele2 Sverige AB proti Post-Och Telestyrelsen a Secretary of State for the Home Department proti Tom Watson a dalším.

inteligencí a automatickým rozhodováním upozornil na několik problematických okruhů: pravdivost údajů, spolehlivost analýzy a rozhodovací proces ze strany analytika.²⁶ Spolehlivost analýzy kriminalistických dat může narážet na samotné limity schopností systémů umělé inteligence, kterými jsou například pochopení sarkasmu a ironie.

S možnou systematickou chybovostí systémů umělé inteligence souvisí zásah do **zákazu diskriminace** (více v kapitole 2.2 Prohlubování nerovností). Diskriminace je termín označující rozlišování lidí založené na předsudku (či předpokladu) vlastností, nebo schopností týkajících se rasy, pohlaví, věku, náboženství nebo jiných skupinových charakteristik. Nediskriminace je pak zcela elementární předpoklad k řádnému fungování moderní společnosti, nicméně některé systémy umělé inteligence se mohou kvůli způsobu jejich fungování podílet na diskriminaci některých ohrožených skupin obyvatel. Toto riziko je vyšší v případě, kdy nejsou dostatečně řešeny etické otázky spojené s vývojem a fungováním těchto technologií s ohledem na riziko diskriminace.

3.2 Právní úprava Evropské unie

3.2.1 Účinná právní úprava

Z účinných právních předpisů Evropské unie se na systémy umělé inteligence, ve kterých dochází k zpracování osobních údajů, týká v současné době především účinná legislativa ochrany osobních údajů. Z ní na Policii České republiky dopadají dva právní předpisy. Jedná se o **Obecné nařízení o ochraně osobních údajů** (známé pod zkratkou „GDPR“),²⁷ které stanoví obecné zásady ochrany osobních údajů. GDPR stanovuje

²⁶European Data Protection Supervisor. EDPS Decision on the own initiative inquiry on Europol's big data challenge. Vydané 5. října 2020. Dostupné z: https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en

²⁷Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

obecná pravidla pro zpracování osobních údajů v členských státech Evropské unie a vztahuje se na všechna zpracování osobních údajů veřejných a soukromých subjektů vyjma zpracování za účelem prosazování práva, což se týká bezpečnostních sborů (v České republice: Policie ČR, Celní správa, Vězeňská služba ČR a Generální inspekce bezpečnostních sborů). Druhým právním aktem je **Směrnice o ochraně údajů v oblasti prosazování práva**²⁸ (dále jen „Směrnice“), která se vztahuje na zpracování osobních údajů 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 Směrnice má užší specifickou oblast působnosti.²⁹

Policie České republiky zpracovává osobní údaje v obou dvou režimech – GDPR i Směrnice – v závislosti na tom, jakou svou činnost právě vykonává. Policie má totiž pravomoci nejen jako ozbrojený bezpečnostní sbor, ale také jako orgán státní správy. Činnosti policie ve smyslu orgánu státní správy jsou regulovány přímo účinným GDPR. Za tyto činnosti policie lze považovat například provádění úkonů dle zákona o silničním provozu, na úseku zbraní a střeliva nebo v rámci přestupkového řízení. Naopak na činnosti policie ve smyslu ozbrojeného bezpečnostního sboru se vztahuje Směrnice. Za tuto činnost policie lze považovat její role v trestním řízení nebo role při bezpečnostních zásazích a udržování pořádku. Samotná Směrnice není v zásadě přímo účinná, protože pravidla v ní stanovená se transponují do českého právního řádu až skrze národní legislativu (více v kapitole 3.3 Právní úprava v České republice). Nicméně je třeba dodat, že současná transpozice Směrnice neproběhla naprosto bezchybně. Je proto vhodné využívat také přesné znění Směrnice, protože interpretace národní legislativy musí být souladná právě se Směrnicí. V případě rozporu národní legislativy se Směrnicí má přednost Směrnice. V následujícím textu bude věnována větší pozornost Směrnici než

²⁸Směrnice 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.

²⁹Pattynová J., Suchánková L., Černý J., Růžicka M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. Str. 540, 2019. Nakladatelství Leges, s. r. o. ISBN 978-80-7502-396-4.

GDPR, protože většina zpracování osobních údajů systémy umělé inteligence policí spadá právě pod ní. Podstatný rozdíl je především v tom, že na rozdíl od GDPR není dle Směrnice souhlas subjektu údajů jedním z právních důvodů zpracování.

Směrnice (podobně jako GDPR) stanoví, že při využívání osobních údajů, musí být splněny určité zásady uvedené v čl. 4 Směrnice. Těmito principy se řídí také výklad souvisejících národních právních předpisů. Mezi tyto zásady dle čl. 4 Směrnice 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. Svěbytný **požadavek zákonnosti zpracování** je pak v článku 8 odst. 2 Směrnice, který ukládá, že právo členského státu upravující zpracování musí stanovit alespoň cíle zpracování, osobní údaje, jež mají být zpracovány, a účely zpracování. Článek 11 Směrnice dále zakazuje plně automatizovaná rozhodnutí založená na využívání osobních údajů (včetně biometrických údajů).

Směrnice v čl. 6 ukládá také povinnost rozdílného zacházení s osobními údaji osob odsouzených nebo podezřelých z trestných činů (když má policejní orgán závažné důvody se domnívat, že konkrétní osoba spáchala nebo se chystá spáchat trestný čin) a mezi osobními údaji osob, které nejsou odsouzené nebo podezřelé z trestné činnosti. Rozlišení různých kategorií osob je důležité, aby došlo k odlišení legitimního a zákonného zpracování údajů u důvodně podezřelých osob a necíleným zpracováváním osobních údajů kterékoliv náhodné osoby. Do první kategorie pak nelze zařadit některá zpracovávání v systémech umělé inteligence, jako například necílené zpracování biometrických údajů osob na veřejných prostorech nebo necílené prohledávání biometrické databáze všech občanů.

Podle Směrnice a 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**. Směrnice (stejně jako GDPR) definuje biometrické údaje v čl. 3 odst. 13 jako *"osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje."* Je tudíž zřejmé, že bude značná část osobních údajů zpracovávaných systémy umělé inteligence spadat mezi citlivé osobní údaje.

Některé systémy umělé inteligence využívané policií spadají do působnosti GDPR (například systémy spravující docházku zaměstnanců policie) a jiná pod Směrnicí (kamerový systém s biometrickým rozpoznáváním obličeje na veřejném prostranství). Přesto existuje řada situací, ve kterých dochází k překryvu různých účelů a není jednoznačné, kterou právní úpravu použít, protože má více účelů. Nejasný režim může být například pro kamerový systém s automatickým čtením registračních značek vozidel, kdy může být systém používán k řešení dopravních přestupků, ale také k vyšetřování trestné činnosti. Pro efektivnější ochranu osobních údajů a odstraňování mezer v zákoně, je stále potřeba důraznější vymáhání práva a jasnějšího výkladu GDPR, Směrnice a jejich vzájemných vztahů. Přesto zásadní východiska pro zpracování osobních údajů při plošném sledování zůstávají stejné, ať se použije GDPR nebo Směrnice, respektive její národní implementace.

3.2.2 Připravovaná právní úprava

V případě systémů umělé inteligence a kamerových systémů s biometrickou identifikací se jedná o rychle se rozvíjející technologie, jejichž regulace je v Evropské unii

nevyhnutelná. V současnosti vrcholí legislativní proces nového nařízení. Již v únoru 2020 vydala Evropská komise Bílou knihu o umělé inteligenci³⁰, která nastínila směřování regulace pro širokou škálu aplikací umělé inteligence.³¹ O rok později v dubnu 2021 zveřejnil Evropská komise samotný **návrh Aktu o umělé inteligenci**.³² V červnu 2023 přijal Evropský parlament k návrhu velké množství významných pozměňovacích návrhů, ovšem základní architektura a směřování Aktu o umělé inteligenci (dále jen „Nařízení“) zůstalo zachováno. Protože finální znění Nařízení není v tuto chvíli stále schváleno, může ještě stále dojít ke změnám, které nelze jednoznačně předvídat.

Návrh Nařízení obsahuje harmonizovaná pravidla pro „systémy umělé inteligence“, přičemž definice tohoto termínu sleduje myšlenku širokého pojetí tak, aby pokrýval co největší okruh možných případů. Podle schváleného pozměňovacího návrhu Evropského parlamentu je systémem umělé inteligence: *„strojový systém, který je navržen tak, aby fungoval s různou úrovní autonomie, a který může pro explicitní nebo implicitní cíle generovat výstupy, jako jsou předpovědi, doporučení nebo rozhodnutí, které ovlivňují fyzické nebo virtuální prostředí“*. Systémy umělé inteligence se budou členit do čtyř kategorií na základě přístupu založeném na posouzení rizik. Návrh nařízení rozlišuje systémy umělé inteligence vytvářejícími: 1) nepřijatelné riziko, 2) vysoké riziko, 3) omezené riziko, 4) nízké nebo minimální riziko.

Systémy umělé inteligence s nepřijatelným rizikem budou zakázané, a to z důvodu jejich rozporu s hodnotami Evropské unie. Nařízením by mělo být zakázáno používat systémy, které zjevně ohrožují život, zdraví, bezpečnost nebo práva jednotlivců. Jedná se ve zkratce o systémy umělé inteligence, které 1) slouží k přidělování sociálního kreditu; 2) jsou používány k rozpoznávání emocí či biometrické identifikaci na dálku; 3) manipulují s chováním lidí; a 4) používají podprahové techniky na zranitelné skupiny.

³⁰Bílá kniha je obecně autoritativní zpráva nebo průvodce, který informuje o určitém problému a představuje filozofii Evropské unie v dané věci. Má pomoci porozumět problematice, vyřešit určité otázky nebo učinit rozhodnutí.

³¹Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Dostupné z: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_cs.pdf

³²Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0206>

Bližší pozornost si v souvislosti s policejní praxí zaslouží především zákaz rozpoznávání emocí a biometrické identifikace na dálku. Původní návrh Evropské komise doznal v tomto ohledu zásadní změny a v současné verzi je zakázáno používání systémů umělé inteligence:

- 1) používání biometrických kategorizačních systémů, které fyzické osoby rozřazují podle citlivých nebo chráněných atributů nebo charakteristik;
- 2) k biometrické identifikaci na dálku „v reálném čase“ na veřejně přístupných místech;
- 3) k posuzování fyzických osob nebo jejich skupin za účelem posouzení rizika, že fyzická osoba spáchá trestný čin nebo přestupek;³³
- 4) vytvářejících nebo rozšiřujících databáze rozpoznávání obličeje prostřednictvím necíleného získávání obrázků obličeje z internetu nebo kamerových záznamů;
- 5) k odvození emocí fyzické osoby v oblasti prosazování práva nebo správy hranic;³⁴
- 6) pro analýzu kamerových záznamů z veřejně přístupných prostorů prostřednictvím systémů „zpětné“ biometrické identifikace na dálku, pokud nepodléhají předchozímu soudnímu povolení a nejsou nezbytně nutné pro cílené vyhledávání spojené s konkrétním závažným trestným činem.³⁵

Systémy umělé inteligence s vysokým rizikem budou systémy, které představují vysoké riziko pro zdraví a bezpečnost nebo pro základní práva fyzických osob. 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.

³³Tyto systémy měly být v původním návrhu považovány za vysoce rizikové, ale nikoliv zakázané.

³⁴Tyto systémy měly být v původním návrhu považovány za vysoce rizikové, ale nikoliv zakázané.

³⁵Původně měly být zakázány pouze systémy biometrické identifikace na dálku na veřejně přístupných místech „v reálném čase“.

Mezi systémy umělé inteligence s vysokým rizikem budou zařazeny systémy ve dvou skupinách v závislosti na vykonávané funkci ale také konkrétním účelu. První skupina se týká výrobků regulovaných evropskými předpisy zajišťujícími jejich bezpečnost, přičemž policii pravděpodobně výrazně nezasáhne. Druhá skupina bude zahrnovat systémy umělé inteligence používané v několika specifických oblastech. Mezi tyto specifické oblasti budou patřit: 1) vymáhání práva a 2) migrace, azyl a správa hraničních kontrol. Konkrétní seznam vysoce rizikových systémů umělé inteligence se nachází v příloze III návrhu Nařízení.

V **oblasti vymáhání práva** se jedná o systémy umělé inteligence určené pro použití donucovacími orgány:

- 1) jako detektory lži a obdobné nástroje;
- 2) za účelem hodnocení spolehlivosti důkazů v průběhu vyšetřování nebo stíhání trestných činů;
- 3) za účelem profilování fyzických osob v průběhu odhalování, vyšetřování nebo stíhání trestných činů;
- 4) za účelem analýz trestné činnosti fyzických osob umožňující prohledávat složité související i nesouvisející rozsáhlé datové soubory, s cílem určit v těchto datech neznámé vzorce nebo objevit skryté souvislosti.

V **oblasti migrace, azyl a správa hraničních kontrol** se jedná o systémy umělé inteligence určené pro použití příslušnými orgány:

- 1) jako detektory lži a obdobné nástroje;
- 2) za účelem posuzování rizika, jež představuje fyzická osoba, která má v úmyslu vstoupit nebo vstoupila na území členského státu;
- 3) za účelem ověřování pravosti cestovních dokladů fyzických osob a odhalování falešných dokladů kontrolou jejich bezpečnostních prvků;
- 4) při zkoumání a posuzování pravdivosti důkazů v souvislosti s žádostmi o azyl, udělení víza a povolení k pobytu;

- 5) pro potřeby monitorování, sledování nebo zpracování údajů v souvislosti s činnostmi správy hranic za účelem odhalování, rozpoznávání nebo identifikace fyzických osob;
- 6) za účelem předpovídání nebo predikce trendů souvisejících s migračním pohybem a překračováním hranic.

Systémy umělé inteligence s omezeným rizikem by měly splňovat minimální požadavky na transparentnost, aby uživatelé mohli činit informovaná rozhodnutí. Zbytková kategorie **systémů umělé inteligence s nízkým nebo minimálním rizikem** by neměla být limitována žádnými specifickými požadavky. Přestože poslední dvě kategorie systémů umělé inteligence jsou bez zásadních požadavků, budou v policejní praxi také využívány (např. chatboty či překladatelské nástroje).

Dalším evropským právním předpisem, který se v současnosti nachází v legislativním procesu, je **návrh nařízení Prüm II**.³⁶ Jedná se o právní instrument, který by měl usnadnit policejní spolupráci na předávání biometrických a dalších údajů mezi členskými státy. Novým prvkem má být především proces předávání zobrazení obličeje určené k biometrické identifikaci. Bližší podrobnosti k tomuto návrhu se nachází v kapitole 6.1 Sdílení biometrických dat v Evropské unii.

3.3 Právní úprava v České republice

Česká právní úprava týkající se ochrany osobních údajů v souvislosti s využíváním systémů umělé inteligence Policií České republiky vychází z právní úpravy Evropské unie. Směrnici v českém právním systému provádí vzhledem k činnosti Policie České republiky dva zákony. Jsou jimi zákon č. 110/2019 Sb., o zpracování osobních údajů, a zákon č. 273/2008 Sb., o Policii České republiky. Nicméně je potřeba zdůraznit, že provedení Směrnice není v uvedených předpisech vyčerpávající ani bezchybné.

³⁶Návrh 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. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0784>

Zpracováním a ochranou osobních údajů orgány veřejné moci za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů se zabývá hlava III části první **zákona č. 110/2019 Sb., o zpracování osobních údajů**. Uvedená hlava zákona však z hlediska osobních údajů, nestanoví nad rámec Směrnice více podrobností. Do uvedené hlavy zákona jsou přepsány v hrubých rysech hlavní povinnosti policie při zpracování osobních údajů a práva subjektu zpracovávaných osobních údajů. Mezi základní práva subjektu údajů patří 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 policie pak patří například povinnost vedení záznamů (logování) při operacích prováděných v databázích osobních údajů, povinnost zpracovat posouzení vlivu na ochranu osobních údajů a povinnost projednat s Úřadem pro ochranu osobních údajů takové operace s osobními údaji, které představují vysoké riziko. V zákoně o zpracování osobních údajů jsou tudíž uvedeny především obecné povinnosti zpracování osobních údajů aplikovatelné na systémy umělé inteligence provozované policií.

Zákonné zmocnění ke zpracování osobních údajů Policií České republiky se pak nachází v **zákoně č. 273/2008 Sb., o Policii České republiky**. Nicméně samotné zmocnění ke zpracování osobních údajů je upraveno nedostatečně a minimalisticky ustanovením § 79 odst. 2 zákona o Policii České republiky. Podle tohoto ustanovení může policie zpracovávat osobní údaje, je-li to nezbytné za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Za stejným účelem může policie zpracovávat osobní údaje také k ochraně důležitých zájmů subjektu údajů. 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.“*

Výslovné omezení 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, sexuální 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 Směrnice, protože omezení je užší a nevztahuje se na biometrické a genetické údaje. Biometrické údaje pak nejsou v zákoně o Policii České republiky zmíněny vůbec. K biometrickým údajům je potřeba doplnit, jak je zákon o Policii České republiky vykládán přímo policií. Podle výkladu policie je možné provádět biometrickou identifikaci z kamerových záběrů „v reálném čase“ i „zpětně“ zásadně bez větších omezení nebo jednoznačné právní úpravy.

Pro **biometrickou identifikaci v kamerových systémech „v reálném čase“** je dle policie podstatný § 62 odst. 1 zákona o Policii České republiky, 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 zákona o Policii České republiky).

Podobně „inovativní“ je policejní výklad § 66 odst. 1 a 2 zákona o Policii České republiky, podle kterého je možné provádět **biometrickou identifikaci z kamerových záznamů „zpětně“** oproti databázi všech osob žijících v České republice. Podle uvedeného ustanovení totiž může policie získávat a zpracovávat digitální fotografie a identifikátory lidí vedených v informačních systémech, konkrétně v informačním systému evidence občanských průkazů, informačním systému evidence cestovních dokladů, informačním systému evidence diplomatických a služebních pasů, registru řidičů, centrálním registru řidičů, nebo informačním systémem cizinců. Ačkoli není v zákoně jednoznačně definován způsob zpracování digitálních fotografií, tak důvodová zpráva k novele

zákona o Policii České republiky uvádí: „Navrhovaná změna přináší policii možnost softwarového vyhledávání a rozpoznávání obličejů, která v případě potřeby dokáže významným způsobem zkrátit čas k odhalení pachatele, případně zabránit dalším hrozícím útokům.“

Důvodová zpráva k zákonu, nikoli ale už text zákona, k němuž se vztahuje, tudíž nepřímě počítá s tím, že záběry z bezpečnostních kamer může policie pomocí softwaru na rozpoznávání obličejů analyzovat a porovnávat s fotografiemi z databáze všech osob žijících v České republice. V konečném důsledku by takto bylo možné vysledovat pohyb konkrétního člověka ve veřejném prostoru nebo identifikovat osoby, které se na záznamu objeví, pokud jsou jejich fotografie v informačních systémech. Analytické nástroje s těmito funkcemi by mohla policie využívat v různé míře, protože zákon není v tomto ohledu konkrétní. Přitom policejní orgány mají obecně tendenci vykládat své pravomoci široce.

Výše uvedená úprava se vztahuje na zpracování osobních údajů v činnostech policie s účelem prevence, vyšetřování a odhalování trestných činů. Krom této právní úpravy se na zpracování osobních údajů policií vztahuje také přímo účinné GDPR pro ty činnosti, ve kterých vystupuje jako správní orgán. Samotné systémy umělé inteligence užívané policejními orgány dosud nejsou explicitně regulovány národními právními předpisy.

4. Současné aplikace

„Bylo hrozně nebezpečné dát volný průchod myšlenkám, když byl člověk na veřejném místě anebo v dosahu obrazovky. Nejmenší drobnost vás mohla prozradit. Nervový tik, neuvědomělý výraz úzkosti, zvyk brblat si sám pro sebe – všechno, v čem byl náznak nenormálnosti, toho, že máte co skrývat. Tvářit se nenáležitě (například s nedůvěrou, když se oznamovalo nějaké vítězství) byl v každém případě sám o sobě přestupek, který mohl být potrestán. V newspeaku na to dokonce existovalo slovo: říkalo se tomu FACECRIME.“

George Orwell, autor dystopického románu 1984

4.1 Biometrika obličeje

Zatím nejvíce diskutovanou aplikací umělé inteligence pro policejní praxi jsou kamerové systémy zpracovávající biometriku obličeje. Jedná se o zdokonalení sledování skrze kamerové systémy, které byly do veřejných prostor hromadně instalovány v minulých letech. Jejich cílem byla prevence kriminality. Podle výsledků studií četnosti kriminality nedošlo v místech instalace kamerových systémů k jejímu snížení, ač měl tento faktor vliv na strukturu kriminality.³⁷ Nyní jsou kamerové systémy vybavovány biometrickým zpracováním lidského obličeje, což ještě zvyšuje intenzitu plošného sledování veřejně přístupných prostor. Přesto může být zpracování biometricky obličeje širší než jen v kamerových systémech. Předmětem vyhledávání konkrétní osoby dle biometrických rysů mohou být také sociální sítě, veřejná média nebo internetové streamovací kanály.

Biometrické údaje jsou informace o biologických vlastnostech, fyziologických charakteristikách, znacích jedince nebo opakovatelném jednání, kdy jsou tyto rysy nebo jednání pro daného jedince jedinečné a měřitelné, a to i tehdy, když použité vzory zahrnují určitý stupeň pravděpodobnosti. Typickými příklady biometrických dat jsou

³⁷Gill M., Spriggs A. Vyhodnocení účinku kamerových systémů. 2007. Český překlad: Institut pro kriminologii a sociální prevenci, Praha, str. 109. ISBN 978-80-7338-061-8.

otisky prstů, lidský hlas, ale také geometrie rukou, vzorky žil nebo některé hluboce zakořeněné dovednosti nebo jiné charakteristiky chování (například ručně psaný podpis, stisknutí kláves, konkrétní způsob chůze nebo mluvy).³⁸ V této kapitole se zaměříme na zpracování struktury obličeje, jako biometrického údaje. Formy jeho zpracování představují různé operace, z nichž nikoliv všechny představují stejné riziko pro ochranu osobních údajů. Mezi tyto operace s biometrií obličeje patří: rozpoznání, identifikace, autentizace a kategorizace.

Nejméně problematickou operací je **rozpoznání obličeje**. Jedná se o operaci, která sama o sobě nevede k identifikaci ani verifikaci osoby. Jedná se o pouhé rozpoznání obličeje člověka na obrazovém záznamu. Tato operace může být využívána policií například k počítání osob na kamerových záběrech. **Kategorizace dle obličeje** je operace zjišťování, zda jednotlivec patří do skupiny osob s určitou předem stanovenou charakteristikou. Ani v tomto případě není smyslem identifikovat nebo ověřit totožnost určitého jednotlivce, nýbrž jej automaticky zařadit do určité kategorie. Jedná se v podstatě o profilování a jeho účelem může nebo nemusí být provedení určitého úkonu. V policejní praxi lze takto například sledovat zda do prostoru vstupují osoby určitého věku, osoby mající roušku nebo určitou pokrývku hlavy. Rozpoznání obličeje a kategorizaci dle obličeje nebude v této kapitole věnována pozornost a zaměří se na další dvě.

Autentizace a identifikace jsou operace, kdy dochází k porovnání shody na dvou nebo více snímcích. To probíhá na základě detekce a měření různých rysů obličeje, extrakce těchto hodnot ze zachycené fotografie a v dalším kroku jejich porovnáním s hodnotami v databázi, které jsou převzaté z jiné fotografie nebo fotografií.³⁹ **Autentizace dle obličeje** (někdy také verifikace) je v podstatě ověření totožnosti osoby pomocí biometrického kamerového systému. Jedná se o proces srovnávání biometrických

³⁸Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019, str. 63. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocní%2Dzprava%2Dza%2Drok%2D2019

³⁹European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. Str. 2, 2019. ISBN 978-92-9474-839-3. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

údajů určité osoby (pořízených v době ověřování totožnosti) s jednou uloženou biometrickou šablonou. Použití této operace může sloužit pro omezení přístupu do určitých prostor jen pro určenou osobu. Od ní se pak liší **identifikace dle obličeje**, při které se již 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.

Kamerové systém provádějící identifikaci dle biometrie obličeje je v návrhu Nařízení o umělé inteligenci nazýván jako **systémem biometrické identifikace na dálku**. Podle 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 budoucí regulace nebude omezovat jen na biometrii obličeje, ale také na další biometrické charakteristiky možné pořídit na dálku jako například chůze. Návrh Nařízení o umělé inteligenci navíc systémy biometrické identifikace na dálku rozděluje na dvě praktické skupiny: „v reálném čase“ a „zpětné“. V **systému biometrické identifikace na dálku v reálném čase** probíhá zachycení biometrických údajů, porovnání a identifikace bez významné prodlevy. Ostatní systémy pak mají být považovány za **systémy zpětné biometrické identifikace na dálku**. Toto 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.

Policie České republiky je subjekt, který kamerové systémy se zpracováním biometrických údajů využívá a dlouhodobě se zasazuje o jejich další nasazení na veřejných prostranstvích. Rozsah využití těchto systémů je do značné míry neprozkoumaný. V některých případech mohou být tyto technologie nasazeny bez toho, aniž by byla veřejnost informována. Navíc se jedná o rychle se rozvíjející oblast a související informace rychle zastarávají. V následující části této kapitoly budou popsány

systémy biometrické identifikace a autentizace, které v současnosti využívá policie, a dále pak některé pokusy rozšířit jejich nasazení do dalších oblastí.

4.1.1 Kamerový systém na Letišti Václava Havla

Zatím jediný veřejně známý systému biometrické identifikace na dálku v reálném čase provozovaný Policií České republiky se nachází na Letišti Václava Havla v Praze. Uvedený systém biometrické identifikace byl vybudovaný na základě usnesení vlády České republiky č. 47/2015, o zvýšení bezpečnosti na mezinárodním letišti Václava Havla v Praze ze dne 19. ledna 2015. Podle sdělení policie je rozmístěno celkem 145 kamer ve veřejném prostoru letiště na místech s vysokou koncentrací osob, především kolem informačních tabulí, kde se cestující a jejich doprovod na delší dobu zastavují.⁴⁰

Dodavatelé biometrického identifikačního systému na Letišti Václava Havla 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."*⁴¹ Podle sdělení Policie České republiky je pro detekci obličeje v kamerovém systému užívána softwarová technologie NEC NeoFace Watch a NeoFace Archiver. Celý kamerový systém s biometrickým zpracováním je dále propojen s dalšími bezpečnostními systémy a databázemi provozu letiště. Celková cena projektu integrace bezpečnostního systému s biometrickou identifikací v kamerových systémech byla na základě smluv a jejich dodatků do září 2020 více než 90 milionů korun.⁴²

⁴⁰Ministerstvo vnitra České republiky. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů. Tisková zpráva ze dne 4. března 2019. Dostupné z: <https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx>

⁴¹Smlouva o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. uzavřená dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-108/ČJ-2015-990656.

⁴²Dodatek č. 6 ke smlouvě o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-197/ČJ-2015-990656.

Detailnější podmínky provozu kamerového systému s biometrickou identifikací na letišti nebyly zveřejněny. Provozovatel systému - Ředitelství služby cizinecké policie - považuje interní předpisy policie za informace, které je potřeba ze strategických důvodů tajit.⁴³ Také smlouva mezi Ministerstvem vnitra s dodavatelem zabezpečovacího systému obsahuje klauzule o mlčenlivosti, podle které jsou okolnosti a údaje získané v souvislosti s plněním zakázky považovány za důvěrné, a to včetně "specifikace předmětu plnění" v příloze smlouvy.⁴⁴ Kamerový systém na Letišti Václava Havla Praha z tohoto důvodu postrádá možnost detailnější kontroly ze strany veřejnosti.

Z informací poskytnutých Policií České republiky není jednoznačné, jak a kým jsou biometrická data z kamerového systému aktivně využívána. Je známo pouze to, že biometrická data získaná z kamerového systému jsou Policií České republiky porovnávána s informačním systémem Pátrání po osobách (PATROS), v němž jsou zpracovávány údaje o hledaných a pohřešovaných osobách. Kromě Policie České republiky mají k záznamům z kamerového systému přístup také Celní správa, Bezpečnostní informační služba a Vojenské zpravodajství, přičemž Policie České republiky může údaje předávat ještě národnímu členovi Eurojustu,⁴⁵ Národnímu bezpečnostnímu úřadu, Národnímu úřadu pro kybernetickou a informační bezpečnost, Vojenské policii, Ministerstvu vnitra, Vězeňské službě České republiky a dalším orgánům veřejné správy.⁴⁶ V jaké míře kamerový systém s biometrickou identifikací jmenované státní orgány skutečně využívají, nebylo Policií České republiky sděleno. Od spuštění systému na letišti dne 15. června 2018 až do 31. prosince 2022 došlo k celkem 234

⁴³Rozhodnutí o částečném odmítnutí žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů vydané dne 20. srpna 2020 Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednací PPR-24979-6/ČJ-2020-990810.

⁴⁴Smlouva o dílo mezi Českou republikou - Ministerstvem vnitra a společnostmi Siemens, s.r.o. a AUROTON COMPUTER, spol. s r.o. uzavřená dne 6. června 2017. Integrace bezpečnostních systémů a systém pro automatickou biometrickou detekci obličejů včetně rozšíření systému CCTV. Číslo jednací objednatele PPR-27225-108/ČJ-2015-990656.

⁴⁵Eurojust (Jednotka Evropské unie pro justiční spolupráci) je agenturou Evropské unie zřízenou za účelem zvýšení efektivity mezinárodní justiční spolupráce v trestních věcech mezi členskými státy Evropské unie, zejména v oblasti vyšetřování a stíhání závažné přeshraniční kriminality a organizovaného zločinu.

⁴⁶Částečné poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednací PPR-24979-5/ČJ-2020-990810.

shodám s osobami vedenými v zájmových databázích.⁴⁷ Údaje o počtech hledaných osob zachycených kamerovým systémem v jednotlivých měsících od začátku provozu kamerového systému až do konce roku 2022 jsou v tabulce 2.

Tabulka 2. Počet hledaných osob, které byly ztotožněny kamerovým systémem na Letišti Václava Havla v Praze 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

Podle našich zjištění je provoz kamerového systému s biometrickou identifikací na Letišti Václava Havla provozován bez řádného splnění všech zákonných povinností. Policie České republiky si pro provozování systému nezpracovala obligatorní posouzení vlivu na ochranu osobních údajů dle Směrnice. Policie to obhájí tvrzením, že v době spuštění sledovacího systému do zkušebního provozu, nebyla Směrnice do národní legislativy transformována a postačovala prý ohlašovací povinnost Úřadu pro ochranu osobních údajů.⁴⁸ Dalším problémem zpracování je zákonnost, kdy policie za zákonný titul k provozu kamerového systému s biometrickou identifikací na Letišti Václava Havla považuje § 62 a § 79 odst. 1 zákona o Policii České republiky, výkladem který je uveden v kapitole 3.3 Právní úprava v České republice.

Povinnost zpracovat tzv. posouzení vlivu na ochranu osobních údajů je stanoven ve čl. 27 Směrnice. Posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů musí správce údajů provést, pokud je pravděpodobné, že určitý druh zpracování,

⁴⁷Poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. dubna 2023 vydané Ředitelstvím služby cizinecké policie pod číslem jednacím CPR-16176-6/ČJ-2021-930103.

⁴⁸Částečné poskytnutí informací na základě žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 24. srpna 2020 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-24979-5/ČJ-2020-990810.

zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům bude zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob.⁴⁹ Používání kamerových systémů k biometrické identifikaci osob na veřejných prostranstvích v reálném čase tyto podmínky naplňuje a posouzení vlivu na ochranu osobních údajů bude podléhat vždy. Uvedené ustanovení Směrnice je provedeno § 37 zákona č. 110/2019 Sb., o zpracování osobních údajů. Posouzení musí obsahovat alespoň obecný popis zamýšlených operací zpracování, posouzení rizik z hlediska práv a svobod subjektů údajů, plánovaná opatření k řešení těchto rizik, záruky, bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů a k doložení souladu s touto směrnicí, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Zákon o zpracování osobních údajů vešel v účinnost dne 24. dubna 2019, což je více než 14 měsíců poté, kdy byl spuštěn kamerový systém s biometrickou identifikací na Letišti Václava Havla. Obecně směrnice nemají přímý účinek ve vnitrostátním právu členských států, jako je to u nařízení. Nicméně v čl. 63 odst. 1 Směrnice, který stanoví podmínky provedení ve vnitrostátním právu, ukládá povinnost členských států přijmout, zveřejnit a uvést v platnost právní předpisy nezbytné pro dosažení souladu se Směrnicí do 6. 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 Evropské unie neprovedl směrnici ve stanovené lhůtě.⁵⁰ Přestože bylo později Evropským soudním dvorem určeno, že přímý účinek je jen vertikální vzestupný, v tomto případě je také tento požadavek splněn, protože směrnice ukládá povinnost členskému státu chránit citlivé osobní údaje jeho občanů.

Přestože byla Směrnice přijata již 27. dubna 2016 a stanovovala členským státům povinnost provést ji do dvou let (6. května 2018), nebylo posouzení vlivu na ochranu osobních údajů pro kamerový systém s biometrickou identifikací na letišti Václava

⁴⁹Pattynová J., Suchánková L., Černý J., Růžicka M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. Str. 630, 2019. Nakladatelství Leges, s.r.o. ISBN 978-80-7502-396-4.

⁵⁰Rozsudek Evropského soudního dvora ze dne 4. prosince 1974. 41/74, Yvonne van Duyn proti Home Office.

Havla Praha zpracováno minimálně do 24. srpna 2020. Demonstruje to nedostatečné vynucování evropské legislativy na ochranu osobních údajů při zpracovávání biometrických údajů policií.

Problematická je také otázka právního základu provozu kamerového systému s biometrickou identifikací. Zpracování biometrických údajů, spadajících do zvláštní kategorie údajů dle čl. 10 Směrnice, není v § 62 a § 79 odst. 1 zákona o Policii České republiky explicitně upraveno. Z uvedených ustanovení tudíž nevyplývá oprávnění policie zpracovávat obrazové záznamy za účelem sestavení biometrické reprezentace obličeje, tyto reprezentace dále uchovávat a využívat k porovnávání s matematickými reprezentacemi osob v databázi. Toto oprávnění nevyplývá ani z žádných dalších ustanovení zákona o Policii České republiky.

Směrnice v čl. 57 ukládá členským státům povinnost stanovit sankce za porušení předpisů přijatých na základě této směrnice a přijmout veškerá opatření nezbytná k zajištění jejich uplatňování. Sankce musí být účinné, přiměřené a odrazující. Zákon o zpracování osobních údajů provádí sankce v Hlavě VI Přestupky, kde je v § 63 odst. 1. písm. k) zákona o zpracování osobních údajů stanoveno, že právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s § 37 zákona o zpracování osobních údajů neprovede posouzení vlivu na ochranu osobních údajů. Podle § 63 odst. 3. zákona o zpracování osobních údajů lze za tento přestupek uložit pokutu do 10 000 000 Kč. Již dva roky (od listopadu 2021) prověřuje Úřad pro ochranu osobních údajů v souvislosti kamerovým systémem s biometrickou identifikací na Letišti Václava Havla podnět luRe, který se týká právě nedostatečného zákonného zmocnění a neprovedení posouzení vlivu na ochranu osobních údajů.

4.1.2 Další navrhované systémy biometrické identifikace „v reálném čase“

Podle vyjádření Úřadu pro ochranu osobních údajů mu byl v rámci konzultační činnosti sportovním klubem pořádající fotbalové zápasy předložen návrh na **využití technologie biometrické identifikace obličejů při vstupech na fotbalový stadion**. Navrhovaný systém měl mezi vstupujícími návštěvníky identifikovat osoby, které narušily průběh předchozích zápasů a byly po určitou dobu vyloučeny z návštěvy fotbalových utkání. Snadná identifikace měla pomoci zamezit nekontrolovanému vstupu těchto osob na fotbalové stadiony. V reakci na to v srpnu 2019 vydal Úřad pro ochranu osobních údajů stanovisko, podle kterého *"nelze najít dostatečný právní důvod ke zpracování biometrických osobních údajů návštěvníků fotbalového utkání technologií face recognition vlastníkem sportovního zařízení v postavení správce osobních údajů."*⁵¹ V odůvodnění pak uvedl, že zpracování biometrických údajů by vyžadovalo výslovné zákonné zmocnění, které musí být přiměřené sledovanému cíli. Úřad pro ochranu osobních údajů doporučil vyčkat novely zákona o podpoře sportu připravované ministerstvem vnitra.⁵² Následně se Úřad pro ochranu osobních údajů v březnu 2020 vyjádřil k navrhované novele zákona, která by uvedené zákonné zmocnění obsahovala. Návrh zákona úřad nepodpořil, protože v návrhu legislativních změn nebyla podle úřadu dostatečně zdůvodněna nezbytnost zpracování biometrických údajů ve srovnání s jinými možnostmi eliminace rizik násilí na stadionech.⁵³

Ze strany Policie České republiky proběhl pokus zavést biometrickou identifikaci dle obličeje „v reálném čase“ v **městském kamerovém systému hlavního města Prahy**.⁵⁴

⁵¹Úřad pro ochranu osobních údajů. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Stanovisko ze dne 16. srpna 2019. Dostupné z: <https://www.uoou.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541>

⁵²Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6107&n=vyrocní%2Dzprava%2Dza%2Drok%2D2019

⁵³Úřad pro ochranu osobních údajů. Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech. Zpráva ze dne 27. března 2020. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40780&n=vyjadreni%2Duou%2Dk%2Dnavrhu%2Dregulace%2Dnasili%2Dna%2Dfotbalovych%2Dstadionech

⁵⁴Česká televize. Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti. 2019. Dostupné z: <https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologie-na-rozpoznavani>

Na základě žádosti Policie České republiky o aktivaci funkcionality identifikace obličeje na šesti lokalitách městského kamerového systému v Praze se Magistrát hlavního města Prahy obrátil v listopadu 2019 na Úřad pro ochranu osobních údajů se žádostí o konzultaci.⁵⁵ Z důvodu nutnosti zpracování posouzení vlivu na ochranu osobních údajů dle § 37 zákona o zpracování osobních údajů byl další postup ze strany Magistrátu hlavního města Prahy přenechán Policii České republiky, která měla být současně zpracovatelem biometrických údajů získaných z pražského kamerového systému.⁵⁶ K dalším krokům ze strany policie následně nedošlo.

Ministerstvo vnitra ČR ve spolupráci s policií dále plánovalo nasazení kamerových systémů s biometrickou identifikací „v reálném čase“ na všech **dalších mezinárodních letištích v České republice: Brno, Ostrava, Pardubice a Karlovy Vary**.⁵⁷ Instalace těchto kamerových systémů měla být na zbývajících letištích dle plánu Ministerstva vnitra ČR realizována do konce roku 2020.⁵⁸ Nicméně od tohoto plánu bylo z dosud neupřesněných důvodů upuštěno. Podobně došlo ke krokům rozmístit kamerové systémy s biometrickou identifikací „v reálném čase“ na Pražském hradě a v pražském metru⁵⁹. Minimálně v případě Pražského hradu mělo jít opět o iniciativu Policie České republiky, která to doporučila Správě Pražského hradu v bezpečnostních reportech.⁶⁰

⁵⁵Úřad pro ochranu osobních údajů. Vyjádření k žádosti o konzultaci k městskému kamerovému systému hl. m. Prahy. Vyjádření ze dne 3. prosince 2019.

⁵⁶Poskytnutí informací na základě Žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 18. srpna 2020 vydané Odborem informatické infrastruktury Magistrátu hlavního města Praha pod číslem jednacím MHMP 1270148/2020.

⁵⁷Česká televize. Pražští policisté „otevírají diskusi“ o technologii na rozpoznávání obličejů. Hřib je proti. 2019. Dostupné z: <https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologie-na-rozpoznavani>

⁵⁸Ministerstvo vnitra České republiky. Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích. Tisková zpráva ze dne 18. února 2018. Dostupné z: <https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx>

⁵⁹Mareš M., Kleiner J., Zwiefelhofer T., Kasl F., Míšek J. Kamerový systém Dopravního podniku hlavního města Prahy v komparativním kontextu bezpečnosti a ochrany osobních údajů. 2021, studie zadaná Dopravním podnikem Hlavního města Prahy.

⁶⁰Česká Televize. Události, komentáře ze dne 17. dubna 2023. (čas 33:22) Dostupné z: <https://www.ceskatelevize.cz/porady/1096898594-udalosti-komentare/223411000370417/>

4.1.3 Informační systém Digitální podoba osob

Informační systém Digitální podoba osob představuje systém provozovaný Policií České republiky ke zpětné biometrické identifikaci na dálku. Informace o provozu systému zveřejnil spolek Iuridicum Remedium na základě informací získaných od policie díky zákonu o svobodném přístupu k informacím.⁶¹

Dodávku technologie biometrické identifikace včetně technické podpory zajistila česká společnost AUTOCONT a.s. Zkušební provoz systému probíhá od 22. srpna 2022 dodnes na základě interního pokynu policejního prezidenta,⁶² jehož přílohou jsou Zásady zkušebního provozu systému DPO, přičemž obsah tohoto pokynu policie z velké části odmítá zveřejnit. Systém je založen na zpětné identifikaci ze záznamu, což znamená, že nedochází k rozpoznávání osob v reálném čase. Účelem informačního systému je ztotožnění zájmové osoby důležité pro konkrétní trestní řízení (pachatele, svědka či poškozeného).

V rámci daného informačního systému dochází ke zpětnému 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 České republice a dle vyjádření Policejního prezidia se v červenci 2023 nacházelo v referenční databázi celkem 19 666 787 fotografií.⁶³ Systém by měl do 15 sekund poskytnout požadovaný počet jednoznačných identifikátorů fotografií osob, u nichž je nejvyšší míra shody se

⁶¹Tisková zpráva IuRe: Policie již téměř rok využívá analytický nástroj na rozpoznávání tváří. Podrobnosti jeho fungování tají. Dostupné z: <https://digitalnisvobody.cz/blog/2023/07/12/tz-policie-jiz-temer-rok-vyuziva-analyticky-nastroj-na-rozpoznavani-tvari-podrobnosti-jeho-fungovani-ale-pred-verejnosti-taji/>

⁶²Rozkaz Policejního prezidenta č. 194/2022, k zajištění zkušebního provozu informačního systému Digitální podoba osob.

⁶³Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 16. srpna 2023 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-35618-5/ČJ-2023-990810.

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

Do informačního systému má přístup celkem 73 osob, které jsou zařazeny na 3 útvech Policie České republiky, tedy Policejním prezidiu České republiky, Národní centrále proti organizovanému zločinu služby kriminální policie a vyšetřování a Národní centrále proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování. Jedná o 37 operačních důstojníků z důvodu zastupitelnosti a směnnosti služby, 7 osob zajišťujících technický provoz, zbývající osoby jsou pak příslušníci služby kriminální policie a vyšetřování. Ke dni 22. července 2023 bylo vyřízeno celkem 149 žádostí o využití funkce porovnání zaznamenané fotografie s celou referenční databází.⁶⁴

Policie považuje za zákonné oprávnění k provozu systému § 66a a § 79 zákona č. 273/2008 Sb., o Policii České republiky (blíže v kapitole 3.3 Právní úprava v České republice). Uvedená ustanovení, přijatá v roce 2019 novelou, ovšem dávají policii pouze oprávnění vytěžovat a následně zpracovávat digitální fotografie ze státních evidencí a zpracovávat osobní údaje za účelem vymáhání práva. Nicméně tato ustanovení přímo neuvádějí možnost biometrické identifikace, ani základní parametry a pravidla fungování a užití popsaného informačního systému. Policie pro informační systém zpracovala v roce 2023 posouzení vlivu na ochranu osobních údajů dle § 37 zákona č. 110/2019 Sb., o zpracování osobních údajů. Nicméně nebylo zpracováno souladně s díkčí čl. 27 Směrnice, který uvádí, že posouzení vlivu musí být zpracováno před započítáním zpracování. Zpracování však bylo započato již v srpnu 2022, tedy dříve, než bylo zpracováno posouzení vlivu na ochranu údajů. Policie poté vyhodnotila, že není nezbytná předchozí konzultace týkající se informačního systému s Úřadem pro ochranu

⁶⁴Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 16. srpna 2023 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-35618-5/ČJ-2023-990810.

osobních údajů, jak jí ukládá § 38 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

4.1.4 Další soukromé biometrické databáze

Mezi soukromými biometrickými databázemi je znepokojující především databáze fotografií společnosti Clearview AI, která obsahuje miliardy fotografií nashromážděných z různých veřejných zdrojů, včetně sociálních sítí Facebooku nebo Twitteru. Uvedená společnost tvrdí, že v budoucnosti bude schopná identifikovat téměř všechny obyvatele planety jen na základě fotografie nebo kamerového záznamu. Její služby využívají především bezpečnostní složky států. Evropský parlament ve svém usnesení ze dne 6. října 2020⁶⁵ označil databázi fotografií společnosti Clearview AI za ilegální a apeloval na členské státy, aby zakázaly svým bezpečnostním složkám tyto databáze při vyšetřování využívat. Policejní prezidium České republiky na dotaz autora této studie na základě zákona o svobodném přístupu k informacím sdělilo, že česká policie služby společnosti Clearview AI ani jiné soukromé biometrické databáze nepoužívá.

4.1.5 Zpětná biometrická identifikace softwarem EyeDentity

Policie v minulosti používala systém zpětné biometrické identifikace na dálku softwarem EyeDentity společnosti Eyedea Recognition. Jedná se o českou softwarovou firmu vyvíjející technologie zpracování obrazu pomocí umělé inteligence. Kromě biometrické identifikace dle obličeje tato společnost vyvíjí nástroje k automatickému čtení registračních značek vozidel, automatické klasifikaci vozidel dle modelu, automatické inspekci vnitřních prostor vozidel (použití pásu, užívání mobilního telefonu za jízdy nebo určování místa pohledu řidiče podle oční duhovky a zorničky).

⁶⁵Usnesení Evropského parlamentu ze dne 6. října 2021 o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech. Dostupné z: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_CS.html

Software na identifikaci dle obličeje společnosti Eyedea Recognition je využíván mimo jiné také Europolem⁶⁶ a francouzskými bezpečnostními složkami⁶⁷. Společnost mimo jiné poskytovala poradenské služby policii v letech 2016 až 2018 při zavádění biometrické identifikace na Letišti Václava Havla.

Uvedená společnost poskytla Krajskému ředitelství policie Ústeckého kraje software EyeDentity s licencí a technickou podporou na dva roky (od listopadu 2018 do listopadu 2020).⁶⁸ EyeDentity je počítačový software, který slouží k automatickému prohledávání digitálních obrazových dat za účelem lokalizace, kategorizace, identifikace a verifikace 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: 1) lokalizovat obličeje v rozsáhlých souborech videozáznamů a fotografií; 2) odhadovat věk a pohlaví zachycené osoby; 3) 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 a poznámky. V databázi osob jsou evidovány: jedna či více fotografií zájmové osoby, jméno, příjmení, datum a místo narození, rodné číslo, číslo občanského průkazu a další údaje osoby. Analytické jádro softwaru je založeno na algoritmech umělé inteligence. Aplikace obsahuje uživatelské rozhraní pro prohlížení databáze osob včetně filtrace, přidávání a odebírání záznamů a jejich editaci. Kromě toho také umožňuje hromadný import a export osob do databáze. Aplikace může pracovat s databází obsahující až několik tisíc osob.

⁶⁶IDnes. Česká firma pomáhá Europolu rozpoznat tváře zločinců a teroristů. Ze dne 7. července 2016. Dostupné z: https://www.idnes.cz/technet/software/eyedea-europol-rozpoznavani-obrazu.A160704_154924_software_pka

⁶⁷Magazín CIO Business World. Francouzská protiteroristická jednotka používá český software pro rozpoznávání obličeje. Ze dne 27. března 2018. Dostupné z: <https://www.cio.cz/aktuality/francouzska-protiteroristicka-jednotka-pouziva-cesky-software-pro-rozpoznavani-obliceje/>

⁶⁸Licenční smlouvy mezi Krajským ředitelstvím policie Ústeckého kraje a Eyedea Recognition s.r.o. uzavřené dne 20. listopadu 2018 a dne 19. listopadu 2019. Poskytnutí licence pro software EyeDentity. Číslo jednací objednávatele KRPU-209961-6/ČJ-2018-0400IT-02A a KRPU-167484-6/ČJ-2019-0400IT-03.

Podle vyjádření Krajského ředitelství policie Ústeckého kraje před používáním softwaru EyeDentity nebylo zpracováno posouzení vlivu na ochranu osobních údajů podle § 37 zákona č. 110/3019 Sb., o zpracování osobních údajů, ani nebylo zpracování softwarem konzultováno s Úřadem pro ochranu osobních údajů ve smyslu § 38 zákona č. 110/3019 Sb., o zpracování osobních údajů.⁶⁹ Povinnost zpracovat posouzení vlivu na ochranu osobních údajů se vztahuje také na využívání softwaru EyeDentity, protože je pravděpodobné, že zpracování biometrických údajů softwarem EyeDentity mohlo mít za následek vysoké riziko pro práva a svobody fyzických osob.⁷⁰ V souvislosti s tím, zda dané zpracování podléhá nebo nepodléhá vypracování posouzení vlivu na ochranu osobních údajů byl Úřadem pro ochranu osobních údajů vytvořen manuál.⁷¹ 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 s vysokým rizikem pro práva a svobody subjektů údajů, a s tím spojené povinnosti, 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 posouzení vlivu na ochranu údajů zpracovává. Uvedené zpracování softwarem EyeDentity dosahuje dle našeho hodnocení kritických hodnot minimálně ve třech kritériích.

Přestože byla licence softwaru EyeDentity zakoupena ještě před účinností zákona o zpracování osobních údajů, který tuto povinnost stanovil v národním právním řádu, byla zakoupena až po uplynutí implementační lhůty v čl. 63 odst. 1 Směrnice. Z uvedeného důvodu vznikla povinnost Krajskému ředitelství Ústeckého kraje řídit se Směrnicí již před schválením zákona č. 110/2019 Sb., o zpracování osobních údajů, a zpracovat

⁶⁹Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 11. září 2023 vydané Krajským ředitelstvím policie Ústeckého kraje pod číslem jednacími KRPU-160885-2/ČJ-2023-0400KR-PI.

⁷⁰Pattynová J., Suchánková L., Černý J., Růžicka M. a kol. Obecné nařízení o ochraně osobních údajů (GDPR) Zákon o zpracování osobních údajů. Komentář, 2. aktualizované vydání. Str. 630, 2019. Nakladatelství Leges, s.r.o. ISBN 978-80-7502-396-4.

⁷¹Úřad pro ochranu osobních údajů. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Verze 1.0. Manuál ze dne 8. ledna 2020. Dostupné z: <https://www.uoou.cz/seznam-druhu-operaci-zpracovani-ne-podlehajicich-pozadavku-na-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=1&p1=3938>

posouzení vlivu na ochranu osobních údajů. Navíc v listopadu 2019 byla Krajským ředitelstvím policie Ústeckého kraje zakoupena nová licence, již v době účinnosti zákona o zpracování osobních údajů. Tím se krajské ředitelství podle všeho dopustilo přestupku dle § 63 odst. 1. písm. k) zákona o zpracování osobních údajů, dle kterého právnická osoba se dopustí přestupku tím, že při zpracování osobních údajů v rozporu s § 37 zákona o zpracování osobních údajů neprovede posouzení vlivu na ochranu osobních údajů.

Problematická z hlediska zákona je také uživatelská praxe. Krajské ředitelství policie sdělilo, že software EyeDentity byl nainstalován na jednom počítači a měl k němu přístup pouze jeden policista, který byl zařazen na odboru analytiky a kybernetické kriminality Krajského ředitelství policie Ústeckého kraje. Software neprováděl logování činností, protože nebyl napojen na žádné evidence či informační systémy, a tudíž ani není zaevidováno, v kolika případech byl během licence software použit. Policista, který software EyeDentity obsluhoval, již prý není ve služebním poměru, tudíž informace, pro jak závažné případy a pro jaké procesní postavení osob byl software využíván, již nelze zjistit. Obecně užívání probíhalo tak, že dožadující policista dodal konkrétní fotografii zájmové osoby a zároveň množinu fotografií, se kterou měla být zájmová osoba porovnána.⁷² Popsaná praxe zpracování osobních údajů opět signalizuje, že se Krajské ředitelství policie Ústeckého kraje mohlo dopustit celé řady přestupků dle § 63 odst. 1 zákona o zpracování osobních údajů.

4.1.6 Biometrická autentizace

Policie České republiky dále využívá tzv. **mobilní inspekční biometrické systémy**, jejichž dodavatelem je česká společnost AUROTON COMPUTER, spol. s r.o. Jedná se o informační systém pro inspekci a kontrolu osob a dokladů pomocí biometrických prvků pro potřeby Policie České republiky. Uvedený biometrický systém neprovádí

⁷²Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 14. září 2023 vydané Krajským ředitelstvím policie Ústeckého kraje pod číslem jednacím KRPU-166623-2/ČJ-2023-0400KR-PI.

biometrickou identifikaci, ale pouze biometrickou autentizaci. Pokud probíhá kontrola totožnosti konkrétní fyzické osoby informační systém je schopený na základě na místě pořízené fotografie nebo odebraného otisku prstu kontrolované osoby ověřit její totožnost. Systém umožňuje mobilní kontrolu identity za využití biometrických prvků a prověření na výskyt v databázích Policie České republiky a ostatních bezpečnostních složek, členských států Evropské unie a mezinárodních organizací.⁷³ Uživatelská praxe těchto inspekčních systémů leží především na jednotlivých Krajských ředitelstvích Policie České republiky, do kterých směřovala dodávka technologických zařízení.

Další systém biometrické autentizace provozovaný Ředitelstvím služby cizinecké policie jsou **biometrické kontrolní brány na Letišti Václava Havla v Praze**.⁷⁴ Jedná se o systém biometrického odbavování cestujících, kteří jsou občané Evropské unie, Evropského hospodářského prostoru a Švýcarska, starší 15 let, a kteří létají mimo Schengenský prostor a vlastní pas s biometrickými údaji. Cestující vloží cestovní doklad do čtecího zařízení, kde proběhne kontrola dat, poté přistoupí k bráně a pohyblivá biometrická kamera ověří obličej. Na tento proces dohlíží policista, který na monitoru počítače sleduje cestujícího a ověření biometrických údajů z pasu. Pokud biometrické údaje pořízené kamerou a uložené v cestovním pasu souhlasí, otevřou se vstupní dveře brány a cestující může překročit hranici.

4.2 Analýza obrazu

Umělá inteligence má pro analýzu obrazu a videozáznamů, krom biometrie obličeje, v policejní praxi mnohem širší uplatnění. Může se jednat o nové „chytré“ funkce, kterými jsou vybaveny dohledové kamerové systémy. Mezi takové funkce patří zejména detekce pohybu a nestandardního chování (například jízda vozidla do protisměru),

⁷³Kupní smlouva mezi Českou republikou - Ministerstvem vnitra a společností AUROTON COMPUTER, spol. s r.o. uzavřená dne 22. prosince 2016 uzavřená na základě a v souladu s výsledky veřejné zakázky „Vybudování mobilního biometrického inspekčního systému a dodávka kontrolních zařízení“. Číslo jednací objednatele PPR-22247-26/ČJ-2016-990656.

⁷⁴Policie České republiky. eGATE - rychlejší odbavování na letišti. Zpráva ze dne 23. července 2015. Dostupné z: <https://www.policie.cz/clanek/egate-rychlejsi-odbavovani-na-letisti.aspx>

detekce a klasifikace různých objektů v obraze (například závadové symboly či loga) nebo detekce a čtení registračních značek vozidel. Uvedené funkce lze využít jak na živém kamerovém přenosu, tak na prohlédávání dlouhých sekvencí videozáznamů. Ze záznamů lze pak dále automatizovaně vytvářet synopse (například časová souslednost průchodu osob určitým místem v průběhu dlouhého časového úseku) nebo záznamy odšumovat či jinak vylepšovat rozlišení nekvalitního záznamu. Krom použití uvedených funkcí na záznamech z kamerových systémů lze podobně pracovat s otevřenými zdroji na internetu. Umělá inteligence tak nachází uplatnění při obrazové forenzní analýze internetových médií, blogů, sociálních sítích nebo streamovacích kanálů. Zmíněné příklady využití analýzy obrazu uvádí Policie České republiky jako oblast svého zájmu v oblasti umělé inteligence.

Systémy umělé inteligence pro analýzu obrazu se již běžně používají v kamerových systémech s funkcí **automatického čtení registračních značek** a dalších indikátorů motorových vozidel. Registrační značka motorového vozidla představuje osobní údaj, tedy informaci, která vede v řadě případů k identifikaci fyzické osoby. Z tohoto důvodu je automatické čtení registračních značek také pokryto právními předpisy na ochranu osobních údajů, byť často k tomuto údaji není jako k osobnímu přistupováno.

Na zpracovávání v podobě automatického čtení registračních značek vozidel ze strany Policie ČR může být aplikován souběžně dvojí právní režim: GDPR a Směrnice. Policie České republiky vykonává pravomoci ve věcech provozu na pozemních komunikacích, což spadá obvykle pod GDPR, ale zpracování údajů o dopravním provozu může sloužit k vyšetřování trestných činů nebo zajišťování bezpečnosti, což již spadá pod Směrnici. Kamerové systémy se čtením poznávacích značek jsou často provozovány obcemi a obecními policiemi, na které se vztahuje regulace dle GDPR. Obecní policie pak údaje ze svých systémů předávají Policii České republiky, což problém relevantní právní úpravy může ještě více komplikovat. Vlastní síť kamer s automatickým čtením registračních značek vozidel provozuje Policie České republiky jako informační systém Centrální

automatická kontrola vozidel.⁷⁵ Kamery systému jsou rozmístěny kolem silnic v různých uzlových bodech. Přesný počet kamer není znám, ale může se odhadovat na tisíce, přičemž jejich počet neustále narůstá. Kamery zachycují každý projíždějící automobil bez ohledu na to, zda se řidič dopouští nějakého přestupku. V CAKV jsou zpracovávány údaje v rozsahu fotografie, výřez fotografie s tabulkou registrační značky, registrační značka vozidla v textové podobě, mezinárodní poznávací značka v textové podobě, datum a čas výskytu vozidla, místo výskytu vozidla označené směrem jízdy vozidla a názvem pozemní komunikace, jedinečný identifikátor zdrojové kamery včetně její GPS souřadnice, identifikace vlastníka, typu kamery (mobilní, stacionární) a příslušnosti ke skupině kamer. Velká přehledová fotografie je pořizována pouze některými kamerami s ohledem na jejich technické možnosti. Záznamy v CAKV se uchovávají po dobu 1 roku od jejich vložení do systému CAKV, s výjimkou velké přehledové fotografie, která je v CAKV uchovávána po dobu 6 měsíců od jejího vložení. Tato uschovací doba je stanovena jako nejvýše možná a může být s ohledem na technickou kapacitu zkrácena.⁷⁶

Významným kamerovým systémem s automatickým čtením registračních značek vozidel, ze kterého mohou být předávány údaje policii, je systém elektronických dálničních známek. Systém zřizovaný Ministerstvem dopravy snímá registrační značky vozidel na dálnicích a porovnává je se seznamem zakoupených elektronických dálničních známek. Kamerový systém je v této podobě spuštěn od ledna 2021.

Kamerové systémy s automatickým čtením registračních značek vozidel, které se zavádějí na úrovni městských samospráv, mají mnohdy řadu dalších funkcí využívající analýzu obrazu. Z obrazu projíždějících aut rozpoznají nejen registrační značky, ale detekují také směr jízdy (např. do protisměru), barvu vozidla, výrobce a model vozidla.

⁷⁵ Policie České republiky. Automatická kontrola vozidel. Zveřejněná informace ze dne 11. listopadu 2022. Dostupné z: <https://www.policie.cz/clanek/zverejnene-informace-2022-automacka-kontrola-vozidel.aspx>

⁷⁶ Policie České republiky. Systém Centrální automatická kontrola vozidel. Zveřejněná informace ze dne 18. 9. 2023. Dostupné z: <https://www.policie.cz/clanek/system-centralni-automacka-kontrola-vozidel.aspx>

Systémy, které jsou dnes komerčně nabízené, pak mohou propojovat detekovaná data s daty z dalších databází.⁷⁷

Policie České republiky využívá v oblasti automatického čtení poznávacích značek pokročilé softwarové systémy dvou společností. První z nich je softwarová společnost BriefCam. Jedná se o americkou softwarovou společnost zabývající se analýzou obrazu pomocí umělé inteligence a hlubokého učení. Ministerstvo vnitra nakoupilo v lednu 2022 licenci k softwaru pro analýzu videa **BriefCam Investigátor**. Uvedený software pro analýzu videa je použitelný pro široké spektrum formátů videa. Umožňuje celou řadu funkcionalit mezi nimiž jsou: vytvoření videosynopse, přímý přechod od videosynopse do původního videa, provedení analytických funkcí pouze ve vybrané oblasti ve scéně, automatická detekce a rozpoznání lidského obličeje, automatická detekce a rozpoznání registračních značek vozidel, automatická detekce objektů ve videu a jejich trasování, klasifikace objektů (osoby, oblečení, vozidla, zvířata), detekce pohybu, detekce překročení linie, detekce vstupu do zájmové oblasti a opuštění zájmové oblasti, filtrace dle barvy, velikosti, rychlosti, směru a trajektorie pohybu, doby výskytu objektu ve scéně, nebo vyhledání podobných objektů. Od stejné společnosti nakoupilo Krajské ředitelství policie Ústeckého kraje další analytický software pro analýzu videozáznamu s názvem **Briefcam Syndex FS**. Tento software má funkcionality, jako jsou videosynopse, rozpoznání objektů, časová indexace a další.

Další společnost pro analýzu videa, jejíž produkty používá Policie České republiky, je česká softwarová společnost CertiCon a.s. Krajské ředitelství policie Moravskoslezského kraje používá od roku 2017 její software pro analýzu videa **CertiConVis**, od něhož si pořídila jednu serverovou licenci a pět klientů. CertiConVis je software určený pro analýzu obrazu. Uživatel si v něm nadefinuje objekty a jejich chování, které chce pomocí kamerových systému detekovat. Jakmile pak ve scéně nastane nadefinovaný úkon (např. odbočení vozidla do protisměru nebo nepovolený

⁷⁷Tři česká města testují chytré kamery, které rozpoznají SPZ, barvu a výrobce vozidla. 2019. Dostupné z: <https://www.systemonline.cz/zpravy/tri-ceska-mesta-testuji-chytre-kamery-ktere-rozpoznaji-spz-barvu-a-vyrobce-vozidla-z.htm>

vstup osoby do zakázané zóny) software uživatele automaticky upozorní. Definovat lze objekty a jejich chování, zóny vstupu, směry pohybu, apod. Analýza může probíhat jak v reálném čase, tak ze záznamu. V druhém případě pak systém automaticky zobrazí zpětně veškeré uživatelem definované momenty v průběhu vybraného časového období. Mezi funkce systému patří detekce a rozpoznávání objektů, analýza chování osob, detekce zneužití (zakrytí) kamery, počítání objektů a statistiky, slučování událostí ze záznamu, detekce podezřelého vniknutí, analýzy dopravní situace, detekce kriminality a nehod.

Systém CertiConVis je také od roku 2018 využíván pro zvýšení bezpečnosti na Letišti Václava Havla. Systém byl integrován do tehdejšího kamerového systému, který čítá 1600 bezpečnostních kamer umístěných v rámci celého areálu letiště. Systém CertiConVis naráz analyzuje obraz ze 150 kamer. Využívají se různé video-analytické funkce pro sledování letištního prostoru. Mezi ty patří například spuštění alarmu v případě protisměrného pohybu v jednosměrných prostorách, detekce pohybu osob v prostoru vyhrazeném pro vozidla, detekce narušení perimetru, detekce odloženého zavazadla či výskytu osob u personálních vchodů a vstupů do strategických místností.

4.3 Analýza audio

Široké uplatnění má pro policii také analýza zvukového záznamu systémy umělé inteligence. Česká policie uvádí v tomto ohledu zájem o celou řadu funkcí. Jedná se jak o nástroje běžně dostupné veřejnosti, které nezpracovávají osobní údaje, tak nástroje, které zpracovávají citlivá osobní data. Z běžných funkcí se jedná o převádění mluveného slova do textu, převádění textu do mluveného slova nebo automatické překládání. Méně běžné funkce, které jsou pro policii zájmové, představují odšumování a zašumování nahrávek, určování kdo a kdy na nahrávce mluví (tzv. diarizace), identifikace užitého jazyka v nahrávce nebo funkce aktivující zařízení při vyslovení určitého klíčového slova. Mezi funkce zpracovávající osobní údaje, a které policie

považuje za zájmové, patří identifikace mluvčího, určení pohlaví mluvčího a dále pak emoční analýza na základě hlasu.

Ačkoliv některé funkce nejsou přímo využity ke zpracování osobních údajů, mohou mít zásadní vliv na míru plošného sledování, díky zrychlení a automatizaci zpracování dlouhých hodin hlasových záznamů. Tím může narůstat poptávka po pořizování stále většího množství zvukových záznamů, které by pomocí běžných metod nebylo možné zpracovat. Česká policie počítá s využitím analýzy zvukových záznamů nejen při zpracovávání odposlechů telefonních hovorů, prostorových odposlechů, nahrávek výslechů a tísňového volání, ale také nahrávek získaných z otevřených zdrojů, jako jsou média, sociální sítě a různé podcasty.

V oblasti analýzy zvukových záznamů pomocí systémů umělé inteligence spolupracuje Policie České republiky se společností Phonexia s.r.o. Jedná se o českou softwarovou společnost, která se zabývá řečovou a hlasovou biometrií. Dle smlouvy s Ministerstvem vnitra ČR dodala v prosinci 2022 Kriminalistickému ústavu Policie České republiky software **Phonexia Voice Inspector** s licencí na 20 let a technickou podporou na jeden rok. Phonexia Voice Inspector je počítačový program pro identifikaci mluvčího na základě hlasu s následujícími funkcemi: automatická identifikace mluvčích, automatické označování mluvčích (diarizace), vytváření databáze mluvčích, segmentace řeči, porovnání signálů, detekce řeči a zvuků.

Analýza zvuku se již nasazuje také na veřejných prostranstvích, kdy se do veřejného prostoru instalují mikrofony a zvuky jsou následně analyzovány. Algoritmy pro detekci zvukových událostí jsou schopné detekovat situace, jako jsou křik, střelba nebo tříštění skla v reálném čase a vyslat upozornění do operačního střediska a také automaticky otáčet kamery směrem k původu podezřelého zvuku. Příkladem takového programu je **Sound Event Detector** české společnosti Jalud Embedded s.r.o., který je nasazený od dubna 2022 v Plzni. Softwarové řešení Sound Event Detector využívá techniky strojového učení s architekturou hlubokých neuronových sítí. V současné době je 53 analyzovaných mikrofونů nainstalovaných v Plzni jako součást městského

kamerového systému městské policie, dalších 10 mikrofonů je pak ve Fakultní nemocnici Plzeň. Další podobné instalace jsou připravovány v Dubí, České Lípě, Ostravě a Písku.⁷⁸

4.4 Analýza textu

Analýza textu pomocí systémů umělé inteligence má pro Policii České republiky široké využití. Česká policie jako oblast svého zájmu uvádí celou řadu funkcí: fulltextové vyhledávání, klasifikaci a kategorizaci dokumentů, sémantickou analýzu, emoční analýzu textu, vytváření souhrnů z rozsáhlých složek, hledání klíčových elementů v textu (jména, adresy, místa, značky atd.) a následné hledání spojení mezi nimi (tzv. *named entity recognition*). Využití těchto nástrojů má význam nejen pro analýzu úředních záznamů a celých vyšetřovacích spisů (včetně těch poskytnutých v rámci mezinárodní justiční spolupráce), ale také otevřených zdrojů, jako jsou média, weby, blogy nebo sociální sítě. Tyto funkce opět pomáhají zrychlovat a automatizovat některé úkony vyšetřování, takže opět umožňují monitoring mnohem většího obsahu, než bylo možné v minulosti.

4.5 Analýza zločinnosti

Další analýzou pomocí systémů umělé inteligence pro účely policie je zpracování různých druhů dat o zločinnosti. V zásadě se jedná o kategorii, která nespadá do žádné z předchozích oblastí analýzy, případně je vzájemně kombinuje. Česká policie uvádí jako oblast svého zájmu v těchto druzích analýz především systémy předpovědi zločinnosti v krátkodobých (v rádech dnů) a dlouhodobých (trendy v rádech let) obdobích, dále pak systémy na detekci sériových zločinů na základě podobného *modu operandi* pachatele,

⁷⁸Novinky.cz. Inteligentní kamery vidí i slyší. Chytré technologie mění česká města. Zpráva ze dne 12. listopadu 2023. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-inteligentni-kamery-vidi-i-slysi-chytre-technologie-meni-ceska-mesta-40450506>

systemy detekce kybernetických zločinů, analýzu zachycených dat a dále pak systém profilování poštovních zásilek, v neposlední řadě pak také systém profilování dat o pasažérech leteckých společností.

Mezi systémy umělé inteligence pro analýzu zločinnosti lze zařadit nástroje Policie České republiky dodané firmou Risk Analysis Consultants zaměřující se na distribuci **software pro digitální forenzní analýzu a kryptoanalýzu**. Používané programy lze rozdělit do dvou kategorií. První pomocí algoritmů analyzují velké objemy digitálních dat a hledají v nich obsah s určitou tematikou (například zbraně, drogy) a ty druhé slouží k prolamování hesel. Do první kategorie patří software EnCase a Magnet Axiom. Pro EnCase nakoupilo policejní prezidium téměř čtyřicet licencí, pro Magnet Axiom dvacet. Magnet Axiom mají k dispozici také Krajská ředitelství policie v Jihočeském a Ústeckém kraji, EnCase potom využívá Krajské ředitelství policie v Praze. Uvedený software je schopný zjišťovat informace z registrů systému Windows, vytahovat data z profilů na sociálních sítích či obnovovat nepřepsaná smazaná data na pevném disku. Slouží hlavně k tomu, aby se vyšetřovatel snáze zorientoval a nemusel pracně procházet všechna data a programy. Mezi nástroje pro dešifrování obsahu používané různými složkami policie patří softwarové nástroje Tableau Password Recovery, Forensic Toolkit, Passware Kit nebo Cellebrite. Z nich je více známo o softwaru Cellebrite, který umí prolomit zabezpečení prakticky každého mobilního telefonu.

Jedním ze systémů umělé inteligence používaný k analýze zločinnosti je **systém Reliéf**. Jedná se o databázi stop sesbíraných v rámci protidrogové činnosti vytvořený Národní protidrogovou centrálou a Kriminalistickým ústavem v Praze.⁷⁹ Software pro policii vytvořila společnost Eyedea Recognition a je v současnosti využíván také Interpolem, který doporučil systém pro všechny členské státy v roce 2016. Cílem systému Reliéf je vytvoření unikátní mezinárodní sbírky všech využitelných relevantních informací získaných ze zkoumání kriminalistických stop na zásilkách drog. Systém Reliéf využívá kombinaci různých metod vedoucích k individuální identifikaci

⁷⁹Policie České republiky. Interpol doporučil databázi Reliéf. Zpráva ze dne 23. května 2016. Dostupné z: <https://www.policie.cz/clanek/interpol-doporucil-databazi-relief.aspx>

zásilek drog. Metody identifikace drogových zásilek probíhá automatickým - na umělé inteligenci založeným - srovnáváním stop, jako jsou chemické profily, loga a stopy po použití nástrojů a taktické informace, které se týkají zabavených zásilek drog. Systém Reliéf tudíž kombinuje různé druhy analýz umělé inteligence (textu a obrazu). Není známo, že by v uvedeném systému docházelo ke zpracování osobních údajů.

Dalším systémem umělé inteligence používaným k analýze zločinnosti jsou tzv. **Mapy budoucnosti**, které v podstatě představují mapový systém předpovídající zločinnost na základě geografického umístění. Jedná se o aktivitu policie a ministerstva vnitra, která byla silně inspirována zahraničními pre-crime projekty připomínajícími známé sci-fi Minority Report. Vyjádření v oficiálních výstupech Ministerstva vnitra může vyznívat problematicky, například: „*pachatel dopaden dřív než zločin spáchal*“. To samo o sobě může vyvolávat právní a etické pochybnosti o právu na spravedlivý proces. Nicméně pokud v tomto plošném monitorovacím systému nejsou zpracovávána osobní data občanů, nemusí se jednat ze zásady o problematickou aktivitu.

Ministerstvo vnitra České republiky realizovalo celkem dva projekty pod označením Mapy budoucnosti. První z nich realizovaný v letech 2014 až 2015 se zaměřoval především na vyhodnocení možných přístupů k predikci kriminality v českých podmínkách. V rámci projektu vznikla mezinárodní srovnávací studie týkající se mapování, analýzy a predikce kriminality, a dále proběhly mezinárodní workshopy policejních orgánů. Následující projekt - Mapy budoucnosti II - byl realizován v letech 2019 až 2022. Druhý projekt měl za cíl využít prostorová data o kriminalitě k vytvoření a otestování nástrojů a postupů pro mapování, analýzu a predikci kriminality.

Na základě především druhého z projektů vznikly statistické a datové výstupy na třech úrovních: 1) pro veřejnost, 2) pro obce a obecní policie a 3) pro potřeby Policie České republiky. Veřejnou část představuje především datový portál Mapa kriminality,⁸⁰ kde lze dohledat časová a prostorová data o kriminalitě na celém území České republiky.

⁸⁰Zmíněný web pro veřejnost je možné nalézt na webové stránce: <https://kriminalita.policie.cz/>

Nejproblematictější částí by mohla být část určená pro potřeby Policie České republiky, která obsahuje tzv. **funkcionalitu predikce kriminality**. Tato funkce založená na strojovém učení vrací pro zadané vstupní hodnoty požadovaný výsledek. Je trénována z historických dat za minulá období pomocí algoritmu boostované rozhodovací stromy (knihovna XGBoost). Funkcionalita je implementována do mapové aplikace tak, že dochází k vizualizaci čtverců (100 x 100 metrů), u kterých si predikční model myslí, že v nich pro daný den dojde ke zvýšenému riziku trestné činnosti. Predikce jsou vytvářeny jen pro některé druhy majetkové trestné činnosti. Čtverce jsou ohodnoceny tak, aby bylo patrné, kde je riziko vyšší nebo nižší. Uživatel jednoduše vybere zájmovou obec a datum predikce.

Podle dostupných informací funkcionalita predikce kriminality nepracuje s osobními údaji, ale proměnnými pro analýzu jsou kriminalistická, geografická, časová a další data. Celkem se jedná o 236 proměnných, které jsou charakteristické pro každý čtverec predikčního modelu. Mezi data využívaná pro funkcionalitu predikce patří kriminalistická data (počet vybraných deliktů, jejich čas a místo v minulosti pro daný čtverec), geografické data pro každý čtverec (rozloha různých druhů využití území, délky silničních komunikací, počty různých druhů objektů), počasí, dny v měsíci a týdnu a podobně. Lze tedy dojít k závěru, že současný softwarový nástroj nepředstavuje zásadní riziko pro práva osob. Nicméně predikční model pracuje s informacemi jako počet sociálně vyloučených lokalit nebo počet různých druhů služeb v daném čtverci. Tudíž by bylo vhodné ověřit, jakým způsobem pracuje policie s tímto softwarovým nástrojem, a zda například na základě výstupů predikčního modelu nepodstupují osoby v sociálně vyloučených lokalitách ponižující kontroly, což by představovalo diskriminační zásah. To ovšem záleží na policejní praxi, která se může v závislosti na lokalitě měnit. Rizikem do budoucna by mohlo být rozšíření analyzovaných proměnných o osobní údaje nebo propojení s dalšími systémy policie, které osobní údaje zpracovávají.

5. Výzkum a vývoj

"Na začátku aktivit odboru prevence kriminality Ministerstva vnitra v oblasti mapování, analýz a predikce kriminality stála inspirace pocházející především ze Spojených států amerických, kdy nás zaujala videa z Los Angeles a dalších měst na západním pobřeží USA, která více než policejní práci, na kterou jsme zvyklí, připomínala sci-fi filmy typu Minority Report."

Michal Barbořík, odbor bezpečnostní politiky a prevence kriminality Ministerstva vnitra ČR

Vývoj policejních systémů umělé inteligence je financován z veřejných rozpočtů České republiky. Financují se takto i projekty vyvíjející aplikace, jejichž nasazení v České republice a celé Evropské unii by nesplňovalo zákonné požadavky stanovené ve Směrnici a GDPR. Tyto projekty jsou financovány zejména skrze Technologickou agenturu České republiky a Bezpečnostní výzkum Ministerstva vnitra České republiky. Minimálně 39 výzkumných projektů tohoto typu bylo v posledních letech podpořeno státní podporou ve výši více než 450,6 milionů Kč. Konkrétně se jedná o 36 projektů se státní podporou ve výši 425 245 000 Kč z Bezpečnostního výzkumu Ministerstva vnitra ČR a tři projekty se státní podporou ve výši 25 377 000 Kč z Technologické agentury ČR. Jejich seznam a základní popis je uveden v tabulce 3.

U aplikací, které výzkumem vznikly, nelze na základě dostupných zdrojů ověřit jejich praktickou použitelnost pro policejní praxi ani možné riziko zásahu do práv občanů, protože oficiální hodnocení výstupů projektů probíhá spíše formalisticky. Je možné, že některé výstupy v podobě aplikací představují systémy umělé inteligence schopné plošného sledování s vysokým rizikem do práv občanů. U jiných systémů umělé inteligence se naopak může jednat o nástroje s velmi omezeným využitím nebo o nástroje, které svým samotným účelem nepředstavují vysoké riziko.

V oblasti biometrie se výzkum zaměřoval na vývoj různorodých aplikací schopných identifikace na základě celé řady fyziologických charakteristik: biometrie obličeje,

chůze a hlas. Byly vyvinuty aplikace pro biometrickou identifikaci dle obličeje z dronových záběrů nebo pro vyhledávání osob v rozsáhlých videosekvencích a data setech fotografií, dále aplikace pro biometrickou identifikaci dle hlasu v telefonních záznamech, a také aplikace pro analýzu ručně psaného písma. V oblasti behaviorální biometrie byly vyvinuty nástroje k emoční analýze řečového a obrazového signálu nebo hodnocení zdravotního stavu řečníka. Výzkum obrazového záznamu pak měl za cíl vytvoření aplikací pro automatické detekce přestupků, rozpoznávání modelů vozidel či čtení registračních značek vozidel. Dále si nechala policie vyvinout nástroj pro algoritmické určování podezřelých poštovních zásilek, predikci výskytu hledaných osob a predikce chování osob překračujících vnější hranice Evropské unie, stylometrické určování autorství anonymních textů v prostředí internetu nebo odstranění šumu nebo zašumění řečové nahrávky. V oblasti analýzy sítí byl vyvinut nástroj využívající behaviorální analýzu pro detekci kybernetických útočníků nebo nástroj pro detekci provozu sítě TOR.

Hlavním nedostatkem a rizikem bezpečnostního výzkumu a vývoje systémů umělé inteligence je skutečnost, že neprobíhá před realizací projektu posouzení vlivu na ochranu osobních údajů předpokládaných výsledků daného projektu. Podpořeny byly již projekty vyvíjející aplikace, které jsou určeny pro nasazení v České republice, ale jejichž použití se následně ukáže jako neslučitelné s právní úpravou ochrany osobních dat. Příkladem může být projekt na vývoj automatizovaného panoramatického dohledového systému pro ochranu osob a majetku na sportovních stadionech, jehož realizace byla pro období let 2017 až 2020 podpořena ze státního rozpočtu Ministerstvem vnitra ČR částkou více než 16 milionů Kč. V hlavních cílech projektu bylo uvedeno: *"Tyto metody umožní detekci a rozpoznání osob podle obličejů nebo oblečení v případě maskování, jejich sledování v davu a vyhledávání jejich pozice v rozsáhlých záznamech."*⁸¹ Právě uvedený projekt měl vyvíjet funkci identifikace dle obličeje osob

⁸¹Technologická agentura České republiky. Automatizovaný panoramatický dohledový systém pro ochranu osob a majetku na sportovních stadionech. Dostupné z: https://starfos.tacr.cz/cs/project/VI20172020105?query_code=q4piaacjw5tq#project-main

na fotbalovém stadionu, což by dle stanoviska Úřadu pro ochranu osobních údajů⁸² bylo v rozporu s platnou legislativou na ochranu osobních údajů. Popsaný příklad, kdy je nejprve financován projekt v řádech milionů korun a následně je zjištěno, že užití jeho výsledků není právně aprobováno, by mohlo vést k postupné erozi a rozvolňování současné právní regulace, protože může docházet ke snahám výsledky nějakým způsobem uplatnit v praxi.

Dalším negativním efektem financování projektů systémů umělé inteligence a biometrické identifikace ze státního rozpočtu je nepřímá podpora vlád nedemokratických režimů, kde nejsou funkční mechanismy ochrany lidských práv, a kde mohou být systémy umělé inteligence zneužívány k potírání politické opozice. Může to být další krok, který následuje, pokud je nemožné využít výsledky aplikovaného výzkumu systémů umělé inteligence přímo v České republice nebo ve státech Evropské unie. Napovídá tomu další příklad, kdy proudí státní finanční podpora na *"výzkum a vývoj nových modulů umělé inteligence pro sledování a detekci anomálií a predikci chování osob."*⁸³ V dubnu 2020 na projekt vývoje popsaného softwaru pod názvem Cogniware Insights 2.0 dostala společnost Cogniware, s.r.o. státní dotaci ve výši více než 16,5 miliónu korun.⁸⁴ Výsledky vývoje byly zaměřeny *"na vyšetřování a pokročilou analýzu podezřelých objektů, aktivit a vztahů s využitím prvků umělé inteligence a statistických analýz, která patří do oblasti známé jako analýza Big Data. Řešení bude obsahovat detekci anomálií, modulu pro klasifikaci objektů do skupin dle příbuznosti, predikci chování, rozpoznávání osob a objektů z obrazu a bude doporučovat vhodné postupy a prioritizace."*⁸⁵ Cogniware Insights 2.0 tak dostal státní dotaci na nástroj k propojování dat získaných z kamerových systémů včetně biometrických dat s osobními

⁸²Úřad pro ochranu osobních údajů. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Stanovisko ze dne 16. srpna 2019. Dostupné z: <https://www.uoou.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541>

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

⁸⁴Smlouva o poskytnutí podpory mezi Česká republika – Technologická agentura České republiky a Cogniware, s.r.o. k projektu č. FW01010562 s názvem Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob.

⁸⁵Technologická agentura České republiky. Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob. Dostupné z: https://starfos.tacr.cz/cs/project/FW01010562?query_code=q4piaacjw5tq

daty získanými z jiných zdrojů, jako například sociální sítě. Analýzou dat má pak uvedený systém na základě algoritmu strojového učení vyhodnotit, jaký postup zvolit v případě zjištění podezřelého chování monitorované osoby.

Podle vyjádření samotné společnosti Cogniware s.r.o. dodávají systémy využívající popsané technologie silovým složkám zemí Středního východu, zejména do Spojených arabských emirátů, Saúdské Arábie, Jordánska nebo Bahrajnu. Společnost to odůvodňuje právě tím, že *"tyto státy mají volnější pravidla, co se ochrany osobních údajů týče."*⁸⁶ V uvedených státech vládou nedemokratické autoritářské režimy a hrozí v nich zneužití sledovacího systému k potlačování politické plurality a k potlačování lidských práv. Dle vyjádření společnosti, lze u vyvíjeného sledovacího systému různě upravit funkce, aby se přizpůsobil právní úpravě v jednotlivých zemích. Ačkoli cílem společnosti je dodávat v budoucnu tyto systémy také Policii České republiky,⁸⁷ faktem je, že z českého státního rozpočtu se financuje vývoj sledovacího systému, který není plně kompatibilní s evropským právem a systémem ochrany osobních údajů, případně bude muset pro potřeby České republiky doznat dalších úprav.

⁸⁶Cogniware. Umělá inteligence z Česka pomáhá chytat zločince po celém světě. Tisková zpráva společnosti Cogniware ze dne 3. září 2020.

⁸⁷Hlaváčová K. Stačí oči a kousek nosu či chůze. Česká kamera rozpozná člověka i konkrétní auto. 2020. Dostupné z: <https://zpravy.aktualne.cz/domaci/staci-oci-a-kousek-nosu-ci-chuze-cesky-kamery-system-pozna/r~0db5c8b2ee8c11eaa6f6ac1f6b220ee8/>

Tabulka 3: Výčet výzkumných projektů podpořených z veřejných financí, které využívají umělou inteligenci pro potřeby veřejné bezpečnosti, zejména policejních orgánů.

Název projektu				
Identifikátor	Doba řešení	Dotace	Účastníci projektu	Poskytovatel
Krátký popis projektu				
Překlenutí jazykové bariéry, komplikující vyšetřování financování terorismu a závažné finanční kriminality				
VD20072010B1 6	1. 8. 2007 - 31. 12. 2010	Statní podpora 12 100 000 Kč	- Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií - Vysoké učení technické v Brně, Fakulta informačních technologií - Západočeská univerzita v Plzni	Ministerstvo vnitra
Cílem projektu aplikovaného výzkumu bylo vytvoření rozsáhlé databáze telefonních nahrávek, nástrojů pro vyhledávání klíčových slov v nahrávkách, rozpoznávání telefonní řeči, rozpoznávání řečníka v telefonní řeči a rozpoznávání jazyka v telefonní řeči. Výsledkem projektu jsou mimo jiné také programy pro detekci klíčových slov, identifikaci mluvčího, přepis řeči na text a identifikaci jazyka.				
Prostředky pro identifikaci obrazového záznamového zařízení, autentifikaci a rekonstrukci obrazu - PIZZARO				
VG2010201306 4	1. 10. 2010 - 30. 9. 2013	Statní podpora 8 773 000 Kč	- Policie ČR Kriminalistický ústav - Ústav teorie informace a automatizace AV ČR, v. v. i.	Ministerstvo vnitra
Cílem výzkumného projektu je softwarová aplikace sestávající se z identifikačního, autentizačního a rekonstrukčního modulu. Výsledkem výzkumného projektu je softwarová aplikace pro podporu identifikace digitálních fotoaparátů a kamer (či jiných snímacích zařízení) a následné ověření pravosti zachycených video a foto snímků (a jejich případné modifikace) a dále pak rekonstrukce zachycené obrazové informace (pokud není dostatečné kvality pro vynesení úsudku o tom, co se na scéně děje, kdo je na ní zachycen apod.). Algoritmy jsou upraveny pro použití v kriminalistické praxi.				

Zvyšování účinnosti zabezpečení rizikových prostor kombinovanými metodami biometrické identifikace osob

VG2010201403 3	1. 09. 2010 - 31. 8. 2014	Statní podpora 19 670 000 Kč	- JIMI CZ, a.s. - Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií	Ministerstvo vnitra
-------------------	------------------------------	---------------------------------------	---	------------------------

Cílem projektu je začlenění kombinovaných biometrických metod do stávající struktury kamerových systémů pro zabezpečení veřejných i soukromých prostor. Takto zdokonalené systémy pak pomocí implementovaných metod automatické identifikace osob dle obličeje, hlasu, postavy a pohybu, a dalších biometrických prvků povedou ke snazšímu odhalení potenciálních hrozeb. Součástí produktů budou rovněž metody emoční analýzy řečového i obrazového signálu sloužící k preventivnímu vyhledání agresivních osob. Výstupem projektu je několik softwarových nástrojů (analýza řečového signálu v reálném čase, systém biometrické identifikace obličeje, řeči a chůze, hodnocení zdravotního stavu řečníka) a také prototyp dohledového kamerového systému s integrovanými moduly pro analýzu zvukového a obrazového signálu.

Portrétní identifikace jedinců ve věkovém rozpětí od 1 roku do 18 let

VD20102010B2 2	1. 2. 2010 - 31. 12. 2010	Statní podpora 1 154 000 Kč	- MTMP s.r.o.	Ministerstvo vnitra
-------------------	------------------------------	-----------------------------------	---------------	------------------------

Projekt byl zaměřen na vytvoření softwarové aplikace využitelné při portrétní identifikaci nedospělých jedinců v kriminalistice, která umožňuje morfometrické srovnání vlastností obličeje, věkové přizpůsobení portrétní fotografie a sestavení portréту.

Analýza přirozeného jazyka v prostředí internetu

VF2010201400 3	1. 10. 2010 - 31. 12. 2014	Statní podpora 7 430 000 Kč	- Masarykova univerzita, Fakulta informatiky	Ministerstvo vnitra
-------------------	-------------------------------	-----------------------------------	---	------------------------

Cílem výzkumného projektu bylo vyvinout a implementovat techniky zpracování přirozeného jazyka umožňující analýzu „extremistických“ jazykových projevů na Internetu s důrazem na určování autorství textů. Předmětem zájmu je veškerý webový obsah produkováný „extremistickými“ skupinami nebo jednotlivci, tj. webové stránky, fóra, chaty, blogy, sociální sítě a další zdroje. Hlavní softwarový výsledek – systém ART – má vysoký potenciál v reálném použití analyzovat velké množství psaného textu na internetu pomocí využití umělé inteligence a stylometrie. Podle jazykových, stylistických, grafických a

jiných charakteristik textu určuje pravděpodobnost shody autorství textů a přiřazuje autorství anonymním textům.

Rozvoj metod zkoumání fotografií v digitální i analogové formě za účelem zjištění, zda v obrazovém záznamu byly provedeny dodatečné zásahy

VF20102012010	1. 11. 2010 - 31. 10. 2012	Statní podpora 311 000 Kč	- Ústav teorie informace a automatizace AV ČR, v. v. i.	Ministerstvo vnitra
---------------	----------------------------	------------------------------	---	---------------------

Cílem projektu je zavést do kriminalistické expertizní praxe některé nové softwarové metody odhalování dodatečných zásahů v nepohyblivém obrazovém záznamu. Výstupem projektu jsou tři softwarové nástroje využívající analýzu obrazu k odhalení manipulace digitálních fotografií.

Nástroje a metody zpracování videa a obrazu pro boj s terorismem

VG20102015006	1. 10. 2010 - 30. 09. 2015	Statní podpora 11 080 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
---------------	----------------------------	---------------------------------	---	---------------------

Výzkumný projekt je zaměřen na zpracování záznamů obrazu a videa s cílem vytvořit funkční vzorek systému, který by umožnil kategorizaci, vyhledávání, porovnání biometrických údajů a jiné zpracování obrazové a video informace. Dalšími cíli jsou metodiky a algoritmy zpracování obrazových a video dat. Mezi výstupy projektu patří například software pro rozpoznání obličeje zaznamenaný z dronu, software pro vyhledávání osob ve videosekvencích, software pro zpracování termosnímků obličeje nebo nástroj pro vyhledávání rozdílů ve videosekvencích.

Multimediální analýza

VF20102014004	1. 10. 2010 - 31. 12. 2014	Statní podpora 7 416 tis. Kč	- Masarykova univerzita, Fakulta informatiky	Ministerstvo vnitra
---------------	----------------------------	---------------------------------	--	---------------------

Cílem projektu je provést rešerši zpracování multimediálních dat a otestování vhodných algoritmů a metod pro vyhledávání, identifikaci, popis, klasifikaci a analýzu multimediálních dat včetně dat na Internetu. Výstupem projektu jsou softwarové aplikace s využitím metod biometrie a strojového čtení k analýze multimediálních dat.

Behaviorální detekce pokročilých útočníků v počítačových sítích

VG20122014079	1. 1. 2012 - 31. 12. 2014	Statní podpora 8 491 000 Kč	- České vysoké učení technické v Praze, Fakulta elektrotechnická - Cognitive Security s.r.o.	Ministerstvo vnitra
---------------	---------------------------	--------------------------------	---	---------------------

Cílem projektu je vývoj nové generace software pro bezpečnostní monitoring sítí, tak, aby byly bezpečnostní týmy zajišťující monitoring citlivých systémů schopny detekovat aktivitu sofistikovaných útočníků. Výsledek projektu umožní detekci na míru připravených útoků, které se dnes stávají standardním operačním postupem státních i kriminálních útočníků.

Aplikovaný výzkum metody pro efektivní management síťové bezpečnosti datových center, ochrany cloud serverů a služeb ověřený praktickým měřením

VG2012201408 6	1. 1. 2012 - 31. 12. 2014	Státní podpora 7 976 000 Kč	- CertiCon a.s. - Cognitive Security s.r.o.	Ministerstvo vnitra
-------------------	---------------------------	--------------------------------	--	---------------------

Projekt je zaměřen na aplikovaný výzkum metody pro automatickou obrannou reakci na zjištěné bezpečnostní anomálie ve vysokorychlostních datových sítích. Výstupem projektu je software schopný reagovat na bezpečnostní hrozby na vysokorychlostních sítích, automatizovaně vyhodnocovat míru rizika zjištěné anomálie a automaticky realizovat obranné kroky na vybraných klíčových prvcích sítě, přičemž veškerá rozhodování by měl provádět na základě automatizovaného učení se z provozu sítě za použití metod umělé inteligence.

Efektivní vyhledávání v rozsáhlých biometrických datech - EFBIO

VG2012201507 3	1. 1. 2012 - 31. 12. 2015	Státní podpora 10 426 000 Kč	- Masarykova univerzita, Fakulta informatiky	Ministerstvo vnitra
-------------------	---------------------------	---------------------------------	--	---------------------

Projekt má za cíl navrhnout, implementovat a experimentálně ověřit univerzální systém vyhledávání v rozsáhlých kolekcích (až stovky milionů) biometrických dat. Výstupem projektu je několik softwarových produktů schopných porovnávat biometriku obličeje a chůze.

Zpřístupnění automatického ověřování mluvího širokého spektru uživatelů v oblasti bezpečnosti

VG2013201512 9	1. 4. 2013 - 30. 9. 2015	Státní podpora 8 926 000 Kč	- Phonexia s.r.o. - Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
-------------------	--------------------------	--------------------------------	--	---------------------

Výzkumný projekt se soustředí na adaptaci algoritmů rozpoznávání mluvího pro potřeby policejních a zpravodajských složek. Výstupem projektu je software schopný zejména vyhledávat a ověřovat mluvího na nahrávkách. Byla v něm implementována diarizace (segmentace nahrávky s označením, kde který mluvčí hovořil). Poskytuje jednoduché zobrazení výsledků tak, aby zodpovědní pracovníci získali včas potřebnou informaci a udrželi si rychlost reakce proti hrozbám a ve vyšetřování. Je možné dotrénovat algoritmy na cílových datech uživatele a zvýšit jejich úspěšnost.

Univerzální softwarová aplikace pro využití dat z kamerových systémů měst a obcí

VF2015201604 6	1. 9. 2015 - 31. 7. 2016	Statní podpora 799 000 Kč	- NITTA Systems s.r.o.	Ministerstvo vnitra
-------------------	--------------------------	---------------------------------	------------------------	------------------------

Cílem projektu bylo vyvinout softwarovou aplikaci umožňující přenos a vyhodnocování dat z různých kamerových systémů měst a obcí do policejní databáze s pokročilým vyhledáváním registračních značek vozidel.

Dolování infoRmAcí z řeči Pořízené vzdÁlenými miKrofony - DRAPÁK

VI2015202002 5	1. 10. 2015 - 30. 9. 2020	Statní podpora 17 656 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií - Phonexia s.r.o.	Ministerstvo vnitra
-------------------	---------------------------	------------------------------------	---	------------------------

Projekt se zaměřil na dolování informací z řeči pro složky bojující proti kriminalitě. Cílem projektu je zvýšit úspěšnost dolování v řeči pořízené vzdálenými mikrofony v reálném prostředí a generovat relevantní informace v odpovídajících operačních scénářích. Výstupem je sada softwarových nástrojů pro využití PČR. Tyto nástroje slouží zejména k automatickému dolování informací z hlasu, rozpoznání mluvčího, odstranění šumu nebo naopak k umělému zašumění řečové nahrávky.

Komplexní analýza a vizualizace heterogenních dat velkého rozsahu

VI2017202009 6	1. 1. 2017 - 31. 12. 2020	Statní podpora 13 927 000 Kč	- Masarykova univerzita, Ústav výpočetní techniky	Ministerstvo vnitra
-------------------	---------------------------	------------------------------------	--	------------------------

Cílem projektu je vytvořit integrovaný systém umožňující komplexní analýzu heterogenních dat velkého rozsahu - zejména digitálních nosičů informací získaných v rámci policejních vyšetřování. Výstupem projektu jsou softwarové nástroje, které umožňují automatizované a asistované vyhledávání komplexních souvislostí či událostí ve velkém objemu dat a jejich přehlednou vizualizaci. Software využívá komplexní interaktivní analýzy sesbíraných nosičů dat, tak i proudové analýzy přicházejících dat, která v reálném čase vyhledává předem známé souvislosti a je schopna upozornit na možnou kriminální činnost (dle známých vzorců chování), nebo sledovat nestandardní chování subjektů zájmu.

Automatizovaný panoramatický dohledový systém pro ochranu osob a majetku na sportovních stadionech

VI20172020105	1. 1. 2017 - 31. 12. 2020	Státní podpora 16 301 000 Kč	- JIMI CZ, a.s. - Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií	Ministerstvo vnitra
---------------	---------------------------	---------------------------------	---	---------------------

Cílem projektu bylo vyvinutí specializovaného dohledového systému pro sportovní stadiony. Dohledový systém má umožňovat panoramatické snímání tribun s diváky ve velmi vysokém rozlišení tak, aby bylo možné provádět automatickou analýzu obrazových dat. Součástí dohledového systému jsou metody pracující v reálném čase pro detekci specifických událostí či objektů (např. výskyt zakázaných hesel či symbolů). Dohledový systém má obsahovat nástroje pro následné zpracování pořízených záznamů, ve kterých bude možné provádět analýzu za účelem získání důkazního materiálu. Dohledový systém má umožňovat detekci a rozpoznání osob podle obličejů nebo oblečení v případě maskování, dále pak jejich sledování v davu a vyhledávání jejich pozice v obsáhlých záznamech. Systém má umožňovat doplnění databáze rizikových osob, kterým byl příslušnými orgány zakázán přístup na utkání. Informace z databáze má být možné sdílet mezi jednotlivými systémy tak, aby se daly rizikové osoby vyhledávat na všech stadionech.

Hardwarově akcelerovaná identifikace osob z videozáznamů s použitím hlubokého strojového učení

VI20172019086	1. 1. 2017 - 31. 12. 2019	Státní podpora 12 020 000 Kč	- GiTy, a.s. - Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií	Ministerstvo vnitra
---------------	---------------------------	---------------------------------	--	---------------------

Projekt byl zaměřen na vývoj pokročilé technologie "CamBrain", který slouží k doplnění funkcí kamerových systémů o schopnosti porozumění obsahu záznamu a jeho analýzu za účelem identifikace nebezpečných osob. Výzkum byl založen na tzv. hlubokém učení. Výstupem projektu je prototyp inteligentního systému doplňující kamerové systémy o schopnost automaticky upozornit ostrahu na hledané či podezřelé osoby v reálném čase.

Systém pro analýzu textových dat pro potřeby Policie ČR - SPAT

VH2017201702 3	1. 3. 2017 - 31. 12. 2018	Státní podpora 1 010 000 Kč	- Univerzita Karlova, Matematicko-fyzikální fakulta	Ministerstvo vnitra
-------------------	---------------------------	--------------------------------	---	---------------------

Projektem vyvíjel a implementoval metody počítačového zpracování textových dat do podmínek Policie ČR. Jednalo se následující metody zpracování textu: 1) automatické hledání pojmenovaných entit a jejich relací (osoby, firmy, adresy, komunikační prostředky, vozidla, účty, zbraně, drogy, významné události atd.) a to včetně hledání entit mimo slovníky (neznámá jména, adresy); 2) pokročilé fulltextové vyhledávání s podporou češtiny a angličtiny a schopností agregovat výsledky dle obsažených pojmenovaných entit; 3) podpora hledání podobných případů sdílejících stejnou podstatu či průběh lišících se ve faktech (např. vyhledá všechny případy, které mají podobný *modus operandi*, ač jsou v různých lokalitách, časech a vyskytují se v něm různé osoby); 4) vytváření souhrnu nejdůležitějších faktů vybraných případů.

Smart Camera - Dohledové centrum nové generace

VI20172019082	1. 1. 2017 - 31. 12. 2019	Statní podpora 7 979 000 Kč	- CertiCon a.s. - České vysoké učení technické v Praze, Český institut informatiky, robotiky a kybernetiky	Ministerstvo vnitra
---------------	---------------------------	--------------------------------	---	---------------------

Cílem projektu je vytvoření metod a jejich implementace pro pokročilou analýzu videa se zaměřením na sledování pohybu objektů (např. osob, vozidel) současným zapojením většího počtu kamer. Využívá možnost vzájemné komunikace kamer pro zpřesnění objektů a jejich chování, porovnává chování identifikovaného objektu se zadanými vzory chování, detekuje nestandardní chování a odhaluje tak bezpečnostní rizika. Výsledkem byl software připravený pro nasazení v akci.

Systém pro analýzu obrazových dat pro potřeby Policie ČR

VH2017201801 4	1. 1. 2017 - 31. 12. 2018	Statní podpora 13 856 000 Kč	- CAMEA, spol. s r.o. - Eyedea Recognition s.r.o. - Ústav teorie informace a automatizace AV ČR, v. v. i. - Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
-------------------	---------------------------	---------------------------------	--	---------------------

Projektem vyvíjel a implementoval metody počítačového zpracování obrazových dat do podmínek Policie ČR. Jednalo se následující metody zpracování obrazových dat: 1) inteligentní přehrávač umožňující vyhledat ve vstupním videu části s pohybem ve vybraném sektoru obrazu, odstranit šum, zaostřit a rekonstruovat poškozený obraz; 2) ze vstupního videa nebo obrázků extrahovat lidské obličeje, uložit je do databáze a porovnat je s již uloženými obličeji za účelem nalezení shody; 3) ze vstupního videa nebo obrázků extrahovat registrační značky vozidel, uložit je do databáze a porovnat je s již uloženými značkami za účelem nalezení shody; 4) ze vstupního videa nebo obrázků extrahovat lidské postavy, uložit je do databáze a rozpoznat jejich vlastnosti/pohyb/činnost, které následně umožní vyhledat.

Integrovaná platforma pro zpracování digitálních dat z bezpečnostních incidentů - TARZAN

VI20172020062	1. 1. 2017 - 30. 6. 2020	Statní podpora 15 775 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
---------------	--------------------------	---------------------------------------	--	------------------------

Projekt byl zaměřen na detekci a analýzu nových forem kybernetické kriminality v prostředí internetu věcí, mobilních a komunikačních aplikací. Cílem projektu byl výzkum nových metod založených na dolování dat, strojovém učení a vizuální analýze. Výstupem projektu je funkčního vzorku integrující různé metody pro efektivní vyšetřování incidentů a dále pak celá řada softwarových nástrojů týkající se zejména detekce provozu sítě TOR, bezpečnostní analýzy mobilních zařízení, řešení incidentů souvisejících s kryptoměnami, prolamování hesel a šifrovacích protokolů nebo analýzy síťového provozu.

Nástroje a metody zpracování videa a obrazu pro zvýšení efektivity operací bezpečnostních a záchranných složek

VI20172020068	1. 1. 2017 - 31. 12. 2020	Statní podpora 22 284 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
---------------	---------------------------	---------------------------------------	--	------------------------

Projekt zkoumal metody pro pořizování a zpracování obrazových dat a videosekvencí. Výstupem projektu byl funkční vzorek systému pro on-line zpracování videosekvencí v reálném čase pro operace bezpečnostních složek. Vyvinutý systém by měl umožňovat analýzu informací z různých obrazových zdrojů z místa zásahu, jejich kategorizaci, vyhledávání, agregaci, archivaci a efektivní reprezentaci. Součástí jsou také softwarové nástroje schopné pracovat s biometrií obličeje nebo s dálkově ovládaným dronem.

Vývoj automatizovaného nástroje pro predikci místa výskytu hledaných nebo pohřešovaných osob (pachatelů)

VH20182021039	1. 7. 2018 - 31. 10. 2021	Statní podpora 33 159 000 Kč	- eago systems spol. s r.o.	Ministerstvo vnitra
---------------	---------------------------	---------------------------------------	-----------------------------	------------------------

Cílem projektu bylo vyvinutí automatizovaného systému, který by vytyčil mapu s možnými vyznačenými místy či plochami, kde by se mohl vyskytovat pachatel nebo pohřešovaná či hledaná osoba. Výstupem projektu je softwarový nástroj pro predikci místa výskytu hledaných nebo pohřešovaných osob (pachatelů) využívající statistické postupy a neurální síť.

Zapojení umělé inteligence do příjmu tísňového volání

VI20192022169	1. 7. 2019 - 31. 5. 2022	Statní podpora 25 579 000 Kč	- Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství - Born Digital s.r.o. - GoodAI Applied s.r.o. - Phonexia s.r.o. - SpeechTech, s.r.o. - Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitřní
---------------	--------------------------	---------------------------------------	--	-------------------------

Projekt zkoumal nasazení umělé inteligence pro příjem tísňových volání pomocí hlasového chat-bota. Výstupem projektu byl hlasový chat-bot (voicebot) pro příjem tísňového volání.

Robustní zpracování nahrávek pro operativu a bezpečnost

VJ01010108	1. 10. 2020 - 30. 9. 2025	Statní podpora 47 937 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií - Západočeská univerzita v Plzni, Nové technologie - výzkumné centrum	Ministerstvo vnitřní
------------	---------------------------	---------------------------------------	---	-------------------------

Cílem projektu je dolování informací z řeči z reálných nahrávek pro potřeby bezpečnostních sborů. Projekt se zaměřuje na automatické rozpoznávání řeči, určení kdy kdo mluví v nahrávce (diarizace) a prohledávání pomocí akustických dotazů. Zkoumané technologie staví na společném rámci neurálních architektur strojového učení. Plánovaným výstupem projektu je 5 softwarových nástrojů, které budou testovány dvěma útvary Policie ČR.

Systém pro analýzu řeči

VH2020202105 0	1. 5. 2020 - 31. 12. 2021	Statní podpora 9 228 000 Kč	- Phonexia s.r.o.	Ministerstvo vnitřní
-------------------	---------------------------	-----------------------------------	-------------------	-------------------------

Cílem projektu bylo vyvinutí nástrojů pro analýzu řeči. Výstupem projektu jsou softwarové nástroje využívající biometrii lidského hlasu určené k identifikaci mluvčího a k automatickému přepisu hlasu do textu.

Algoritmy pro ztotožňování entit užívaných PČR

VH20202021054	1. 9. 2020 - 31. 12. 2021	Statní podpora 3 263 000 Kč	- ACREA CR, spol. s r.o.	Ministerstvo vnitra
---------------	---------------------------	--------------------------------	--------------------------	---------------------

Cílem projektu byl vývoj algoritmů, metod a technik, které umožní ztotožnění entit při činnosti policie (fyzická osoba, právnická osoba, vozidlo, adresa, bankovní účet, telefonní číslo apod.). Výstupem projektu je softwarový nástroj využívající těžbu dat, zpracování přirozeného jazyka a další pokročilé metody.

Mezinárodní spolupráce ve forenzní analýze otisků prstů a obrázků obličeje pro službu kriminální policie

VJ01030006	1. 1. 2021 - 30. 6. 2023	Statní podpora 2 892 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
------------	--------------------------	--------------------------------	--	---------------------

Cílem projektu je rozvoj spolupráce se zahraničními policejními složkami v oblasti analýzy a zpracování otisků prstů a biometrických dat obličeje. Výstupem projektu je workshop k získání zahraničních podnětů pro nové verze vyvíjených aplikací.

Čtení člověkem nečitelných poznávacích značek s nízkým rozlišením

VB01000003	1. 1. 2022 - 31. 12. 2023	Statní podpora 2 742 000 Kč	- Eyedea Recognition s.r.o.	Ministerstvo vnitra
------------	---------------------------	--------------------------------	-----------------------------	---------------------

Cílem projektu byl vývoj systému pro analýzu lidským okem nečitelných registračních značek vozidel. Výstupem projektu má být nástroj využívající metody umělé inteligence umožňující zachytit kamerovými systémy registrační značku vozidla v dostatečné kvalitě pro její přečtení.

Nástroje forenzní expertizy ručně psaného písma

VJ02010019	1. 1. 2022 - 31. 12. 2025	Statní podpora 16 216 000 Kč	- Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií - Ministerstvo vnitra, Policie ČR Kriminalistický ústav	Ministerstvo vnitra
------------	---------------------------	---------------------------------	---	---------------------

Cílem projektu je vývoj softwarových nástrojů, založených na kombinaci umělé inteligence, počítačového vidění a matematické statistiky, pro expertizu ručně psaného písma k získávání důkazního materiálu.

Sada forenzních analytických nástrojů ke zpracování obrazu a videa pro službu kriminální policie a vyšetřování

VJ02010041	1. 1. 2022 - 31. 12. 2025	Statní podpora 33 407 000 Kč	- Vysoké učení technické v Brně, Fakulta informačních technologií - České vysoké učení technické v Praze, Fakulta elektrotechnická	Ministerstvo vnitra
------------	---------------------------	---------------------------------	---	---------------------

Cílem projektu a předpokládaným výsledkem projektu je výpočetní jednotka s instalovaným softwarem. Softwarový nástroj má mimo jiné funkce být schopný provádět analýzu obrazových dat s lidskými postavami za účelem extrakce biometrických rysů osob a vyhledávání konkrétních objektů a scén ve velkých datových sadách.

Bezpečné dopravní systémy nové generace

VB01000048	1. 1. 2022 - 31. 12. 2023	Statní podpora 7 674 000 Kč	- CAMEA Technology, a.s. - Vysoké učení technické v Brně, Fakulta informačních technologií	Ministerstvo vnitra
------------	---------------------------	--------------------------------	---	---------------------

Projekt je zaměřen na monitorování silniční dopravy, včetně automatické detekce přestupků. Cílem je vytvoření výrobku typu kamerového senzoru využívajícího postupy umělé inteligence a jeho následného nasazení v praxi.

EyeDentity - rozpoznávání obličejových rysů pro odhad identity osob

TA04010768	1. 1. 2015 - 31. 12. 2017	Statní podpora 3 175 000 Kč	- Eyedea Recognition s.r.o.	Technologická agentura ČR
------------	---------------------------	--------------------------------	-----------------------------	---------------------------

Projekt byl zaměřen na obrazové rozpoznávání tváří v reálném prostředí bez kontrolovaného osvětlení, bez požadavků na vysoké rozlišení snímaných tváří a bez požadavku na specifické natočení tváře. Cílem projektu bylo vyvinout softwarový nástroj, který zefektivní vyhodnocení rozsáhlých video dat pro rozpoznávání tváří pomocí komplexního systému složeného z mnoha algoritmických modulů. Výstupem projektu byl softwarový modul Eyedentity Face SDK a funkční vzorek Eyedentity určené pro vysoce účinné rozpoznávání identity tváře. Systém Eyedentity lokalizuje tváře v obraze a všechny nalezené tváře následně porovnává vůči databázi zájmových osob. Systém umožňuje vyhodnocovat tváře v různém obrazovém rozlišení, je robustní vůči změně orientace tváře, změně emocí tváře, částečným zákrytům a vůči různým světelným podmínkám.

Pokročilé rozpoznávání výrobce a modelu vozidla

FW01010336	1. 1. 2020 - 31. 12. 2021	Statní podpora 4 118 000 Kč	- Eyedea Recognition s.r.o.	Technologická agentura ČR
------------	---------------------------	--------------------------------	-----------------------------	---------------------------

Cílem projektu byl vývoj algoritmů pro novou generaci systému rozpoznávání výrobce a modelu vozidla nezávisle na detekci registrační značky se zvýšenou účinností ve zhoršených světelných podmínkách. Výstupem projektu je softwarový nástroj využívající hluboké učení.

Analýza textových dat – extrakce entit

VC202320230 06	1. 1. 2023 - 31. 12. 2023	Statní podpora 4 939 000 Kč	- ACREA CR, spol. s r.o. - České vysoké učení technické v Praze, Fakulta informačních technologií	Ministerstvo vnitra
-------------------	------------------------------	-----------------------------------	--	------------------------

Cílem je vývoj algoritmů, metod a technik, které umožní automatickou extrakci pojmenovaných entit, užívaných při činnosti Policie ČR, a nalezení jejich vzájemných vazeb. Entity (např. fyzická osoba, právnická osoba, vozidlo, adresa, bankovní účet, telefonní číslo) jsou definovány v rámci existujícího centrálního datového modelu. Cílem je vyvinout softwarový nástroj, který dokáže extrahovat uvedené entity včetně jejich vazeb z volných nestrukturovaných textů. Jedná se o lingvistickou doménu policejních textů v českém, anglickém, německém, francouzském, španělském a ruském jazyce

Profilace drogových zásilek a kurýrů

VC202220230 03	25. 10. 2022 - 24. 10. 2023	Statní podpora 1 691 000 Kč	- ACREA CR, spol. s r.o.	Ministerstvo vnitra
-------------------	--------------------------------	-----------------------------------	--------------------------	------------------------

Cílem projektu je vyvinout softwarového nástroj, který na základě naučených pravidel a strojového učení, dokáže s předem definovanou mírou pravděpodobnosti navrhnout konkrétní zásilku nebo přepravce, aby ji nebo jeho podrobily zákonné kontrole orgánů činných v trestním řízení. Dnes dochází k náhodným kontrolám, kontrolám na základě detekčních prostředků (technické, pomocí psa) nebo na základě operativních informací, kdy se např. z celkového počtu desítek miliónů zásilek ročně podaří na našem území odhalit cca. 500 zásilek. Algoritmická profilace pomocí nového nástroje má tento počet významně zvýšit.

Výzkum a vývoj nových modulů umělé inteligence Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob

FW01010562	1. 1. 2020 - 31. 12. 2022	Statní podpora 18 084 000 Kč	- Cogniware, s.r.o.	Technologick á agentura ČR
------------	------------------------------	---------------------------------------	---------------------	-------------------------------

Cílem projektu bylo vyvinutí softwarového nástroje Cogniware Insights 2.0 pro sledování a detekci anomálií a predikci chování osob. Softwarový nástroj byl zamýšlen jako komplexní, integrovaná a otevřená platforma zaměřená na vyšetřování a pokročilou analýzu podezřelých objektů, aktivit a vztahů

s využitím prvků umělé inteligence a statistických analýz Big Data. Softwarový nástroj by měl obsahovat detekci anomálií, modulu pro klasifikaci objektů do skupin dle příbuznosti, predikci chování, rozpoznávání osob a objektů z obrazu.

Vývoj a testování algoritmů pro prediktivní behaviorální analýzu osob překračujících vnější hranice EU

VH2018201903 4	1. 5. 2018 - 31. 10. 2019	Statní podpora 2 806 000 Kč	České vysoké učení technické v Praze, Fakulta informačních technologií	Ministerstvo vnitra
-------------------	------------------------------	-----------------------------------	--	------------------------

Cílem projektu bylo zvýšit pravděpodobnost včasného odhalení a dopadení zájmových osob policie a jiných správních orgánů, překračujících vnější hranice EU a ČR. V rámci projektu byly vyvinuty algoritmy, které vyhodnocují rizika u jednotlivých osob z vazeb mezi záznamy z minulosti a těmi aktuálně získanými.

Predikce a ochrana před kybernetickými incidenty

VI2015202002 6	1. 9. 2015 - 31. 8. 2020	Statní podpora 8 352 000 Kč	- CZ.NIC, z.s.p.o.	Ministerstvo vnitra
-------------------	-----------------------------	-----------------------------------	--------------------	------------------------

Hlavním cílem projektu bylo vybudování systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů. Tento systém má na základě analýzy dat a informací o provozu v Internetu z celé řady nejrozumnějších zdrojů vytvářet metody a postupy pro vyhodnocování zranitelností kritické informační infrastruktury.

6. Mezinárodní spolupráce

„Zároveň je nutno uvést, že riziko spojené s hrozbou selhání lidského faktoru není možné úplně odstranit.“

Ladislav Adámek, pověřenec pro ochranu osobních údajů Policie České republiky

6.1 Sdílení biometrických dat v Evropské unii

Za účelem řešení mezinárodní kriminality byla dne 27. května 2005 v německém městě Prüm dojednána **Prümská úmluva**.⁸⁸ Prvních sedm států – Rakousko, Belgie, Francie, Německo, Lucembursko, Nizozemsko a Španělsko – na základě této mezivládní úmluvy začalo sdílet otisky prstů, profilů DNA a registračních značek vozidel. Policejní orgány států, který je stranou úmluvy, získaly možnost porovnat otisky prstů nebo profily DNA v databázích ostatních států úmluvy. Základní prvky Prümské úmluvy byly v roce 2008 převzaty Prümským rozhodnutím,⁸⁹ které umožnilo sdílení otisků prstů, profilů DNA a registračních značek vozidel mezi všemi státy Evropské unie. Kromě členských států Evropské unie se prümského systému účastní nebo na něm přislíbilo účast Norsko, Island, Velká Británie, Švýcarsko a Lichtenštejnsko.

Prümský systém nemá žádnou centrální složku nebo databázi, kde by byly všechny údaje. Systém policejním orgánům členských států umožňuje přístup k anonymním datům vnitrostátních databází všech připojených členských států, v nichž jsou zaevidovány profily DNA a otisky prstů. Tento přístup je umožněn pouze národním kontaktním místům. Zatímco odpověď týkající se nalezené shody je poskytnuta během několika vteřin nebo minut, může trvat i týdny než tazatel odpovídající osobní údaje

⁸⁸Úmluva 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.

⁸⁹Rozhodnutí 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.

související s nalezenou shodou obdrží. Výměna informací po zjištění shody se řídí vnitrostátním právem, a podléhá tak různým pravidlům a postupům.

V současnosti je zvažována „modernizace“ průmského 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 navrhla Evropská komise dne 8. prosince 2021 **nové nařízení Prüm II**.⁹⁰ Návrh 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. Bude to znamenat, že se všechny vnitrostátní databáze v každém členském státě budou připojovat k centrálnímu směrovači, místo aby se připojovaly jedna k druhé. Návrh nařízení dále upravuje automatizovanou výměnu dalších kategorií údajů, jako jsou zobrazení obličeje a policejní záznamy. Součástí průmského systému by se měl stát také Europol, který by na základě tohoto nařízení spravoval biometrické údaje osob získané ze třetích zemí.

Implementací návrhu by byla vytvořena jedna z nejrozsáhlejších biometrických sledovacích infrastruktur na světě kombinující několik různých biometrických charakteristik. Nejkontroverznější změnou v průmském systému je právě rozšíření o vyobrazení obličeje a možnost spouštět proti nim algoritmy pro rozpoznávání obličejů. Byla by tak prakticky využívána ke zpětné biometrické identifikaci na dálku. Zahrnuty by do tohoto systému byly miliony fotografií obličejů lidí, které členské státy zpracovávají. Maďarsko má 30 milionů fotografií, Itálie 17 milionů, Francie 6 milionů a Německo 5,5 milionu. Tyto fotografie mohou zahrnovat podezřelé, obviněné, odsouzené, žadatele o azyl a neidentifikovaná mrtvá těla. Nicméně některé členské státy vytvořily databáze zobrazení obličejů na základě civilních registrů. Příkladem je

⁹⁰Návrh 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. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0784>

Maďarsko a také Česká republika (blíže v kapitole 4.1.3 Informační systém Digitální podoba osob).

Vyhodnocením stavu připravenosti na implementaci nařízení Prüm II mezi členskými státy se zabýval projekt *Towards the European Level Exchange of Facial Images* (dále jen „**TELEFI**“). Projekt financovaný Evropskou unií byl v letech 2019 až 2021 realizován skupinou šesti evropských institucí: Estonský forenzní institut, Estonský úřad policie a pohraniční stráž, Finský národní úřad pro vyšetřování, Lotyšský státní úřad forenzních věd, Nizozemský forenzní institut a Švédské národní forenzní centrum.

Projekt měl za cíl především zmapovat stav využívání biometricky obličejů v jednotlivých členských státech. V rámci toho bylo zjišťováno, zda členské státy a některé mezinárodní subjekty zřizují národní databáze vyobrazení obličejů; jaké praktiky a postupy realizují; jaký software a počítačové systémy využívají; jaká je vnitrostátní právní úprava v jednotlivých členských státech; jaké používají standardy kvality pro snímky obličejů; a jaké mají policejní orgány vize a názory na budoucí výměnu snímků obličejů. Součástí projektu byla také mezinárodní konference policejních orgánů. Výstupem projektu pak byla studie o využívání biometrické identifikace dle obličejů policejními orgány v členských státech Evropské unie.

Podle informací od národních policejních orgánů byla zpětná biometrická identifikace na dálku do prosince 2020 implementována v jedenácti členských státech Evropské unie (Rakousko, Finsko, Francie, Německo, Řecko, Maďarsko, Itálie, Lotyšsko, Litva, Nizozemsko a Slovinsko), ve Spojeném království a Europolu a Interpolu. V sedmi členských státech Evropské unie (Chorvatsko, Kypr, Česká republika, Estonsko, Rumunsko, Španělsko a Švédsko) dosáhla příprava na nasazení zpětné biometrické identifikace na dálku fáze, že bylo očekáváno spuštění během jednoho až dvou let. Přitom vzhledem k současným poznatkům bylo v České republice již nasazeno (více v kapitole 4.1.3 Informační systém Digitální podoba osob) a lze očekávat, že i v ostatních zmíněných státech. Devět policejních orgánů členských států (Belgie, Bulharsko, Dánsko, Irsko, Lucembursko, Malta, Polsko, Portugalsko a Slovensko) v době realizace

projektu uvádělo, že zatím nemají konkrétní plány na zavedení biometrické identifikace dle obličeje.⁹¹

Policie České republiky již provádí technické kroky k tomu, aby přizpůsobila svou infrastrukturu na budoucí průmyskový systém a současně integrovala dílčí biometrické databáze. Zásadním krokem je budování **Centrálního biometrického informačního systému** na základě veřejné zakázky o celkové předpokládané hodnotě 635 milionů Kč. Jedná se o biometrický informační systém, který by měl integrovat celou řadu různých způsobů biometrické identifikace. Součástí dodávky jsou komunikační rozhraní s národními a mezinárodními biometrickými systémy. Zakázku realizuje společnost VÍTKOVICE SOLUTIONS a.s. V červnu 2023 bylo dokončeno vybavení koncových pracovišť včetně analýzy a dodávky softwarového řešení Centrálního biometrického informačního systému. Do konce roku 2023 má pak proběhnout integrace s externími systémy, migrace dat a spuštění Centrálního biometrického informačního systému do provozu.

Centrální biometrický informační systém bude slučovat funkcionality použití biometrie pro účely jak kriminalistické práce, tak pro účely bezpečnostní. V oblasti bezpečnostní bude systém poskytovat služby zejména pro cizineckou policii v oblasti cizinecké a migrační politiky České republiky a v oblasti kriminalistické práce pro službu kriminální policie a vyšetřování. Systém by měl nahradit stávající policejní databázi otisků prstů (AFIS).⁹² Bude navíc pracovat s identitami, které jsou vedeny v policejní databázi profilů DNA (FODAGEN) a informačním systému Cizinci s povoleným pobytem (CIS). Informační systém bude sloužit jako jediné komunikační rozhraní pro ostatní systémy, které budou s biometrickými údaji pracovat. Bude umožňovat zpracování: otisků prstů (píchané i valené), otisků dlaní, hran dlaní, stop prstů, stop dlaní, fotografií osob (portrét, celá postava, trojdílná fotografie), fotografií tetování i dalších zvláštních znamení, barevných kopií dokladů, biografických a demografických dat, popisu osob.

⁹¹TELEFI Project. Summary Report of the project "Towards the European Level Exchange of Facial Images" Version 1.0. Závěrečná zpráva projektu ze ledna 2021.

⁹²AFIS je automatizovaný systém identifikace otisků prstů z anglického „Automatic Fingerprint Identification System“

Centrálního biometrického informačního systému bude sloužit k výměně dat dle mezinárodních smluv a nařízení Evropské unie. Bude vybaven rozhraními se systémy Prüm, Eurodac⁹³, AFIS FBI a dalšími. Navíc bude schopný komunikovat s externími systémy: Schengenský informační systém (SIS), Vízový informační systém (VIS), Systém vstup/výstup (EES)⁹⁴, Evropský informační systém rejstříku trestů – státní příslušníci třetích zemí (ECRIS-TCN) a dalšími.

V budoucnu by měl systém umožňovat rozšíření o identifikaci dle oční duhovky či sítnice, ale také o fonetickou identifikaci mluvcího (zpracování *voice printů* osob z telekomunikačního provozu, prostorových odposlechů a jiných zvukových záznamů). S rozvojem technologie lze předpokládat, že v budoucnu bude možné identifikovat fyzické osoby jen na základě způsobu chůze nebo jiných behaviorálních znaků zachycených kamerovým systémem. Z toho důvodu má být Centrální biometrický informační systém flexibilní a snadno rozšiřitelný o další komponenty zpracovávající jiné biometrické charakteristiky.

6.2 Mezinárodní výzkum spojující soukromý a veřejný sektor

Policie České republiky se zapojila také do mezinárodního výzkumu a vývoje systémů umělé inteligence, které fungují na bázi *Public-Private Partnership*. Jedná se o dva mezinárodní projekty dotované z evropského fondu Horizont 2020, přičemž oba projekty jsou realizovány konsorciem desítek členů z řad národních policejních orgánů členských států a dále soukromých společností, které se věnují vývoji systémů umělé inteligence v oblasti kriminalistiky. Celková podpora ze zdrojů Evropské komise za oba projekty činí 24 milionů Euro, což odpovídá zhruba 600 milionů korun.

⁹³Eurodac je systém pro srovnání otisků prstů žadatelů o azyl.

⁹⁴EES z anglického „*Entry/Exit System*“ je systém evidující příjezd a odjezd cizinců ze třetích zemí do prostoru Evropské unie.

První z nich pojmenovaný Analýza sítě, textu a mluvčího v reálném čase pro boj s organizovaným zločinem uváděný pod akronymem **ROXANNE** (z anglického „*Real time network, text, and speaker analytics for combating organized crime*“) byl výzkumný projekt realizovaný v letech 2019 až 2022. Jeho cílem bylo vytváření systémů umělé inteligence k odhalování zločineckých skupin a osob analýzou textů, řeči, videa a sítí v reálném čase. Na projektu spolupracovaly policejní orgány, průmyslové společnosti a výzkumné instituce. Projektové konsorcium zahrnovalo 25 organizací z 16ti členských států Evropské unie, přičemž 11 z nich byly policejní orgány z 10ti různých zemí. Projektovým koordinátorem byla švýcarská společnost IDIAP. Za Českou republiku byly kromě Policie České republiky do projektu zapojeny také společnost Phonexia a.s. a Vysoké učení technické v Brně. Výše příspěvku Evropské komise a rovněž celkové náklady projektu byly 7 milionů Euro. Konečným produktem byla technická platforma, která využívá nové nástroje rozpoznávání hlasu, jazyka a video technologií. ROXANNE byl testován na reálných datech z devíti členských států Evropské unie.

Druhý z nich Udržitelná autonomie a odolnost pro policejní orgány používající umělou inteligenci proti hrozbám s vysokou prioritou uváděný pod akronymem **STARLIGHT** (z anglického „*Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats*“) je výzkumný projekt započatý v říjnu 2019, který by měl trvat až do října 2025. Projekt je zaměřen na boj proti zločinu souvisejícímu s umělou inteligencí pomocí řešení na základě systémů umělé inteligence. Projekt má za cíl najít řešení, jak mají policejní orgány reagovat na nové hrozby, a to prostřednictvím lepší kybernetické bezpečnosti a vyššímu povědomí o nepřátelské umělé inteligenci. Na projektu spolupracují policejní orgány, průmyslové podniky a výzkumné instituce. Projektové konsorcium je složeno z celkem 52 organizací z 18ti evropských států, přičemž 15 z partnerů projektu jsou policejní orgány. Projektovým koordinátorem je francouzská výzkumná organizace Komise pro atomovou energii a alternativní energie. Z České republiky je jediný partner projektu – Policejní prezidium Policie České republiky. Celkové náklady projektu jsou ve výši 18,8 milionů Euro z nichž Evropská komise přispívá částkou 17 milionů Euro. STARLIGHT má pomoci policejním orgánům chránit své vlastní systémy umělé inteligence a zvýšit schopnosti policejních orgánů proti

zločinu a terorismu podporovanému umělou inteligencí. Výstupem projektu mají být datové soubory, standardizovaný rámec a centrum umělé inteligence pro policejní orgány.

7. Zdroje informací

7.1 Odborné

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

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

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

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

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

Mareš M., Kleiner J., Zwiefelhofer T., Kasl F., Míšek J. Kamerový systém Dopravního podniku hlavního města Prahy v komparativním kontextu bezpečnosti a ochrany osobních údajů. 2021. Studie zadaná Dopravním podnikem Hlavního města Praha.

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

7.2 Zveřejněné dokumenty

Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Dostupné z:

https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_cs.pdf

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

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

European Data Protection Supervisor. EDPS Decision on the own initiative inquiry on Europol's big data challenge. Vydané 5. října 2020. Dostupné z: https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en

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

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

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

Licenční smlouvy mezi Krajským ředitelstvím policie Ústeckého kraje a Eyedea Recognition s.r.o. uzavřené dne 20. listopadu 2018 a dne 19. listopadu 2019. Poskytnutí licence pro software EyeDentity.

Číslo jednací objednatele KRPU-209961-6/ČJ-2018-0400IT-02A a KRPU-167484-6/ČJ-2019-0400IT-03.

Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0206>

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. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0784>

Nejvyšší státní zastupitelství. Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019. V Brně dne 29. ledna 2020, 3 SE 101/2020.

Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. dubna 2023 vydané Ředitelstvím služby cizinecké policie pod číslem jednacím CPR-16176-6/ČJ-2021-930103.

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

Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 16. srpna 2023 vydané Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednacím PPR-35618-5/ČJ-2023-990810.

Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 11. září 2023 vydané Krajským ředitelstvím policie Ústeckého kraje pod číslem jednacím KRPU-160885-2/ČJ-2023-0400KR-PI.

Poskytnutí informací na základě žádosti o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ze dne 14. září 2023 vydané Krajským ředitelstvím policie Ústeckého kraje pod číslem jednacím KRPU-166623-2/ČJ-2023-0400KR-PI.

Rozhodnutí o částečném odmítnutí žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, vydané dne 20. srpna 2020 Odborem komunikace a vnějších vztahů Policejního prezidia pod číslem jednací PPR-24979-6/ČJ-2020-990810.

Rozkaz Policejního prezidenta č. 194/2022, k zajištění zkušebního provozu informačního systému Digitální podoba osob.

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

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

TELEFI Project. Summary Report of the project "Towards the European Level Exchange of Facial Images" Version 1.0. Závěrečná zpráva projektu ze ledna 2021.

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

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

Usnesení Evropského parlamentu ze dne 6. října 2021 o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech. Dostupné z: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_CS.html

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

7.3 Právní předpisy

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

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

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

Nařízení Evropského parlamentu a Rady (EU) 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).

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

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

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

Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

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.

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.

7.4 Internet

Alsharif M., Santan C. Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology. 2023. Dostupné z <https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447>

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

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

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

Česká Televize. Události, komentáře ze dne 17. dubna 2023. (čas 33:22) Dostupné z: <https://www.ceskatelevize.cz/porady/1096898594-udalosti-komentare/223411000370417/>

Hlaváčová K. Stačí oči a kousek nosu či chůze. Česká kamera rozpozná člověka i konkrétní auto. 2020. Dostupné z: <https://zpravy.aktualne.cz/domaci/staci-oci-a-kousek-nosu-ci-chuze-cesky-kamerovy-system-pozna/r-0db5c8b2ee8c11eaa6f6ac1f6b220ee8/>

IDnes. Česká firma pomáhá Europolu rozpoznat tváře zločinců a teroristů. Ze dne 7. července 2016. Dostupné z: https://www.idnes.cz/technet/software/eyedea-europol-rozpoznavani-obrazu.A160704_154924_software_pka

Magazín CIO Business World. Francouzská protiteroristická jednotka používá český software pro rozpoznávání obličejů. Ze dne 27. března 2018. Dostupné z: <https://www.cio.cz/aktuality/francouzska-protiteroristicka-jednotka-pouziva-cesky-software-pro-rozpoznavani-obliceje/>

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

Ministerstvo vnitra České republiky. Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích. Tisková zpráva ze dne 18. února 2018. Dostupné z:

<https://www.mvcr.cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezinarodnich-letistich.aspx>

Novinky.cz. Inteligentní kamery vidí i slyší. Chytré technologie mění česká města. Zpráva ze dne 12. listopadu 2023. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-inteligentni-kamery-vidi-i-slysi-chytre-technologie-meni-ceska-mesta-40450506>

Policie České republiky. Automatická kontrola vozidel. Zveřejněná informace ze dne 11. listopadu 2022. Dostupné z: <https://www.policie.cz/clanek/zverejnene-informace-2022-automaticka-kontrola-vozidel.aspx>

Policie České republiky. eGATE – rychlejší odbavování na letišti. Zpráva ze dne 23. července 2015. Dostupné z: <https://www.policie.cz/clanek/egate-rychlejsi-odbavovani-na-letisti.aspx>

Policie České republiky. Interpol doporučil databázi Reliéf. Zpráva ze dne 23. května 2016. Dostupné z: <https://www.policie.cz/clanek/interpol-doporucil-databazi-relief.aspx>

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

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

Tisková zpráva luRe: Policie již téměř rok využívá analytický nástroj na rozpoznávání tváří. Podrobnosti jeho fungování taji. Dostupné z: <https://digitalnisvobody.cz/blog/2023/07/12/tz-policie-jiz-temer-rok-vyuziva-analyticky-nastroj-na-rozpoznavani-tvari-podrobnosti-jeho-fungovani-ale-pred-verejnosti-taji/>

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

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

Úřad pro ochranu osobních údajů. Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech. Zpráva ze dne 27. března 2020. Dostupné z:

https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40780&n=vyjadreni%2Duoou%2Dk%2Dnavrhu%2Dregulace%2Dnasili%2Dna%2Dfotbalovych%2Dstadionech

Václavíková J. "Počítač se spletl." Policie zatkla špatného muže kvůli technologii na poznání tváře. 2020. Dostupné z: <https://zpravy.aktualne.cz/zahranici/pocitac-se-spletl-policie-zatkla-spatneho-muze-kvuli-technol/r-b3cdeb14c1cb11ea8972ac1f6b220ee8/>

7.5 Judikatura

Nález německého ústavního soudu ze dne 15. prosince 1983. 1 BvR 209/83. Dostupné na: https://www.bverfg.de/e/rs19831215_1bvr020983.html

Nález pléna Ústavního soudu České republiky ze dne 22. března 2011. Pl. ÚS 24/10.

Nález Ústavního soudu České republiky ze dne 10. října 2021. II. ÚS 1022/21.

Rozsudek Evropského soudu pro lidská práva ze dne 10. února 2000. Amann proti Švýcarsku, číslo stížnosti 27798/95.

Rozsudek Evropského soudu pro lidská práva ze dne 28. dubna 2003. Peck proti Spojenému království, číslo stížnosti 44647/98.

Rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2008. S. a Marper proti Spojenému království, číslo stížnosti 30562/04.

Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 8. dubna 2014. Spojené věci C-293/12 a C-594/12, Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další.

Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 6. října 2015. C-362/14, Schrems proti Data Protection Commissioner.

Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 21. prosince 2016. Spojené věci C-203/15 a C-698/15, Tele2 Sverige AB proti Post- och Telestyrelsen a Secretary of State for the Home Department proti Tom Watson a dalším.

Rozsudek Evropského soudního dvora ze dne 4. prosince 1974. 41/74, Yvonne van Duyn proti Home Office.

Český Minority Report: Využití umělé inteligence Policií České republiky

Mgr. et Mgr. Václav Mach, Ph.D.

Vydalo Iuridicum Remedium, z.s. v prosinci 2023

Přístavní 1236/35, 170 00 Praha 7 (sídlo)

Jeseniova 10, 130 00 Praha 3 (kancelář)

Kontakt

420 776 703 170

iure@iure.org

www.iure.org

www.digitalnisvobody.cz

www.bigbrotherawards.cz

Licence

Na titulní stránce je využit grafický prvek, který byl součástí kampaně ReclaimYouFace.eu.

Text *Český Minority Report: Využití umělé inteligence Policií České republiky*
autora Iuridicum Remedium, z. s. je publikován pod licencí **CC-BY-SA 4.0**

